KU LEUVEN

ARENBERG DOCTORAL SCHOOL
Faculty of Engineering Science

Digital Certificate Usage and Management in Vehicular Communication Systems

Takahito Yoshizawa

Supervisor:
Prof. dr. ir. Bart Preneel

Dissertation presented in partial fulfillment of the requirements for the degree of Doctor of Engineering Science (PhD): Electrical Engineering

November 2023

Digital Certificate Usage and Management in Vehicular Communication Systems

Takahito YOSHIZAWA

Examination committee:
Prof. em. dr. Adhemar Bultheel, chair
Prof. dr. ir. Bart Preneel, supervisor
Prof. dr. ir. Vincent Rijmen
Prof. dr. ir. Sofie Pollin
Dr. ir. Dave Singelée
Prof. dr. ir. Mathy Vanhoef
Prof. dr. Panos Papadimitratos
(KTH Royal Institute of Technology)
Prof. dr. Jan Tobias Mühlberg
(Université Libre de Bruxelles)

Dissertation presented in partial fulfillment of the requirements for the degree of Doctor of Engineering Science (PhD): Electrical Engineering

November 2023

© 2023 KU Leuven – Faculty of Engineering Science
Uitgegeven in eigen beheer, Takahito Yoshizawa, Kasteelpark Arenberg 10, B-3001 Leuven (Belgium)

Alle rechten voorbehouden. Niets uit deze uitgave mag worden vermenigvuldigd en/of openbaar gemaakt worden door middel van druk, fotokopie, microfilm, elektronisch of op welke andere wijze ook zonder voorafgaande schriftelijke toestemming van de uitgever.

All rights reserved. No part of the publication may be reproduced in any form by print, photoprint, microfilm, electronic or any other means without written permission from the publisher.

Preface

Pursuing a PhD degree is mostly a solitary endeavor. It is certainly true for the most part. It was especially exacerbated by Covid-19 period during which much of the work in this thesis was done. However, looking back, I realize that I have met and worked together with more than a few people along the way. They have been an indispensable part of the work that have eventually culminated to this thesis. I have learned many things along the way, thanks to their help in different capacities. For this reason, I would like to thank the following people. Prof. Bart Preneel, Dr. Dave Singelée, of ESAT COSIC group in KU Leuven, Prof. Jan Tobias Muehlberg of Cybersecurity Research Center in Université Libre de Bruxelles, Prof. Chris Tampère and Dr. Mohammad Ali Arman of Mechanical Engineering department in KU Leuven, Dr. Stephane Delbruel of University of Bordeaux, Prof. Amirhosein Taherkordi of University of Oslo, Dr. Xavier Carpent and Ms. Dimah Almani of University of Nottingham, Prof. Gunes Acar of Radboud University, and Dr. Farhad Aghili of Sirris.

I would like to thank the professors in the examination committee: Prof. Adhemar Bultheel of NUMA in the engineering science dept. Prof. Bart Preneel, Prof. Vincent Rijmen, and Dr. Dave Singelée of COSIC, Prof. Sofie Pollin of WaveCoRE, Prof. Mathy Vanhoef of DistriNet, Prof. Panos Papadimitratos of KTH Royal Institute of Technology, and Prof. Jan Tobias Mühlberg of Université Libre de Bruxelles.

I would also like to thank Prof. Frank Kargl of University of Ulm and all the participants I have met at the Dagstuhl seminar in June 2023. It was an exceptional experience.

This list of people to thank is not complete without mentioning all the people at conferences for interesting discussion – although I have already forgotten many of their names. Lastly, I would like to thank my friends and ex-colleagues for the moral support and encouragement I received during this period.

This thesis is dedicated to my parents. Lastly, I would like to thank my wife, Hilde, for her patience and understanding over the years.

Abstract

Along with autonomous driving, integrating telecommunication capabilities into vehicles is one of the new trends in the automotive industry. This communication integration, or so-called Intelligent Transport Systems (ITS), is an area where traditionally two different industries intersect: a crossroad of automotive and telecommunication industries. The objective of ITS is to improve road safety by vehicles sharing information with one another by directly communicating among them.

In 1999, the US Federal Communications Commission (FCC) allocated spectrum in 5.9 GHz band for ITS systems. A similar spectrum allocation followed in Europe by the European Commission in 2008. Since then, Standard Developing Organizations (SDOs) have been standardizing ITS technology; some of the most prominent ones include the Institute of Electrical and Electronics Engineers (IEEE), the Society for Automotive Engineers (SAE), and the European Telecommunication Standard Institute, Intelligent Transport Systems (ETSI ITS).

To achieve the goal of improving road safety, as with any ICT technologies, the vehicular communication needs to be secure so that it can provide a reliable and trustworthy service. One essential requirement is that only legitimate entities can gain access to the communication channel. This is a vital property in cyber-physical systems (CPS) such as road traffic involving vehicles and other road users. Potential consequences of failing to meet this property include accidents, physical damage, loss of property, or loss of life. Furthermore, user privacy needs to be guaranteed to ensure vehicle owners' personal information will not be compromised due to the use of vehicular communication. In other words, this technology needs to have sufficient protection mechanisms in place against adversaries and malicious activities such as eavesdropping and tracking. Irrespective of the usefulness of this technology and resulting improvement in road safety, if the vehicular communication fails to protect legitimate communication participants from these threats, ITS technology may

as well result in doing more harm than good. In this sense, security and privacy aspects are of paramount importance in vehicular communication.

The original use case for vehicular communication was vehicle-to-vehicle direct communication, or V2V in short. Subsequently, use cases expanded to include infrastructure (vehicle-to-infrastructure (V2I)), network or cloud access through mobile network (vehicle-to-network (V2N) or vehicle-to-cloud (V2C)), and other road users such as pedestrians and cyclists (vehicle-to-person or vehicle-to-pedestrian (V2P)). Collectively, vehicular communication is referred as Vehicle-to-Everything (V2X). In this sense, the scope of security and privacy protection has also expanded.

The theme and the objective of this thesis is to examine and evaluate the security and privacy in the existing ITS standards from a V2X communication perspective. We mainly focus on IEEE 1609, SAE, and ETSI ITS standard specifications. We selected these standards due to the functionalities they provide to realize basic safety-related services which are the fundamental building blocks for realizing road safety. When appropriate, we propose new solutions to resolve the issues identified and fill gaps to further improve the quality of these standards toward improving road safety.

Beknopte samenvatting

Samen met autonoom rijden is het integreren van telecommunicatiemogelijkheden in voertuigen één van de nieuwe trends in de auto-industrie. Deze communicatie integratie, aangeduid met de term Intelligente Transportsystemen (ITS), is een gebied waar van oudsher twee verschillende industrieën elkaar kruisen: de auto- en de telecommunicatie-industrie. Het doel van ITS is om de verkeersveiligheid te verbeteren door voertuigen informatie met elkaar te laten delen door rechtstreeks met elkaar te communiceren.

In 1999 wees de Amerikaanse Federal Communications Commission (FCC) spectrum toe in de 5,9 GHz-band voor ITS-systemen. Een vergelijkbare spectrumtoewijzing werd in Europa uitgevoerd door de Europese Commissie in 2008. Sindsdien zijn de organisaties belast met het opstellen van standaarden (SDO's) actief bezig met het standaardiseren van ITS-technologie. Enkele van de meest prominente onder hen zijn het Institute of Electrical and Electronics Engineers (IEEE), de Society for Automotive Engineers (SAE) en het European Telecommunication Standards Institute, Intelligent Transport Systems (ETSI ITS).

Om de verkeersveiligheid te verbeteren, moet, zoals bij elke ICT-technologie, de voertuigcommunicatie veilig zijn, zodat het een betrouwbare dienstverlening kan bieden. Deze betrouwbaarheid in communicatie wordt gewaarborgd door alleen legitieme entiteiten toegang te geven tot het communicatiekanaal. Dit is een essentiële eigenschap in cyberfysische systemen (CPS) zoals wegverkeer waarbij voertuigen en andere weggebruikers betrokken zijn. Mogelijke gevolgen van het niet voldoen aan deze eigenschap zijn ongelukken, fysieke schade, verlies van eigendom of verlies van mensenlevens. Bovendien moet de privacy van de gebruiker worden gewaarborgd zodat de persoonlijke informatie van een voertuigeigenaar niet in gevaar wordt gebracht door het gebruik van communicatie. Met andere woorden, deze technologie moet voldoende beschermingsmechanismen hebben tegen kwaadwillende activiteiten zoals afluisteren en volgen. Ongeacht het nut van deze technologie en de daaruit

voortvloeiende verbetering van de verkeersveiligheid, als de communicatie er niet in slaagt om alle deelnemers aan de communicatie te beschermen tegen deze bedreigingen, ITS-technologie meer kwaad dan goed doen. In die zin zijn beveiligings- en privacyaspecten van het grootste belang bij voertuigcommunicatie.

De oorspronkelijke gebruikssituatie voor voertuigcommunicatie was directe voertuig-tot-voertuig communicatie, of kortweg V2V. Vervolgens werden de gebruikssituaties uitgebreid tot infrastructuur (vehicle-to-infrastructure (V2I)), netwerk- of cloud-toegang via een mobiel netwerk (vehicle-to-network (V2N) of vehicle-to-cloud (V2C)), en andere weggebruikers zoals voetgangers en fietsers (voertuig-naar-persoon of voertuig-naar-voetganger (V2P)). Gezamenlijk wordt voertuigcommunicatie Vehicle-to-Everything (V2X) genoemd. In deze zin is de reikwijdte van beveiliging en privacy bescherming ook uitgebreid.

Het thema en het doel van dit proefschrift is het onderzoeken en evalueren van de beveiliging en privacy in de bestaande ITS standaarden vanuit het perspectief van V2X communicatie. We richten ons voornamelijk op IEEE 1609, SAE en ETSI ITS standaardspecificaties. We hebben deze standaarden geselecteerd vanwege de functionaliteiten die ze bieden om basisveiligheidsdiensten te realiseren die de fundamentele bouwstenen zijn voor het realiseren van verkeersveiligheid. Waar nodig stellen we ook nieuwe oplossingen voor om de geïdentificeerde problemen op te lossen en de hiaten op te vullen om de kwaliteit van deze standaarden verder te verbeteren voor het realiseren van een veiliger verkeer.

List of Abbreviations

3GPP	3rd Generation Partnership Project
5G	5th Generation
AA	Authorization Authority
ACA	Authorization CA
ACPC	Activation Code for Pseudonym Certificates
AD	Additional Data
ADAS	Advanced Driver Assistance System
AEAD	Authentication Encryption with Associated Data
AES-GCM-SIV	AES Galois/Counter Mode Synthetic Initialization Vector
AS	Application Server
ASN.1	Abstract Syntax Notation One
AT	Authorization Ticket
AV	Autonomous Vehicle
BC	Blockchain
BSM	Basic Safety Message
BTMPP	Balancing Trust Management and Privacy Preservation
C2C-CC	Car-to-Car Communication Consortium
CA	Certificate Authority
CAM	Cooperative Awareness Message
CAN	Controller Area Network
CCAM	Cooperative Connected and Automated Mobility
CCMS	Cooperative ITS Credential Management System
C-ITS	Cooperative ITS
CPS	Cyber Physical System
CR	Certificate Request
CRACA	Certificate Revocation Authorizing CA
CRL	Certificate Revocation List
CSR	Certificate Signing Request
C-V2X	Cellular V2X

D2D	Device-to-Device
DAA	Direct Anonymous Attestation
DCM	Device Configuration Manager
DDoS	Distributed Denial of Service
DENM	De-centralized Environmental Notification Message
DSRC	Dedicated Short Range Communications
E2E	End-to-End
EA	Enrolment Authority
EC	European Commission
ECA	Enrolment CA
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECU	Electronic Control Unit
EEBL	Emergency Electronic Brake Light
ETSI	European Telecommunications Standard Institute
EVA	Emergency Vehicle Alert
FCC	Federal Communications Commission
GDPR	General Data Protection Regulation
GPA	Global Passive Adversaries
HSM	Hardware Security Module
ICA	Intersection Collision Avoidance
ICA	Intermediate CA
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFAL	Issue First Activate Later
IOI	Item of Interest
IoT	Internet of Things
IPWAVE	IP Wireless Access in Vehicular Environment
ITS	Intelligent Transport System
ITS-S	ITS Station
KEM	Key Encapsulation Mechanism
KGK	Key Generation Key
LA	Linkage Authority
LAA	Local Active Adversaries
LoC	Line of Code
LOP	Location Obscurer Proxy
LPC	Lightweight Pseudonym Changing
LSB	Least Significant Byte
LTE	Long Term Evolution
MA	Misbehaviour Authority
MFA	Multi-Factor Authentication

MLGS	Message Linkable Group Signature
MNO	Mobile Network Operator
MR	Misbehaviour Report
MTU	Maximum Transmit Unit
NHTSA	National Highway Traffic Safety Administration
NIS	Network and Information System
NIST	National Institute of Standards and Technology (US)
OBU	On-Board Unit
OCB	Outside the Context of Basic service set
OCSP	Online Certificate Status Protocol
P2PCD	Peer-to-Peer Certificate Distribution
PCA	Pseudonym CA
PK	Public Key
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
PRF	Pseudo-Random Function
ProSe	Proximity Service
RA	Registration Authority
RCA	Root CA
RCA	Registration CA
RSA	Road Side Alert
RSU	Road Side Unit
RTS	Road Traffic Safety
SA	Security Association
SAE	Society of Automotive Engineers
SCMS	Security Credential Management System
SDO	Standard Developing Organization
SUMO	Simulation of Urban MObility
TAA	Threshold Anonymous Announcement
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TR	Technical Report
TS	Technical Specification
TSG	Technical Specification Group
UE	User Equipment
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2P	Vehicle-to-Person / Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VAM	VRU Awareness Message
VRU	Vulnerable Road User
WAVE	Wireless Access in Vehicular Environments

Contents

Abstract iii

Beknopte samenvatting v

List of Abbreviations vii

Contents xi

List of Figures xvii

List of Tables xix

I Digital Certificate Usage and Management in Vehicular Communication Systems 1

1 Introduction 3

1.1 Overview of Relevant Standards 3

1.1.1 IEEE 802.11p 4

1.1.2 Cellular V2X (C-V2X) 6

1.1.3 IEEE 1609 7

1.1.4 SAE 8

1.1.5 ETSI ITS 8

1.1.6 Characteristics of Security Solutions in IEEE 1609.2 and ETSI ITS 10

1.2 Properties of Vehicular Communication 13

1.2.1 Privacy Properties 13

1.3 Research Questions 14

1.4 Contributions 15

1.4.1 Identifying Gaps in Security and Privacy Aspects 15

1.4.2 Proposing Security-Enhancing Scheme 15

1.4.3 Proposing Privacy-Enhancing Scheme 15

2 Gaps in Standards on Security and Privacy Aspects 17
2.1 Introduction 17
2.2 Analysis and Issue Categorization 19
2.2.1 Overview 19
2.2.2 Privacy Protection 19
2.2.3 Certificate-Based Message Verification 23
2.2.4 Communication Modes 28
2.2.5 Message Handling 29
2.2.6 System Level 30
2.3 Root Cause Analysis 32
2.3.1 Conflicting or Insufficient Specification 32
2.3.2 Characteristics of Vehicular Communication Environment 33
2.3.3 Broadcast-Based Communication 33
2.3.4 Implementation-Dependent Ambiguity 34
2.3.5 Certificate Usage and Management for Vehicles 34
2.3.6 Certificate Management of Non-Vehicle ITS-S Types . . 34
2.3.7 RSU Infrastructure Dependency 34
2.3.8 Mobile Operator Involvement and Dependency 35

3 Security Enhancements 37
3.1 Overview 37
3.2 Misbehaviour Reporting 37
3.3 Pseudonym Certificate Generation and Distribution 39
3.4 Post-Quantum Impact on Certificates 41
3.5 Certificate Digest Handling 44

4 Privacy Enhancement 49
4.1 Overview 49
4.2 A New Beacon Scheme 49

5 Closing Discussion 53
5.1 Discussion 53
5.1.1 Answers to the Research Questions 53
5.1.2 Adversarial Assumptions (Attacker Models) 56
5.2 Future Work 57
5.3 Closing Remarks 58

6 Conclusion 61

Bibliography 71

II Publications **73**

List of Publications **75**

A Survey of Security and Privacy Issues in V2X Communication Systems **79**

1 Introduction 82
1.1 Overview 82
1.2 Methodology and Contributions 84
1.3 Document Organization 85
2 Related Work 86
3 V2X Technologies 88
3.1 IEEE Standard 88
3.2 3GPP Standard 89
3.3 Differences between ITS-G5/DSRC and C-V2X 89
3.4 ISO Standard 91
4 Security Management System Overview 92
4.1 ETSI C-ITS and IEEE 1609.2 92
4.2 Differences between ETSI C-ITS and IEEE 1609.2 . . . 93
5 Attack Types and Threats 96
6 Security Issue: Privacy Protection 97
6.1 Privacy and Vehicle Operation 98
6.2 Applicability of Privacy 1: Vehicle Types and Usages . . 99
6.3 Applicability of Privacy 2: Non-Vehicle ITS-S 100
6.4 Privacy and Cooperative Awareness 100
6.5 Privacy vs. Road Safety 101
6.6 Privacy and Use of Unicast 102
7 Security Issue: Use of Certificates 104
7.1 Certificate-Based Message Verification 104
7.2 Certificate Usage and Change Policy 105
7.3 Certificate Reloading 105
7.4 Certificate Revocation 106
7.5 Certificate Management of RSUs 109
7.6 Certificate Management of VRUs 109
7.7 Certificate Usage in Multiple Communications 111
8 Security Issue: Communication Modes 112
8.1 Broadcast-Oriented Communication 112
8.2 Unicast – Confidentiality Protection 112
9 Security Issue: Message Handling 114
9.1 Plausibility Validation and Misbehavior Detection . . . 114
9.2 Communication involving Vulnerable Road Users 117
10 Security Issue: System Level Issues 117
10.1 ITS-S Device-Dependent Trust Level 117

10.2 Interconnection between Multiple Security Management Systems . . . 118
10.3 Multiple Security Management Systems for Different ITS-S Types . . . 120
10.4 Absence of Consideration on Post-Quantum Cryptography Technologies . . . 120
11 Root Cause Analysis And Recommendations . . . 121
12 Conclusion and Future Work . . . 127
References . . . 133

Survey of Security Aspect of V2X Standards and Related Issues 147
1 Introduction . . . 149
2 Evolution OF V2X Standards . . . 150
2.1 802.11-OCB mode (formerly 802.11p) . . . 150
2.2 IETF IPWAVE . . . 152
2.3 IEEE 1609 and ETSI ITS . . . 154
2.4 Cellular-based: LTE V2X . . . 155
2.5 Cellular-based: 5G V2X . . . 157
3 Security Consideration on The Hybrid Approach . . . 159
4 Conclusion and Future Work . . . 160
References . . . 160

A New Privacy Enhancing Beacon Scheme in V2X Communication 163
1 Introduction . . . 165
2 Related Work . . . 166
2.1 Our contribution . . . 167
3 New Beacon Scheme . . . 168
3.1 Overview . . . 168
3.2 Security Properties of the Beacon Scheme . . . 169
3.3 Adversary Model . . . 170
3.4 Beacon Scheme Algorithm . . . 170
3.5 Consideration on Security Properties . . . 172
4 Simulation . . . 173
4.1 Approach . . . 173
4.2 Discussion and Evaluation . . . 175
5 Conclusions and Future Work . . . 178
References . . . 178

On Handling of Certificate Digest in V2X Communication 181
1 Introduction . . . 183
2 CAM Transmission and Reception . . . 185
3 Simulation to Reproduce Real-World Traffic Flow . . . 186
3.1 Traffic Data . . . 187

3.2 Approach and Methodology . . . 188
4 Discussion and Evaluation . . . 191
5 Related Work . . . 195
6 Conclusion and Future Work . . . 195
References . . . 196

Misbehaviour Reporting in ETSI ITS Standard Considered Broken 199
1 Introduction . . . 201
2 Related Work . . . 202
3 Background . . . 203
4 Misbehaviour Scenario Descriptions . . . 204
4.1 Scenario 1 . . . 204
4.2 Scenario 2 . . . 205
5 Issues of Misbehaviour Reporting in The ETSI ITS Standard . 205
5.1 Absence of MA ID in Vehicles . . . 206
5.2 No Unique Information in the AT . . . 207
5.3 Lack of Communication Models . . . 208
5.4 Lack of Revocation Details . . . 208
5.5 Problem Statement and the Root Cause . . . 209
6 Solution . . . 209
6.1 Design Goals . . . 210
6.2 Solution Part 1: Identifying an MA for a Vehicle . . . 210
6.3 Solution Part 2: Resolving a Vehicle from an AT . . . 211
7 Discussion and Evaluation . . . 214
8 Recommendations . . . 215
9 Conclusion . . . 216
References . . . 216

A New Approach To Pseudonym Certificate Management in V2X Communication 221
1 Introduction . . . 223
2 Related Work . . . 224
3 Background and Related Standards . . . 225
3.1 IEEE 1609.2, 1609.2.1 (SCMS) . . . 225
3.2 ETSI ITS (CCMS) . . . 226
3.3 Issue First Activate Later (IFAL) . . . 226
4 IFAL Issues . . . 228
4.1 Wasted Certificates . . . 228
4.2 Transfer of Private Key Information over Activation . . 228
4.3 No Forward and Backward Secrecy . . . 228
4.4 Inflexible AT Usage Policy . . . 229
4.5 Gap Period in Passive Revocation . . . 229
4.6 Sub-optimal and Unreliable Activation Channels . . . 229

5 A Novel Activation Scheme 230
5.1 Goals and Assumptions 230
5.2 Solution Description 230
5.3 Detailed Description – Activation 231
5.4 Detailed Description – OBU Tx Operation 234
5.5 Detailed Description – Certificate Use 234
6 Analysis and Discussion 234
6.1 Security Properties 234
6.2 Storage and Bandwidth Comparison 236
6.3 Simulation Result of AES-GCM-SIV 236
6.4 Advantages 240
6.5 Disadvantages 240
7 Conclusion and Future Work 241
References 241

Post-Quantum Impacts on V2X Certificates – Already at The End of The Road 245
1 Introduction 247
2 Background 248
2.1 Certificate Definition in V2X Standards 248
2.2 Emergence of PQC Algorithms 249
2.3 Migration to PQC Algorithm 249
3 Discussion 250
3.1 Absence of Forward Compatibility 250
3.2 Impacts on Pseudonym Certificates 251
3.3 Mitigating Ineffective Channel Usage 255
3.4 Impacts on RCA and ICA Certificates 255
4 Proposals 256
5 Related Work 257
6 Conclusion and Future Work 258
References 258

Curriculum 263

List of Figures

1.1 Communication Model between Vehicles 4
1.2 V2X Protocol Stacks 5
1.3 IEEE 1609.2.1 PKI Architecture (reproduced from Fig.1 in IEEE 1609.2.1) 10
1.4 ETSI ITS PKI Architecture (reproduced from Fig.11a in ETSI TS 102 940) 12

A Survey of Security and Privacy Issues in V2X Communication Systems 79
1 Overview of V2X Communication System 83
2 Overview of Security and Privacy Aspects in V2X Systems. . . 84
3 Overview of Security Management System 93
4 DENM and Privacy Requirement 102
5 Scenario of Interconnection between Management Systems . . . 119

Survey of Security Aspect of V2X Standards and Related Issues 147
1 Protocol Stack for ETSI ITS / 802.11 OCB, 3GPP PC5, and 3GPP Uu Interfaces 151
2 IPWAVE Architecture – V2V and V2I Inter-Connection 153
3 V2X Reference Architecture 156

A New Privacy Enhancing Beacon Scheme in V2X Communication 163
1 CAM Usage over 24hr Period (Large City, Weekdays) 176
2 CAM Usage over 24hr Period (Small City, Weekdays) 177
3 CAM Usage over Varying Provisional CAM Probability (p) . . 177

On Handling of Certificate Digest in V2X Communication 181
1 Route of the Simulated Traffic 187
2 Traffic Combinations 190

3 In-Range Event per Second (The red, green, and blue bars represent the number of events per second in 300m, 400m, and 500m communication range, respectively. For each bar, the darker color at the bottom and the lighter color at the top show the *high-impact* and *low-impact* category.) 192

Misbehaviour Reporting in ETSI ITS Standard Considered Broken 199
1 Use Case Scenarios 205
2 Architectural Difference between IEEE 1609.2 and ETSI ITS 102 940 206
3 Determining the MA from an AT 210
4 Linkage Generation and Resolution 212
5 Improved MR Reporting in Scenario in Fig. 1(a) 213

A New Approach To Pseudonym Certificate Management in V2X Communication 221
1 Epoch Key Derivation in IFAL 227
2 OAuth Model in Vehicle Context 231
3 Activation Status Generation and Verification 232

Post-Quantum Impacts on V2X Certificates – Already at The End of The Road 245
1 Certificate Definition in IEEE 1609.2 251
2 Hybrid Certificate and a Message That Contains It 251
3 Channel Capacity Reduction (Hybrid Certificates) 253

List of Tables

1.1 IEEE 1609 Specifications 7
1.2 V2X-Related SAE Specifications 9
1.3 ETSI ITS Specifications 9
1.4 CA Entities in IEEE 1609.2 and ETSI ITS 11

2.1 Issue Categorization 20
2.2 Root Causes 33

A Survey of Security and Privacy Issues in V2X Communication Systems 79
1 US and EU ITS Specifications (Security Specific) 93
2 Attack Types and Threats 96
3 Summary of Security Issues 122
4 List of Recommended Actions to ETSI ITS Specifications . . . 126
5 V2X Related Survey Papers 129
6 V2X Related EU Projects 132

Survey of Security Aspect of V2X Standards and Related Issues 147

A New Privacy Enhancing Beacon Scheme in V2X Communication 163
1 Simulation Parameters 173
2 Traffic Congestion in Brussels by Time of the Day (2019) . . . 174

On Handling of Certificate Digest in V2X Communication 181
1 Vehicle Routes 187
2 Traffic Density (vehicles/hour) 189
3 Unknown Certificate Handling Matrix 191
4 In-Range Duration (sec.) 193
5 Reduced Overhead Due to InlineP2pcdRequest Message Supression 194

Misbehaviour Reporting in ETSI ITS Standard Considered Broken 199

1 Symbol Definitions 204
2 Terminologies of Equivalent System Entities 207
3 Problem Description and Root Cause 209

A New Approach To Pseudonym Certificate Management in V2X Communication 221
1 Notation Definitions 232
2 Comparison of Required Storage and Bandwidth 237
3 Simulation Result of Authorization Query / Response 237
4 Comparison of Key Points in Solutions 239

Post-Quantum Impacts on V2X Certificates – Already at The End of The Road 245
1 Certificate and Message Size for The Legacy and PQC Algorithms 254

Part I

Digital Certificate Usage and Management in Vehicular Communication Systems

Chapter 1

Introduction

1.1 Overview of Relevant Standards

Over the past decades, wireless communication technologies have proliferated to many different usages, purposes, and applications in various industries. One of these trends is the use of wireless communication in automobiles. Vehicles nowadays are equipped with many sensors and with over 100 computers [81], most of which are intended for dedicated purposes. These on-board computers are connected with one another over a bus called Controller Area Network (CAN) bus [83]. This vehicular communication is envisioned to realize road safety by communicating and sharing vehicle movement and safety-related information with other vehicles and other entities on the road such as Road Side Units (RSUs). This technology complements existing vehicle sensors, and is expected to support autonomous driving functionality to make it a reality. The communication model of direct Vehicle-to-Vehicle (V2V) communication is shown in Figure 1.1.

This vehicular communication is achieved through a protocol stack consisting of multiple standards. The exact set of standards in the protocol stack varies depending on two aspects: (1) countries and regions, and (2) access technologies. From the first perspective, the US and Europe have defined their own standards. At high level, European standards can be characterized as an adaption and modification of the US standards. From the second perspective, IEEE 802.11-based and mobile system-based technologies (Cellular V2X, or *C-V2X*) are defined as the access technologies. The IEEE 802.11-based solution was first defined in 2010, and subsequently C-V2X was standardized by the 3rd

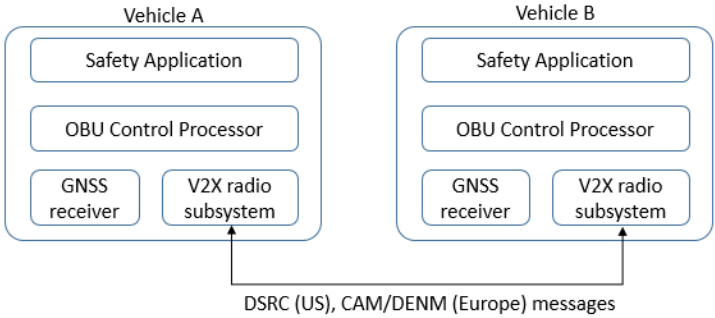


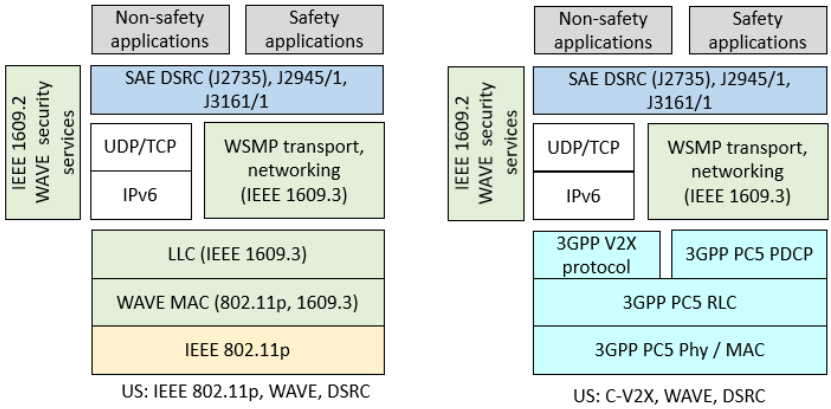
Figure 1.1: Communication Model between Vehicles

Generation Partnership Project (3GPP) in the second half of 2010s.

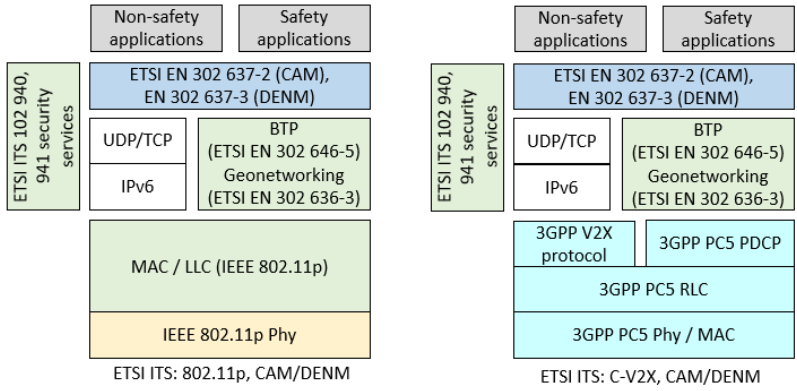
Figure 1.2 illustrates the four variations of protocol stacks. Figure 1.2(a) shows the US standard based on 802.11 (left) and C-V2X (right). Figure 1.2(b) shows the European standard based on 802.11 (left) and C-V2X (right). For the rest of this section, we provide an overview of these standards.

1.1.1 IEEE 802.11p

In Oct. 1999, the FCC has allocated 75 MHz of spectrum in the 5.9 GHz frequency bands (5.850-5.925 GHz) for the purpose of vehicular communication, or *Intelligent Transport System (ITS)* [16]. In 2004, the IEEE 802.11 committee launched the standardization work to specify vehicular communication based on the wireless LAN standard (commonly referred as "Wi-Fi"). They published the first version of this standard in 2010 as an amendment called 802.11p, titled *"Amendment 6: Wireless Access in Vehicular Environments"* [78]. The technical nature of this amendment can be characterized as a simplified version of the conventional 802.11 standard where some control-plane and user-plane functionalities are either simplified or removed. These changes include: (1) no discovery and association between devices, (2) no device authentication, and (3) no encryption of user data. This simplification was necessary in the vehicular communication environment where the communication topology constantly changes due to moving vehicles. This 802.11p amendment was subsequently incorporated into the main 802.11 standard specification in 2016 [48]. At this time, the set of functionalities specified in 802.11p was renamed to "Outside the Context of Basic service set" (*OCB mode*). In simple terms, the *OCB mode* allows 802.11 devices to transmit 802.11 user data frames in clear without establishing association and authentication between devices. This simplification



(a) US Standard (IEEE WAVE), 802.11p based, C-V2X-based



(b) European Standard (ETSI ITS), 802.11p based, C-V2X-based

Figure 1.2: V2X Protocol Stacks

enables moving vehicles to transmit safety-related messages and communicate with surrounding vehicles within communication range.

The communication environment of vehicles can be characterized as follows – if we consider a set of vehicles within the communication range of a reference vehicle ($S = (v_1, v_2, ...v_n)$ where v_n denotes nth vehicle), the members of this set S constantly change due to the movement of the reference vehicle itself and other vehicles. Due to this dynamic nature, it is not practical to try to identify each vehicle within this set S as vehicles moves in and out of the communication range from a given vehicle as a point of reference depending on the relative speed and direction. Due to this dynamic nature, broadcast-based

communication naturally suits direct vehicule-to-vehicle (V2V) communication where the transmitting vehicle is not aware of, nor is it concerned with, the exact number and identities of the receiving vehicles. In this sense, one can see that the type of simplification made in 802.11p (*OCB mode* in 2016 version of 802.11 specification [48]) is the necessary modification to the 802.11 standard.

1.1.2 Cellular V2X (C-V2X)

Despite the completion of the 802.11 standard, its actual commercial deployment was slow due to various technical and non-technical reasons. Partly due to this reason, some vehicle manufacturers shifted their attention away from 802.11-based access technology. In 2015, 3GPP started the standardization work of Cellular V2X (*C-V2X*) as a Release-14 feature.[1] It is a solution that operates in LTE systems. Following this, 3GPP started work for the equivalent feature based on 5G in the Release-15 time frame. Partly due to the slow deployment of the 802.11-based Dedicated Short Range Communications (DSRC) services since the spectrum was allocated, C-V2X has gained momentum [16]. In addition, V2X communication based on successful mobile technologies such as LTE and 5G also offers the potential to expand the V2X use cases involving non-vehicle entities, such as pedestrians and cyclists who use smartphones.

Following this growing momentum of C-V2X, in 2019, FCC issued a statement that the spectrum in the 5.9 GHz band previously allocated for ITS purposes is being re-allocated [17]. Specifically, the 75 MHz spectrum originally allocated to the 802.11-based DSRC service is split into three parts: (1) the lower 45 MHz (5.850-5.895 GHz) for the expansion of unlicensed usage (i.e. WiFi), (2) the next 20 MHz (5.895-5.915 GHz) for C-V2X usage, and (3) the remaining upper-most 10 MHz (5.915-5.925 GHz) for the 802.11-based DSRC service. In other words, this proposed change means that both 802.11-based and C-V2X-based V2X access technologies become viable and legitimate technologies in the market. Subsequent to this announcement, the FCC further announced in 2022 that C-V2X will replace the remaining 10 MHz spectrum left for 802.11-based DSRC service [15]. This means that the C-V2X, as the access technology, will completely replace the 802.11-based DSRC service in the future as the latter technology is phased out.

As stated above, C-V2X is based on mobile technology. Because the mobile terminals, or *User Equipment* (UE) in 3GPP terminology, communicate with

[1] 3GPP Release 14 started from the 3rd quarter of 2014 and ended in the 2nd quarter of 2017. V2X was one of the main features in this release along with other features such as mission critical communication, cellular IoT, machine-type communication (MTC), WLAN coordination, and voice-over LTE (VoLTE).

the mobile network through base stations, a new access procedure needed to be defined in order to realize direct communication between UEs for direct communication among vehicles (V2V). Because 3GPP has previously defined a technically similar feature for public safety community, this solution was used as a baseline to define solution for V2X. From the system architecture perspective, this direct communication link between UEs is called the *PC5* reference point. From a radio-centric perspective, it is called *sidelink*. Specifically for the V2X solution, the C-V2X architecture is specified in 3GPP TS 23.285 [3] for LTE and TS 23.287 [5] for 5G.

1.1.3 IEEE 1609

Subsequent to the start of 802.11p standardization work by the 802.11 committee, IEEE launched the 1609 committee in the mid-2000s to specify higher layer vehicular communication over 802.11p as the physical and data link layers; they coined the term *Wireless Access in Vehicular Environments (WAVE)*. The 1609 standard consists of multiple specifications as shown in Table 1.1.

Table 1.1: IEEE 1609 Specifications

Specification	Latest version	Title
1609.0	2019	WAVE Architecture
1609.2	2022	WAVE Security Services for Applications and Management Messages
1609.2.1	2022	WAVE Certificate Management Interfaces for End Entities
1609.3	2020	WAVE Networking Services
1609.4	2016	WAVE Multi-Channel Operations
1609.11	2010	WAVE Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS)
1609.12	2019	WAVE Identifier Allocations

Around 2006, the IEEE 1609 standard committee started publishing vehicular communication standard specifications. In particular, the IEEE 1609.2 specification defines the security aspects of the WAVE standard.

A large proportion of the security solution in WAVE is dedicated to the Public Key Infrastructure (PKI). A PKI system is organized in a hierarchical manner in which the top-level entity is called the root CA (RCA); it issues digital certificates to lower-level authorities such as intermediate CA (ICA) and other end entities. The certificate management system for vehicular communication, as

a PKI system, generates and distributes digital certificates for the system entities and end entities such as vehicles. This PKI solution in IEEE 1609.2 is called Security Credential Management System (SCMS). The PKI entities includes Certificate Authorities (CAs) such as the Root CA (CA), the Enrolment CA (ECA), the Registration CA (RA), the Authorization CA (ACA), the Linkage Authority (LA), and the Certificate Revocation Authorizing CA (CRACA). The end entities include vehicles, Roadside Units (RSU), and other road user devices.

1.1.4 SAE

The Society for Automotive Engineers International (SAE International) is a Standards Defining Organization (SDO) that creates standards for various industries, such as aerospace and automotive industries. One of the well-known automotive-related standards specified by SAE is J3016: *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* [73]. It is the categorization of the level of autonomous driving capabilities in vehicles, with level 0 being no automation and level 5 being full autonomy.

The most representative SAE specifications for vehicular communication are listed in Table 1.2. Dedicated Short-Range Communication (DSRC) is the standard that specifies the *application layer* of the vehicular communication. It is specified in J2735 *Dedicated Short Range Communications (DSRC) Message Set Dictionary*, first published in 2009 [70]. It sits on top of the 802.11p and WAVE layers, and specifies the message formats and contents vehicles transmit. The latest version of J2735 is from 2022 [76]. The standard defines 32 messages; some of its representative message types include: Basic Safety Message (BSM), Emergency Vehicle Alert (EVA), Intersection Collision Avoidance (ICA), and Road Side Alert (RSA). As can be seen from these message types, DSRC defines types of events or conditions to disseminate among vehicles on the road to improve road safety. In addition, J2945/1 *On-Board System Requirements for V2V Safety Communications* [74] specifies requirements for the minimum function and performance of BSM by light vehicles.

1.1.5 ETSI ITS

In Europe, the ETSI Technical Specification Group (TSG) Intelligent Transport Systems (ITS) was formed in 2007; its first specification was published in late 2000s. From the protocol stack perspective, the ETSI ITS standard is equivalent to the combination of IEEE 1609 and SAE J2735. Compared to

Table 1.2: V2X-Related SAE Specifications

Specification	Latest version	Title	Ref.
J2735	2022	Dedicated Short-Range Communication (DSRC) Message Set Dictionary	[76]
J2945/1	2020	On-board System Requirements for V2V Safety Communications	[74]
J2945/2	2018	Dedicated Short Range Communications (DSRC) Performance Requirements for V2V Safety Awareness	[72]
J3061	2021	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	[75]

the IEEE 1609 and SAE standards, the ETSI ITS standard consists of a large number of specification documents, each one of them covering a specific technical aspect. Because our interest is in security and privacy aspects of vehicular communication, we focus on the set of specifications that are relevant to security and privacy. Table 1.3 contains these specifications.

Table 1.3: ETSI ITS Specifications

Spec #	Latest Version	Title	Ref.
TS 102 731	V.1.1.1, 2010-09	Intelligent Transport System (ITS); Security; Security Services and Architecture	[21]
TS 102 940	V.2.1.1, 2021-07	Intelligent Transport System (ITS); Security; ITS Communications Security Architecture and Security Management	[27]
TS 102 941	V.2.1.1, 2021-10	Intelligent Transport System (ITS); Trust and Privacy Management	[32]
TS 102 942	V.1.1.1, 2012-06	Intelligent Transport Systems (ITS); Security; Access Control Technical Specification	[22]
TS 102 943	V.1.1.1, 2012-06	Intelligent Transport Systems (ITS); Security; Confidentiality Services	[23]
TS 103 097	V.2.1.1, 2021-10	Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats	[33]

Security and privacy aspects of ETSI ITS specifications are mostly based on IEEE 1609.2 starting from the PKI system architecture model to the ASN.1 definitions. However, there are some significant differences between them. These

differences can be characterized as architectural simplifications in ETSI ITS version compared to the one in IEEE 1609.2.

1.1.6 Characteristics of Security Solutions in IEEE 1609.2 and ETSI ITS

Figure 1.3 shows the overall PKI architecture of the vehicular communication certificate management system for the US, taken from the IEEE 1690.2.1 [49] specification. This is called a Security Credential Management System (SCMS). Its architecture includes multiple CAs as summarized in Table 1.4. Similarly, Figure 1.4 shows the corresponding PKI architecture defined in ETSI TS 102 940 [27] for Europe. By comparing these two figures, it is clear that the former defines more entities than the latter. This means that the SCMS system is more complex as these entities need to interact and coordinate with one another to realize the overall certificate management functionalities.

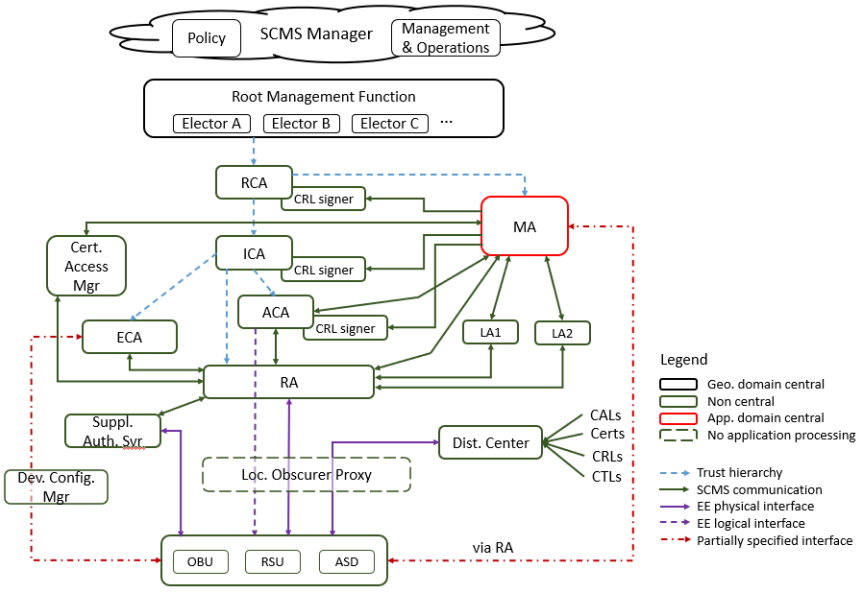


Figure 1.3: IEEE 1609.2.1 PKI Architecture (reproduced from Fig.1 in IEEE 1609.2.1)

Some entities that exists only in the IEEE 1609.2 PKI system are defined to offer more elaborate features. Examples includes the Registration Authority (RA)

Table 1.4: CA Entities in IEEE 1609.2 and ETSI ITS

IEEE 1609.2 PKI system entity Name (Acronym)	ETSI ITS PKI system entity Name (Acronym)	Main functionality
Root CA (RCA)	Root CA (RCA)	the top-most CA
Intermediate CA (ICA)	(see note 1)	one level below RCA
Enrollment CA (ECA)	Enrolment Authority (AA)	handle end entity enrolment
Authorization CA (ACA)	Authorization Authority (AA)	issue pseudonym certificates to end entities
Registration Authority (RA)	(see note 2)	accept and handle registration request from end entities.
Linkage Authorities (LA1,LA2)	(see note 2)	create and resolve linkage between pseudonym and real identity of end entities.
Misbehavior Authority (MA)	Misbehaviour Authority (MA)	investigate the misbehaviour of end entities.
Location Obscurer Proxy	(see note 2)	hide vehicle location from the PKI system.
Distribution Center	Distribution Center (see note 3)	distribute lists, e.g. CRLs.

Note 1: The ETSI ITS architecture does not explicitly define the ICA although equivalent functionalities may be required to deploy the solution.

Note 2: The ETSI ITS architecture does not explicitly define these entities because it does not require such functionalities.

Note 3: The ETSI ITS architecture specifies that this is an optional entity.

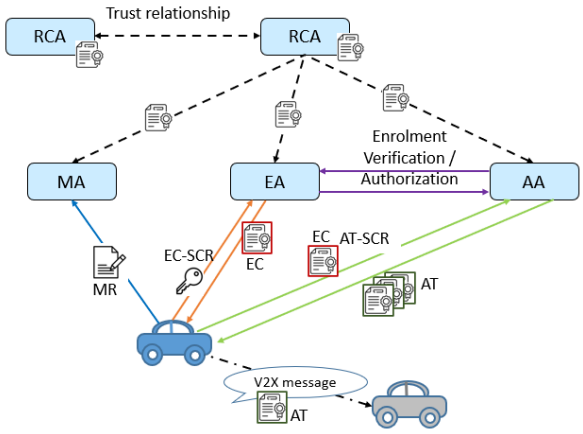


Figure 1.4: ETSI ITS PKI Architecture (reproduced from Fig.11a in ETSI TS 102 940)

that acts as the point of entry to the PKI system for end entities. Depending on the type of incoming request from end entities, the RA routes the request to the appropriate system entity that handles this request. For example, if a vehicle enrolls itself with the PKI system, the RA routes this request to the Enrolment CA that handles this request and executes the enrolment procedure.

Further, the IEEE 1609.2 PKI system supports a feature to obscure requesting end entities from the rest of the PKI system. This is for the purpose of protecting vehicle owners to prevent leakage of privacy information in the case that the identity would be compromised by either internal or external adversaries. The Location Obscurer Proxy mixes requests from multiple vehicles before forwarding them to the RA. This way, PKI entities from the RA onward are not able to identify the requesting vehicle. Furthermore, this standard defines two Linkage Authorities (LA1 and LA2) in the system and advises to keep them under separate organizational entities. In other words, in order to trace a specific vehicle (or vehicle owner), it requires both LAs to collaborate. This arrangement requires that both LAs need to be compromised by adversaries to identify vehicles and subsequently owners' privacy-related information, thus raising the bar for both internal and external adversaries to compromise the system.

The above functionalities are not defined in the ETSI ITS architecture, as can be observed from Fig. 1.4. We believe this is a conscious design decision by the ETSI ITS standard committee.

1.2 Properties of Vehicular Communication

1.2.1 Privacy Properties

One of the key properties of vehicular communication defined by the standards discussed in Sec. 1.1 is the protection of user privacy. In other words, these standards aim to prevent compromise of personal data of vehicle owners through the use of this technology. The first definitions for privacy protection have been given by Pfitzmann and Hansen [66]. The introduction of General Data Protection Regulation (GDPR) in Europe in 2016 has led to clear definitions of anonymity and pseudonymity [63, 39, 40]. According to these definitions, the key elements of privacy protection include the following elements:

1. Anonymity
2. Pseudonymity
3. Unlinkability
4. Undetectability
5. Unobservability

Anonymity is *"process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party"* [50, 63]. Pseudonymity is *"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"* [63]. It should be noted that there is a significant difference between anonymity and pseudonymity [6]. The former is disassociated from specific individuals; thus anonymised data cannot identify an individual. On the other hand, the latter can potentially be traced to an individual through the use of *additional information*; therefore, pseudonymous data is still personal data [6]. There are multiple approaches to pseudonymisation; however, there is no single solution that can be universally applied in all possible scenarios [39].

Unlinkability means that attackers *"cannot sufficiently distinguish whether these Item of Interests (IOIs) are related or not"* within IOIs, e.g. messages, actions. Undetectability of an IOI means that attackers *"cannot sufficiently distinguish whether it exists or not."* Unobservability of an IOI means: (1) *"undetectability*

of the IOI against all subjects uninvolved in it", and (2) *"anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI"* [66].

To protect personal data, the standards specify the vehicles shall use pseudonyms and periodically change them. The use of pseudonyms rather than real identities makes it harder to track vehicles. Each pseudonym certificate contains a unique public key, and using it under a unique pseudonym ensures that public keys and pseudonyms remain unlinkable. In addition, vehicles change their MAC addresses and IPv6 addresses (when IP communication is used) at the same time of pseudonym change. Changing these identities and addresses in a privacy-preserving manner prevents tracking of pseudonym changes.

Based on these definitions in [66] and applying them in the vehicular communication context, observers of messages cannot: (1) correlate which vehicle a given pseudonym belongs to, (2) correlate if two or more pseudonyms belong to the same vehicle or not, (3) identify from which vehicle a given message originated from.

1.3 Research Questions

As discussed in Sec. 1.1, the IEEE 802.11, IEEE 1609, SAE J2735, and ETSI ITS standards specify how communication between vehicles is accomplished to achieve road safety while preserving the privacy of vehicle owners. Specifically, IEEE 1609.2 [79], 1609.2.1 [49], and ETSI TS 102 940 [27] define a certificate management system, or a PKI system. However, upon close examination of these specifications, we realized that there are a number of gaps and issues in these specifications. In this respect, we raise the following research questions:

1. Are the existing standards, specifically regarding the certificate management system based on the PKI paradigm, sufficient to realize the overall objective of improving road safety and preserve users' privacy?
2. Are there areas where these standards may cause negative impacts on the intended road safety?
3. What are the key gaps and issues in these standards? For these gaps and issues, what are possible solutions to address them?
4. Are there further enhancements to supplement the existing functionalities in the standards? If so, what are they and how can they improve the security and privacy of vehicular communication?

1.4 Contributions

As the result of our detailed analysis of the security and privacy aspects of the aforementioned standards, we present three main perspectives.

1.4.1 Identifying Gaps in Security and Privacy Aspects

First, in Chapter 2, we discuss and summarize our observations from our close analysis of security related specifications, namely, the IEEE 1609.2 [79], the IEEE 1609.2.1 [49], and the ETSI ITS specifications that define a PKI solution such as TS 102 940 [27], TS 102 941 [32], EN 302 737-2 [28] (CAM), EN 302 637-3 [29] (DENM), TS 103 097 [33]. We present the key observations and highlights from our paper [90].

1.4.2 Proposing Security-Enhancing Scheme

In Chapter 3, we present our contributions to enhance the security aspects of vehicular communication. This part consists of four published papers. The first paper deals with optimizing the traffic in the communication channel to resolve unknown certificates [87]. The second paper describes the gap in the ETSI ITS standard on resolving misbehaviour reportings by vehicles [86] – the ETSI ITS architecture [27] does not take the cross-border scenario into account. Due to this reason, vehicles crossing country borders face a situation where anomalies and misbehaviour reporting in vehicular communication cannot be resolved due to the absence of cross-border PKI communication. The third paper identifies issues associated with a candidate scheme to distribute pseudonym certificates called Issue First Activate Later (IFAL) [88]. The last paper highlights the absence of forward-looking capabilities such as future adoption of Post-Quantum Cryptography in digital certificates in both IEEE 1609.2 and ETSI ITS PKI systems [89]. Specifically, both of these standards do not take the need for future migration toward a post-quantum certificate format into account. Furthermore, future migration to Post-Quantum Cryptography will likely cause significant issues to the operation of vehicular communication and may make it challenging to deploy.

1.4.3 Proposing Privacy-Enhancing Scheme

In Chapter 4, we present our scheme to enhance the privacy protection of vehicular communication [91]. Specifically, the Cooperative Awareness Message

(CAM) in the ETSI ITS standard [28] and the SAE J2735 Basic Safety Message (BSM) [76] disseminate vehicle information to surrounding vehicles so that all vehicles in the vicinity establish and maintain dynamic maps of the presence, positions, and movements of other vehicles. However, this message dissemination does not take vehicle presence into consideration. In other words, vehicles transmit these messages irrespective of whether there are other vehicles within the vicinity or not. If vehicles transmit these messages even when there are no other vehicles, doing so does not achieve road safety, but only leads to exposing information for possible eavesdroppers. This point is notable given that CAM and BSM messages are broadcast-based, thus these messages are sent in clear without confidentiality protection. Because both the MAC message header and its payload content are visible, potential exposure of privacy-related information that are derived from both the message header and the payload are equally at risk. For example, a vehicle's pseudonym (i.e. station ID) is carried in the CAM message header which is contained in the MAC frame payload. This value in clear allows persistent eavesdroppers to identify messages and to track vehicles across pseudonym changes. To address this point, our enhanced scheme takes the presence of other vehicles into consideration upon transmitting CAM or BSM messages.

Chapter 2

Gaps in Standards on Security and Privacy Aspects

Content in this section corresponds to the following paper in Part II:

- Yoshizawa, T., Singelée, D., Mühlberg, J. T., Delbruel, S., Taherkordi, A., Hughes, D., and Preneel, B. A Survey of Security and Privacy Issues in V2X Communication Systems. ACM Computing Surveys (CSUR), Vol. 55, No. 9, pp. 1–36, 2023.
  – See p. 79
- Yoshizawa, T., and Preneel, B. Survey of Security Aspect of V2X Standards and Related Issues. In 2019 IEEE Conference on Standards for Communications and Networking (CSCN), IEEE, pp. 1–5, 2019.
  – See p. 147

2.1 Introduction

At the start of our research, we analyzed the relevant standards and related documents to understand the overall scope and to which extent standards specify how vehicular communication will be realized. Some of the most notable

standards and specifications related to vehicular communication are listed below.[1]

- IEEE standards:
  - IEEE 802.11p (Wireless LAN, MAC and Phy, Wireless Access in Vehicular Environments (WAVE)) [78]
  - IEEE 1609.2 (WAVE Security Architecture) [79]
  - IEEE 1609.2a1 (WAVE Security Architecture, Amendment 1) [80]
  - IEEE 1609.2.1 (WAVE Security Architecture from End Entities' Perspective) [49]
- SAE standards:
  - SAE J2735 (Dedicated Short-Range Communications (DSRC) Communication Message Set Dictionary) [69, 70, 76]
  - SAE J21434 (Road Vehicles Cycbersecurity Engineering) [51]
  - SAE J29451 (System Requirements for V2V Communication) [74]
  - SAE J29452 (DSRC Performance Requirements for V2V Communication) [72]
  - SAE J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems) [71]
- ETSI ITS standards:
  - ETSI ITS TS 102 940 (ETSI ITS Security Architecture) [27]
  - ETSI ITS TS 102 941 (ETSI ITS Security Procedures) [32]
  - ETSI ITS TS 103 097 (ETSI ITS Certificate Definition) [33]
  - ETSI ITS EN 302 637-2 (ETSI ITS Cooperative Awareness Messages (CAM)) [28]
  - ETSI ITS EN 302 637-3 (ETSI ITS De-centralized Enrivonmental Notification Messages (DENM) [29]
  - ETSI ITS TR 103 415 (Pre-Standardization Study on Pseudonym Change Management) [25]
- IETF standards:

[1] This list represents the most notable and thus important set of specifications from a security and privacy perspective. Thus it is not an exhaustive list of all standard specifications related to vehicular communication.

  - IP Wireless Access in Vehicular Environment (IPWAVE) use cases [53]
  - Transmission of IPv6 Packets over 802.11p WAVE [65]

- 3GPP standards:
  - LTE-based Cellular-V2X (C-V2X) [2, 3]
  - 5G-based C-V2X [4, 5]
  - Security aspects of C-V2X [1]

2.2 Analysis and Issue Categorization

2.2.1 Overview

We first captured the overall landscape of relevant standards and their relations in our paper [85]. This paper clarifies the two competing radio access technologies, namely WAVE based on IEEE 802.11 technology and C-V2X based on cellular mobile technology, and their similarities and differences from a security perspective.

As the next step, we analyzed these standards in detail from both security and privacy perspectives. As a result, we have identified a number of issues and gaps in these standards. The culminating result of our findings resulted in our journal paper [90]. We grouped these issues into five categories as shown in Table 2.1. For the rest of this section, we present a high level overview of these categories and associated issues.

2.2.2 Privacy Protection

The first category is privacy protection (Sec. 6 in [90]). As described in Sec. 1, vehicular communication involves the use of digital certificates that are issued by the PKI system for V2X security management. Messages that vehicles transmit contain digital certificates. To protect vehicle owners' privacy, standards specify that vehicles need to use pseudonyms and associated pseudonym certificates to hide the identities of vehicles, and periodically change them in such a way that these pseudonyms remain unlinkable from others used by the same vehicle or other vehicles.

The rest of this section describes the areas related to privacy protection that are not specified in the standards.

Table 2.1: Issue Categorization

Category	Sec. No.	Issue
Privacy protection (Sec.6)	Sec. 6.1	Privacy and vehicle operation
	Sec. 6.2	Applicability of privacy 1: vehicle types and usages
	Sec. 6.3	Applicability of privacy 2: non-vehicle ITS-S
	Sec. 6.4	Privacy and cooperative awareness
	Sec. 6.5	Privacy vs. road safety
	Sec. 6.6	Privacy and use of unicast
Certificate-based message verification (Sec.7)	Sec. 7.1	Certificate-based message verification
	Sec. 7.2	Certificate usage and change policy
	Sec. 7.3	Certificate reloading
	Sec. 7.4	Certificate revocation
	Sec. 7.5	Certificate management of RSUs
	Sec. 7.6	Certificate management of VRUs
	Sec. 7.7	Certificate usage in multiple communications
Communication modes (Sec.8)	Sec. 8.1	Broadcast-oriented communication
	Sec. 8.2	Unicast - confidentiality protection
Message handling (Sec.9)	Sec. 9.1	Plausibility validation and misbehavior detection
	Sec. 9.2	Communication involving VRUs
System level (Sec.10)	Sec. 10.1	ITS-S device-dependent trust level
	Sec. 10.2	Interconnection between multiple security mgmt. systems
	Sec. 10.3	Multiple security mgmt. systems for different ITS-S types
	Sec. 10.4	Absence of consideration on PQC technologies

Note: The section numbers in this table refer to our paper [90].

Privacy and vehicle operation

Sharing certificates implicitly requires that vehicles, benign or not, are expected to internally store certificates of other vehicles they encounter on the road for a certain period of time. Vehicles refer to these stored certificates as needed given that not all received messages contain a full certificate. Therefore, privacy protection implicitly includes protection against benign vehicles as well as malicious ones. This raises the question how long vehicles are required to retain these received certificates from other vehicles when they are no longer used (e.g. vehicles move away from the communication range).

Applicability of privacy 1, vehicle types and usages

Given that privacy protection is intended to protect vehicle owners, not all vehicles on the road are subject to the same level of protection. In other words, privately-owned vehicles may require a different level of protection compared to vehicles owned by public entities and businesses such as public transportation, police cars, trucks, and taxis. Therefore, a different level of privacy protection may need to be defined in the standards. Another related aspect is the change of vehicle ownership and necessary handling of privacy-related information in vehicles upon transfer of ownership.

Applicability of privacy 2, non-vehicle ITS-S

End entities, or ITS Stations (ITS-S) consists of multiple types, the most prominent ones being vehicles. Other types include Road Side Units (RSU) such as dedicated devices on the road side or devices embedded in the existing road infrastructure such as traffic lights. RSUs have no associated human user; they are likely owned and deployed by national or regional government entities. Therefore, strictly speaking, RSUs do not require privacy protection; they do not require pseudonym certificates. Even if they are assigned with them, RSUs do not need to change them as frequently as vehicles do. On the other hand, other ITS-S types include other road users such as pedestrians, cyclists, motorcycles, mopeds, electric scooters, and animals. They are collectively called Vulnerable Road Users (VRU) because they tend to be more severely injured than vehicle drivers and passengers when an accident occurs. One characteristic of VRUs is that they are even more closely associated with specific individuals than vehicles. In this sense, VRUs likely need even higher level of privacy protection than vehicles. As a conclusion, different ITS-S types likely require different level of privacy protection.

Privacy and cooperative awareness

CAM messages are periodically broadcast within the communication range of the transmitting vehicle. This helps establish and maintain *situational awareness* of surroundings to help achieve safe maneuvering. Standards require vehicles to change pseudonyms periodically for privacy protection purposes. However, doing so does not necessarily offer *unlinkability*. A simple example is a situation where there are only two vehicles on the road within communication distance of each other. In this case, if one vehicle changes its pseudonym, it is trivial for the other vehicle to link pseudonyms *before* and *after* the change. In this sense, simply changing pseudonyms is a naive approach that is insufficient for some settings.

Several papers propose solutions to this problem, such as mix zones [9], silent periods [46], and dynamic transmission power adjustment [8]. However, all of these solutions introduce undesirable side effects that lead to new issues. Another approach is to enforce a strict one-time use of pseudonym. However, it still does not guarantee unlinkability if a series of changes is observed and a large-scale correlation is performed. Thus, no clear countermeasure exists to guarantee the privacy protection through periodic pseudonym changes.

Privacy vs. road safety

There exists a fundamental conflict between privacy protection and road safety. The purpose of using pseudonym certificates and periodically changing them is to make the correlation between the owner of these certificates and actual vehicle impossible for observers and other surrounding vehicles. However, its intended inability to correlate the message source and the actual vehicle may cause a dangerous situation on the road and thus result in decreased road safety.

A simple example is a situation where a vehicle suddenly brakes in crowded traffic (i.e. Emergency Electronic Brake Light (EEBL) event in De-centralized Environmental Notification Message (DENM) in ETSI ITS terminology). In this case, a vehicle right behind it also needs to brake immediately in order to avoid an imminent collision. If this receiving vehicle is not able to identify which vehicle has braked, it follows that this vehicle cannot determine if it should brake itself or not. Similarly, if another vehicle, that is not in immediate danger due to this braking event, decides to brake, doing so will be perceived by its trailing vehicles that it has braked for no reason at all, which leads to an even more dangerous condition. In other words, protecting vehicle owners' privacy (e.g. driver's names, place of residence and work) may significantly compromise the road safety. In summary, the intended property of privacy protection to

prevent identifying the source vehicle of a specific event can actually hinder achieving road safety and results in an opposite effect.

Privacy and use of unicast

Examples of unicast communication include use cases such as remote driving [38, 64] and platooning [55]. The use of unicast and the need for periodic pseudonym certificate changes for privacy protection are at odds with each other as unicast communication is identified by a unique pair of identities, such as IP address, MAC address, and pseudonym certificate. Pseudonym changes require changing all of them at the same time.

This change of identities will require coordination between the two endpoints of the unicast communication to avoid disruption of the ongoing communication. This coordination violates the *unlinkability*, *undetectability* and *unobservability* properties the privacy protection aims to achieve. It follows that privacy protection cannot be applied in unicast communication. Once the unicast communication is completed, each endpoint should change its pseudonym and other identities (e.g. MAC address) to avoid tracking by the previous unicast peers. This situation also implies that confidentiality protection (i.e. encryption) needs to be applied in all unicast communications in order to prevent eavesdroppers from intercepting this identity change coordination. In this sense, unicast communication needs protection against both internal and external threats.

2.2.3 Certificate-Based Message Verification

The second category is the certificate-based security solution (Sec. 7 in [90]). Similar to the previous section, the rest of this section describes areas that are not specified in the standards.

Certificate-based message verification

The fundamental nature of achieving road safety within the context of moving vehicles requires real-time communication in which messages need to be processed and acted upon in the order of 10s of milliseconds or less. Due to the certificate-based message authentication and verification, the real-time processing of received messages requires immediate availability of these certificates in the receiving vehicles. However, it is not necessarily the case under all circumstances. Periodic messages such as CAM contain the certificate

in the message only once per second. The remaining messages within the 1 second interval contain certificate *digest* which is the 8 least-significant digits of the hash output of the certificate ($digest \leftarrow LSB8(Hash(cert))$).

If a vehicle receives a CAM message containing a certificate *digest* but does not internally hold the corresponding full certificate, then this vehicle needs to resolve this *unknown digest* by sending a query to surrounding vehicles using the *Peer-to-Peer Certificate Distribution (P2PCD)* mechanism. This query and response will likely take 100s of milliseconds assuming that there is at least one vehicle that can respond to this query. If no vehicle responds to this query, then this requesting vehicle needs to wait for the next CAM message from this transmitting vehicle that contains the full certificate. In this case, the worst case waiting time for this certificate can be as long as 1 full second.

The same situation applies if the receiving vehicle does not have the complete certificate chain from a pseudonym certificate to the RCA certificate because not all messages contain the complete chain of certificates up to the RCA. Without this information, the receiving vehicle cannot verify the authenticity of the transmitting vehicle. In this case, the receiving vehicle needs to resolve the missing certificates through the use of this P2PCD mechanism.

Certificate usage and change policy

Standards do not specify the exact algorithm of pseudonym change and how many pseudonym certificates are issued to vehicles in a given time interval. As it is not scalable to enforce a strict one-time-only certificate rule, a sensible assumption is that vehicles will reuse a finite set of certificates in a specific period, e.g. 20 simultaneously valid certificates per week. This implies that the exact pseudonym change algorithm is left up to implementations in the certificate management system and by the vehicle manufacturers. The consequence is that some implementations may be more effective than others from a privacy perspective by applying schemes to make linkability more difficult. This variation in effectiveness will likely lead to vulnerabilities and weaknesses in certain systems or makes of vehicles.

Certificate reloading

Another unspecified area in standards is the reloading of pseudonym certificates in vehicles. There are also variations in terms of for how long and how many pseudonym certificates are preloaded to vehicles up front. There are variations in schemes, such as 3 years [11], 5 years [82], and no definitive definition [26].

Combined with the variation of pseudonym change algorithms discussed in the above point, it will impact the storage capacity requirement in vehicles.

Under any circumstance, running out of usable pseudonym certificates needs to be avoided. In this sense, reliable mechanisms need to be in place to reload pseudonym certificates whenever and wherever it is necessary. Some solutions discuss the use of RSUs as a point of contact for vehicles to reload pseudonym certificates [68]. However, ubiquitous installation and availability of RSUs is only an assumption. It will be most likely dependent on areas with slow deployment over many years given that they are installed and deployed by government entities that require appropriate budget allocations by national or local governments. Deployment of RSUs will most likely follow different market dynamics from that of automobiles. This problem is somewhat akin to the installation and availability of charging stations for electric vehicles. Standards do not have clear answer to this problem, most likely leaving it as an implementation-dependent matter. Varying level of vehicle's storage capacity from various makes and models will also limit practical solutions.

Certificate revocation

Certificate revocation is one of the unresolved issues in PKI systems [43]. It works in theory but not in practice. Within the context of Internet web browsing, IETF has standardized a series of solutions from CRL [58] to OCSP [60] to OCSP stapling [19] to OCSP must staple [44]. Despite their effort, each of these solution comes with its own issues. Thus, a universal solution that resolves all problems does not yet exist.

One key observation regarding revocation in the vehicular communication context is that the target of revocation is vehicles, not individual certificates. The reason is that vehicles hold multiple simultaneously active pseudonym certificates for privacy protection purpose. Therefore, upon positive misbehavior detection, all current and future pseudonym certificates of this vehicle need to be invalidated. SCMS [11] that became the base of IEEE 1609.2 [79] provides a mechanism called *linkage value* to link an individual pseudonym certificate to all pseudonym certificates assigned to the vehicle. This mechanism addresses revoking multiple certificates in a scalable manner. However, the issue related to scalable distribution of the CRL to all vehicles remains open. This is a significant departure from conventional computer networks such as revoking certificates from HTTP web servers where a certificate and the web server are in a 1-to-1 relationship.

There are two types of revocation: *active* and *passive*. *Active* revocation is the traditional CRL-based approach. *Passive* revocation takes advantage of

the pseudonym certificate reloading mechanism. When a vehicle requests a certificate reload, the PKI system rejects this request if the system indicates that this vehicle is revoked. Once this vehicle runs out of valid certificates, it can no longer generate valid signatures, thus is no longer able to send valid messages in the communication channel.

SCMS [11] supports CRL-based *active* revocation as well as *passive* revocation. However, SCMS does not offer any consideration to the existing issues associated with the CRL-based approach, including its scalability issue [43]. This is a major issue given that target entities are moving vehicles. It is a significant challenge to guarantee that all vehicles under a single PKI system receive the latest CRL in a timely and scalable manner. IETF has not solved the revocation issue for the general Internet browser context as mentioned in the beginning of this section; the hurdle is even higher for moving vehicles. Contrary to this situation, ETSI ITS [26] supports only *passive* revocation.

Another issue of CRL-based revocation is the time gap between when a vehicle is revoked and when it is evicted from the communication channel. Even after the PKI system declares a vehicle is revoked, this vehicle can and will continue to transmit messages in the communication channel as long as it has valid certificates. Until such time that a revoked vehicle runs out valid certificates, receiving vehicles are responsible for detecting the revocation status of all transmitting vehicles and for rejecting messages from revoked ones. Ideally, a revocation event should immediately block the vehicle from transmitting. However, this requires a different approach than CRLs.

Yet another issue of CRL-based revocation is that a proportion of its content may be irrelevant to vehicles if they never encounter revoked vehicles listed in the CRL. Optimizing this aspect is a large open question as it involves identifying or predicting vehicles' movement in order to optimize the CRL content tailored to specific vehicles. In our paper [90], we call it CRL *relevance*. The number of CRL entries may become large depending on the number of vehicles or certificates to be revoked. However, if a vehicle never encounters any of the indicated vehicles (or certificates assigned to vehicles), that entry in the CRL is not *relevant* to that vehicle, while it occupies storage space in the vehicle.

So far, we have mainly discussed issues associated with *active* revocation. However, *passive* revocation also has issues. Because this scheme is triggered by the certificate reloading mechanism, a longer preloading period (e.g. 3 years worth of certificates to be preloaded at the time of enrolment to the certificate management system) implies that this vehicle will not trigger a reloading request to the system until the end of this preloading period. If this vehicle is revoked well before the existing certificate pool depletes, the time gap discussed for the

active revocation also applies.

Certificate management of RSUs

The pseudonym certificate management is defined in the standards from a vehicle-centric perspective only. It is evident by studying the system architecture of the certificate management system in IEEE 1609.2 [79] and ETSI TS 102 940 [27] and their description. However, as discussed under *privacy protection* category earlier in Sec. 2.2.2, the required level of privacy protection in RSUs is likely lower given that they are not associated with any particular individual. On the contrary, some use cases involving RSUs may require vehicles to uniquely identify an RSU. In this sense, RSUs may require longer certificate validity period than vehicles.

Certificate management of VRUs

Relatively recently (2019 $\sim$ 2021), ETSI ITS has issued a new set of specifications for VRUs. These specifications define relevant use cases, a functional architecture, and message services specific to VRUs. However, they do not cover security aspects equivalent to vehicles. Specifically, these specifications do not cover enrolment and issuance of certificates to VRUs.

The certificate management functions related to VRUs strongly differ from those for vehicles due to several reasons. First, VRUs use standalone commercial devices such as smartphones. Smartphones are generic consumer products that exist independent of vehicular communication or ITS systems. This is in contrast to vehicle OBUs that are embedded in vehicles and are built exclusively for vehicular communication. Second, the coupling between a smartphone and a human user is tighter than that of vehicles. In this respect, privacy protection for VRUs needs to be even more stringent than for vehicles. In other words, a privacy breach of smartphones can readily lead to a compromise of its user's privacy.

In the VRU context, this fundamental difference implies that an appropriate mechanism needs to be in place to verify and admit legitimate smartphones to the vehicular communication systems. Similarly, pseudonym certificates need to be issued and delivered to legitimate smartphones so that their users can benefit from the additional safety protection that ITS services provide. Furthermore, misbehavior detection and investigation, and subsequent revocation of certificates need to be in place for smartphones. This last point is significant given that consumer products such as smartphones built on

an open-source platform, such as Android OS, can be more vulnerable from a cybersecurity perspective as consumer products are readily accessible to adversaries to modify in order to cause negative consequences to vehicular communications. ETSI ITS and IEEE 1609 need to address these points.

Certificate usage in multiple communications

According to the GeoNetworking-related ETSI ITS specifications, multicast communications, similar to broadcast communications, do not support confidentiality protection (i.e. encryption) of user data. On the other hand, unicast communication can take advantage of confidentiality protection. In this sense, the separation of pseudonym certificates in different communication modes (broadcast, multicast, and unicast) would make sense. This implies that multiple pseudonym certificate pools need to be configured in vehicles for different communication modes. Therefore, a single pool, as described in the standards, is not sufficient.

2.2.4 Communication Modes

The third category is the communication modes and their impacts on security (Sec. 8 in [90]). This section describes areas that needs appropriate improvement in the standards.

Broadcast-oriented communication

As discussed in the previous section, broadcast and multicast communications do not apply confidentiality protection. Specifically in broadcast, messages are sent to an unknown and undefined group of entities within the sender's communication range. Through applying the periodic pseudonym certificate change, tracking specific vehicles is not trivial in vehicular communication. However, due to the absence of confidentiality protection, all broadcast messages are sent in clear, allowing passive observers, legitimate or not, to detect the use of a specific pseudonym by simply observing messages in the channel. Thus, broadcast communication offers no protection against persistent observers. If this observation is carried out on a wider scale, such as city-wide observation by collecting data observed in a wide area, tracking vehicles become possible, leading to the breach of privacy for vehicle owners.

Unicast – confidentiality protection

Unlike broadcast and multicast, unicast communication offers confidentiality protection. However, its usage is limited to specific use cases in vehicular communication, e.g. remote driving and platooning. Therefore, the use of unicast is an exception in vehicular communication contrary to general internet traffic. Unicast communication is likely an IP-based purpose-specific service that requires TCP and TLS session estabishment. Furthermore, due to the nature of moving vehicles, the lifetime of unicast communication may be limited when both end points are moving. In some scenarios, the session duration may be quite short. In such cases, the session establishment overhead becomes more pronounced, leading to a less efficient overall channel usage.

2.2.5 Message Handling

The fourth category is security-related message handling that impacts the overall road safety (Sec. 9 in [90]).

Plausibility validation and misbehavior detection

In vehicular communication, as a type of cyber-physical systems, the concept of plausibility validation is intuitively clear. It is vital in vehicular communication to prevent accidents that are triggered by accepting incorrect information in malicious messages as real. Similarly, incorrect or inaccurate information sent by vehicles containing a malfunctioning sensor needs to be detected and ignored. Furthermore, the presence of a misbehavior is a decision based on the cumulative failure of plausible validation events. This implies that a misbehavior detection is not a single observation of a plausible validation event, but constitutes a minimum level of confidence by observing multiple such failure events.

The vehicular PKI system needs to promptly address these misbehaving vehicles by revoking their certificates and by evicting them from the communication channel. However, ensuring such validation and detection is a challenging task. The existing standards only discuss the necessity of such functionalities without specifying how they can be realized. This current state of these standards will most likely result in implementation-dependent solutions. This situation means that the effectiveness of individual solutions or implementations will vary in reality – an undesirable situation from a road safety perspective.

Communication involving VRUs

As discussed in Sec. 2.2.2, VRUs refers to road users who tend to be more severely injured than vehicle drivers and passengers when an accident occurs. Examples include pedestrians and cyclists. The objective of including such road users into vehicular communication is to further enhance road safety by warning for dangerous situations on the road involving more vulnerable road users. Since 2019, ETSI ITS has issued three specifications on VRUs – TS 103 300-1 [31] (uses cases), TS 103 300-2 [34] (functional architecture), and TS 103 300-3 [36] (VRU Awareness Message (VAM)). However, despite its intent, a careful reading of these specifications reveals that they are more of an exploratory work rather than implementable specifications. The prime example is the discussion in Annex G of the VAM specification [36]. This Annex describes the general difficulties associated with VRUs, such as their transition of state – from a cyclist to a pedestrian when a person steps off of a bicycle, or from a pedestrian to non-pedestrian when she steps on a bus. In addition, pedestrians' inertia is significantly lower than that of vehicles, and they have a tendency to ignore traffic rules and signals more frequently than vehicles. These fundamental characteristics of pedestrians often makes it more difficult to accurately predict their movements. This way, detection and prediction of VRUs' movement will continue to be a challenge to make VAM messaging an effective tool to achieve road safety. In addition, we assume that VRUs, such as pedestrians, use their existing device (i.e. smartphones). In this context, how to incorporate consumer devices into the ITS system is an open issue.

2.2.6 System Level

The last category are PKI system-level issues when applied to vehicular communication (Sec. 10 in [90]).

ITS-S device-dependent trust level

Vehicular communication involves multiple entity types. Vehicles are the most prominent ones. Other types include Road Side Units (RSUs) that are owned and managed by government authorities, such as police or highway traffic authority. Therefore, RSUs can be viewed as more trusted entities and assigned functionalities that provide authoritative information. One example is to collect misbehaviour-related information from vehicles and conduct initial information processing to supplement investigation by a Misbehaviour Authority (MA) which determines the final conclusion of the misbehaviour investigation.

Interconnection between multiple security management systems

IEEE 1609.2 [79] and ETSI ITS TS 102 940 [27] define the PKI system and interactions among system entities, describing the overall functionalities of the system. On the other hand, roads in Europe are shared by vehicles from multiple countries. Given that vehicles need to communicate with one another irrespective of their origin, PKI systems from different countries also need to interact to coordinate the necessary management functionalities. However, these standards discuss functionalities within a single PKI system only, and do not address interaction among multiple PKI systems. Such interactions are necessary to conduct and resolve system-level issues such as misbehaviour detection and revocation involving vehicles from different countries. Another example is dissemination of CRLs to revoke vehicles across country borders; as active revocation using CRL is defined in IEEE 1609.2 only, this scenario is relevant to the US system only.

Multiple security management systems for different ITS-S types

Vehicles, RSUs, and VRU devices (i.e. smartphones) are owned, used, and managed by distinctively different entities. The majority of vehicles are privately owned; RSUs are owned by government entities; and smartphones are owned by consumers. In this respect, PKI systems that issue pseudonym certificates to these devices have their unique characteristics. For example, admitting smartphones into the ITS system (i.e. vehicular communication) may require verification of a valid user subscription with mobile operators that provide service to the end users. Doing so prevents illegitimate devices used by adversaries from injecting fake messages with malicious intent to cause chaos on the road. The existing standards cover the management of the first type only (i.e. vehicles), leaving the type-specific management details of the other devices types as an open issue.

Absence of consideration on post-quantum cryptography

Advancement of quantum computers in the past years raises concerns to the security of currently-used cryptographic primitives. One of the most well-known "threats" is Shor's algorithm [77] that shows that quantum computers can factor large integers and solve discrete logarithms in polynomial time [56]. This implies that the existing primitives such as RSA and Elliptic Curve Cryptography (ECC) will be vulnerable when the sufficiently powerful quantum computer become available. At the time of this writing (2023), the most advanced quantum computer has a capacity of 433 physical qubits [47].

There are different opinions when this situation becomes an imminent threat in reality. A report by NIST in 2016 states that "it is likely that a quantum computer capable of breaking 2000-bit RSA in a matter of hours could be built by 2030" [14]. Another paper in 2004 indicates that a 160-bit elliptic curve cryptographic key "could be broken on a quantum computer using around 1000 [logical] qubits while factoring the security-wise equivalent 1024-bit RSA modulus would require about 2000 [logical] qubit" [67]. On the other hand, a whitepaper in 2021 suggests that running Shor's algorithm will require millions of physical qubits, and it is still 25 to 30 years away before quantum computers reach that capacity [57].

Based on their analysis of this threat [14], NIST has started the selection process of Post-Quantum Cryptography (PQC) algorithms in 2016 [7], and have announced standardization of three quantum-resistant algorithms in 2022 [61]. Although we acknowledge that both IEEE 1609 and ETSI ITS standards started earlier than NIST to start its work on PQC standardization, it is important to note that vehicular communication standards have no answer to the emergence of quantum computer and the need to incorporate PQC algorithms. This point is acknowledged in ETSI's recent report issued in May 2023 [35]. This report analyzes the impacts on the existing ETSI ITS standard and concludes that none of the three standardized post-quantum signature algorithms are suitable for vehicular communication due to the long signature and public key size. To supplement this point, one of our papers [89] points out several major issues that will make vehicular communication non-usable after migration toward PQC-ready digital certificates.

2.3 Root Cause Analysis

The issues we discussed in the previous sections are captured in Table 2.1; they are grouped into multiple root causes. The list of our categorization is shown in Table 2.2. This list shows one way to characterize and categorize issues to specific root causes as there is likely not an absolutely correct way to do so. In some cases, an issue originates from multiple root causes. For a detailed discussion, we refer to our paper [90]. For the rest of this section, we briefly describe the nature of these root causes.

2.3.1 Conflicting or Insufficient Specification

The existing standards either include conflicting requirements or do not sufficiently define all the necessary functionalities. Privacy protection and

Table 2.2: Root Causes

Root cause
Conflicting or insufficient specification
Characteristics of vehicular communication environment
Broadcast-based communication
Implementation-dependent ambiguity
Certificate usage and management for vehicles
Certificate management of non-vehicle ITS-S types
RSU infrastructure dependency
Mobile operator involvement and dependency

road safety are fundamentally at odds with each other – if one is supported, then the other is compromised. This is indeed the case when the anonymity property requires unobservability of a transmitting vehicle, resulting in receiving vehicles to be unable to determine an appropriate reaction. An example of insufficient specification includes absence of interaction between different PKI systems across country borders for misbehavior reporting and investigation.

2.3.2 Characteristics of Vehicular Communication Environment

Moving vehicles means constant change of the communication topology. The set of vehicles within a given vehicle's communication range changes depending on the relative moving speed and direction. Combined with short-range direct communication among vehicles, such communication environment will likely limit the type of services.

2.3.3 Broadcast-Based Communication

Due to the dynamic topology change discussed above, basic services are necessarily limited to broadcast-based services. CAM, DENM, and BSM messages are the prime examples of these basic services to improve road safety. Broadcast-based communication necessarily implies that it is an *open* communication given that no confidentiality protection is applied to messages, thus any entity with receiving capability can receive them including adversaries with malicious intent. How to protect this *open* communication remains a challenge.

2.3.4 Implementation-Dependent Ambiguity

Existing standards leave many areas open in terms of how to realize specified functionalities. Some examples include effective plausible validation, misbehaviour detection and subsequent investigation. The absence of a specific solution implies that it is left up to individual vehicle manufacturers or certificate management system to determine the implementation details. This situation will most likely lead to non-uniform effectiveness of solutions from one vehicle manufacture to another or one PKI system to another. In this sense, a set of common guideline or criteria needs to be defined to guarantee minimum functionalities to gain consumers' confidence.

2.3.5 Certificate Usage and Management for Vehicles

The actual usage of pseudonym certificates is not defined in the existing standards. This includes aspects such as usage period, change criteria, and reloading mechanism and criteria. ETSI ITS has a pre-standard report on pseudonym change schemes [25]. However, it stays at the level of itemizing and comparing key characteristics of proposed solutions.

2.3.6 Certificate Management of Non-Vehicle ITS-S Types

Beside vehicles, end entities in vehicular communication include RSUs and VRUs. Existing standards do not specify if or how these entities are managed by the PKI. One example is the use of pseudonyms in RSUs and if they require frequent pseudonym changes similar to vehicles. Another example is how VRUs (e.g. pedestrians' smartphones) are admitted as legitimate members of vehicular communication system, and how they are revoked, if and when necessary.

2.3.7 RSU Infrastructure Dependency

The deployment of RSUs has a different market dynamic from that of vehicles. RSUs are owned and managed by government entities that require budget allocation by national or local governments. Therefore, the deployment of RSUs are likely to occur over many years and coverage will remain spotty. In other words, ubiquitous presence of RSUs cannot be assumed when designing solutions for services. In this sense, service capabilities involving RSUs should include smooth transition and migration toward more RSU-dependent solution.

2.3.8 Mobile Operator Involvement and Dependency

Vehicular communication involves connection to the PKI system which requires wide-area wireless communication such as cellular systems. As this requires some level of service guarantee, how the expected services are fulfilled by using cellular systems needs to be clarified. This area may be deployment-dependent, and thus outside the scope of standardization. However, as a service user of cellular connectivity, vehicular communication is dependent on it in many use cases. Thus not specifying this area can lead to ineffective service in reality. In addition, whether or how mobile operators are involved in the admission of VRUs (e.g. pedestrians' smartphones) in vehicular communication is an open area.

Chapter 3

Security Enhancements

3.1 Overview

In this chapter, we introduce our four papers in [86, 88, 89, 87] by providing an overview of their backgrounds and contents.

3.2 Misbehaviour Reporting

Content in this section corresponds to the following paper in Part II:

- Yoshizawa, T., and Preneel, B. Misbehaviour Reporting in ETSI ITS Standard Considered Broken. In 2022 IEEE Conference on Standards for Communications and Networking (CSCN), IEEE, pp. 144–150, 2022.

  – See p. 199

Misbehavior reporting and analysis are integral parts of the PKI system, especially in the context of vehicular communication. Vehicles disseminating incorrect or misleading information are not only sources of nuisance from other vehicles' perspectives, but they can also cause negative consequences, such as accidents, if they are taken as real and valid information. In this respect, misbehaving vehicles need to be evicted from the communication channel promptly to ensure and maintain road safety. This implies that a solid mechanism needs to be in place to report and investigate such

misbehaving vehicles. The PKI architectures in both IEEE 1609.2 and ETSI ITS standards include an entity called *Misbehavior Authority* that is responsible for investigating reported misbehaviors and determine if a misbehavior in fact exist or not, and evict the identified vehicle from the vehicular communication if needed.

Determining whether a misbehavior exists or not by itself is far from trivial as multiple factors come into play. For example, misbehavior may be triggered by benign causes such as a faulty vehicle hardware or software, or ill-intentioned actions by adversaries to cause road accidents. Even in these cases, a single observation of misbehaving action by a vehicle will likely not automatically result in a positive misbehavior. It requires series of observations and reports to positively identify a misbehavior.

From a standardization perspective, one area that is not clearly specified is a system-level design to coordinate misbehavior reporting and investigation between multiple PKI systems. In Europe, it is a key common event that vehicles from one country cross a border to an adjacent country. The end result is what we see typically on highways on a daily basis – trucks and passenger vehicles from multiple countries coexist on the road. Misbehavior reporting and investigation need to take this fundamental situation into account. However, the existing ETSI ITS standard ignores this aspect. Specifically, the ETSI ITS standard does not discuss interaction between multiple PKI systems. The same situation applies to the IEEE 1609.2 standard also if the contiguous North America is divided into multiple regions where each PKI system is allocated to a distinct jurisdiction. This area clearly falls into the domain where an international standard such as ETSI ITS needs to ensure that vehicular communication covers every aspects of cross-border vehicle movements and such events do not negatively impact operations of vehicular communication. Unfortunately, this is not the case today.

In our view, this is a significant shortcoming of both the ETSI ITS and IEEE 1609.2 standards. The consequence is that misbehavior reporting and investigation cannot be done when vehicles originating from multiple countries or regions are involved. According to the existing ETSI ITS specification, vehicles that detect misbehavior of another vehicle cannot even identify the suitable Misbehaviour Authority (MA) to send a misbehavior report to.

We discuss this issue in our paper and propose a solution for misbehavior detection and resolution in cross-border scenarios [86]. Our solution is to introduce a new information element (IE) in the pseudonym certificate definition so that vehicles observing a misbehavior of another vehicle can uniquely identify the appropriate MA that is responsible for investigating the misbehavior of the vehicle. Given that vehicles' messages include certificates for the purpose of

verifying the digital signature, receiving vehicles can identify the responsible MA by looking at the appropriate field in the certificate. Our solution is simple, straightforward, and effectively addresses the issue.

We believe that this is an urgent issue that the ETSI ITS standard committee needs to address given that retrofitting changes and introducing additional functionalities to already-deployed system is a challenging task. Otherwise, it will introduce additional migration and compatibility issues with vehicles with legacy implementations based on the existing standards. To avoid such issues, a solution needs to be included to the deployment from day one.

After publication of our paper in 2022 [86], ETSI has published a new specification on misbehaviour reporting, TS 103 759 [37]. It is a normative specification following the conclusion of pre-standard work, TR 103 460 [30] in 2020, which we discussed in our paper [86]. This new specification in [37] defines an architecture and an overall framework of misbehaviour detection. It is certainly a step forward in specifying a more concrete solution. However, it contains sections that indicate rather unrealistic expectations, and some sections explicitly states that certain aspects of misbehaviour detection is implementation specific. In this respect, this specification requires further work.

3.3 Pseudonym Certificate Generation and Distribution

Content in this section corresponds to the following paper in Part II:

- Yoshizawa, T., and Preneel, B. A New Approach To Pseudonym Certificate Management in V2X Communication. In 2023 IEEE Conference on IEEE Vehicular Networking Conference (VNC), IEEE, pp. 25–32, 2023.

  – See p. 221

The PKI system architecture as defined in IEEE 1609.2 [79, 80, 49] and ETSI ITS 102 940 [27] describe the functionalities of the system entities. The Authorization CA in [79] and the Authorization Authority (AA) in [27] are responsible for generating and distributing pseudonym certificates to vehicles. However, exact details of how generation and distribution are performed are not specified. As the next step to define this area, ETSI has published a pre-standard report to identify multiple candidate schemes in ETSI TR 103 415 [25]. One of the candidate schemes described in this TR document is called *Issue First Activate Later (IFAL)* [82].

Some of the unique advantages that set IFAL apart from other schemes includes: (1) a clear separation of certificate distribution and activation, hence the name of this scheme, and (2) each pseudonym certificate is used only once and never reused. For the first point, this scheme takes a modular approach to allow pre-loading of potentially a large amount of pseudonym certificates to a vehicle up-front, and regularly activate a set of pseudonym certificates on an ongoing basis per period called *epoch*. The IFAL paper [82] proposes this *epoch* to be 90 days. This per-*epoch* activation is carried out by the PKI system to deliver an *activation key* prior to the start of each *epoch*. This *activation key* is encrypted using a *transport key* that is assigned to a vehicle at the time of its successful enrolment with the PKI system. For the second point, each pseudonym certificate is pre-allocated to a specific 12-minute period. Therefore, this scheme makes tracking vehicles more difficult for adversaries as pseudonym certificates are never reused. Thus, it can be argued that this solution is more privacy-protecting.

At first glance, this solution appears to be promising with positive characteristics. However, upon careful study, we notice that this scheme has questionable features. This observation motivated us to study this scheme in detail. The end result is captured in our paper [88].

The following is a succinct list of issues we have identified in the IFAL scheme.

1. Wasted certificates – a large number of pseudonym certificates are wasted due to fixed allocation of day/time while no vehicle is driven 24 hours/day and 365 days/year.
2. Transfer of private key information over activation – the secret key to derive private keys for pseudonym certificates are transferred at the time of per-*epoch* activation.
3. No forward and backward secrecy – the transport key to encrypt the epoch key is never renewed. Thus, once the transport key is broken, all private keys for the past, present, and future *epochs* are revealed.
4. Inflexible pseudonym certificate usage – all pseudonym certificates fixed to a 12-minute period makes the pseudonym change periodic and predictable, making it pseudonym change correlation easier compared to when certificates are changed at a random time interval.
5. Gap period in passive revocation – the 90-day *epoch* duration implies a revoked vehicle will continue to participate in communication for up to 90 days before it is evicted, a significant lag of revocation to take effect.
6. Sub-optimal and unreliable activation channel – the use of SMS or manual operation is already known to be insecure and unreliable.

Based on our observation of these IFAL issues, we proposed an alternative scheme that addresses all of these issues. It is based on a modified OAuth framework [45] by re-framing message signature as a type of service Hardware Security Module (HSM) provides to the On-Board Unit (OBU) in the vehicle. In other words, when an owner or driver opens the vehicle door and starts the engine, this event triggers a re-authentication of the vehicle with the PKI system. If the result of the re-authentication procedure is successful, then the vehicle's HSM continues to provide the signature generation as a service (i.e. *Signature-as-a-Service*) for all messages the OBU generates and transmits. If, on the other hand, the re-authentication is unsuccessful, then the vehicle's HSM rejects future message signature generation requests by the OBU. This procedure is repeated on a regular basis, such as once every 24 hours. This way, a vehicle is no longer able to transmit valid messages as soon as the re-authentication result indicates that the vehicle is revoked.

As the mechanism to realize this re-authentication procedure, we use AES Galois/Counter Mode Synthetic Initialization Vector (AES-GCM-SIV). AES-GCM-SIV is a type of Authentication Encryption with Associated Data (AEAD) that guarantees both confidentiality and authenticity of data.

We also introduce an additional feature to AES-GCM-SIV to make every iteration of the procedure to use a unique key pair to encrypt the message and guarantee its integrity. Doing so further makes the procedure more robust. Our solution also takes into account realistic situations such as the fact that vehicles may not be driven every day. The end result is that our re-authentication mechanism is a straightfoward, lightweight, and robust solution.

3.4 Post-Quantum Impact on Certificates

Content in this section corresponds to the following paper in Part II:

- Yoshizawa, T., and Preneel, B., Post-Quantum Impacts on V2X Certificates – Already at The End of The Road. In 2023 IEEE Vehicular Technology Conference (VTC), IEEE, pp. 1–6, 2023.

  – See p. 245

It has been known that, since early 1990s [54, 13], certain mathematical problems that have been used as a fundamental building block in cryptographic solutions will become vulnerable in the face of quantum computers. The most notable example is the problem of large integer factorization and discrete logarithms which are used in public-key-based algorithms such as RSA and Elliptic Curve

Cryptography (ECC) [14]. How long a given cryptographic key can remain secure against the growing threat of quantum computers depends on factors such as the duration for which data needs to be kept secure and the time it takes to deploy a quantum-safe solution. If the quantum computers' capabilities surpass these criteria, the cryptographic key is clearly not safe [59].

Shor's algorithm can factor large numbers in polynomial time [77]. However, authors of [10] claim that running this algorithm requires "billions of operations on thousands of logical qubits."[1] The quantum computer introduced in 1998 had two physical qubits. As of 2019, the largest quantum computer made by Google had 53 qubits [57]. In 2021, their scale increased to 127 qubits. The latest quantum computer introduced by IBM as in 2022 has 433 qubits, which is more than three times of the one in the previous year [47]. Although the number of qubits are steadily increasing, the current scale is still far from running Shor's algorithm. If we assume that Moore's law applies to the capacity increase of quantum computers, reaching millions of physical qubits scale is expected to take 25 to 30 years [57]. Despite this situation, out of abundant caution, National Institute of Standards and Technology (NIST) recommends that those potentially vulnerable algorithm are replaced by Post Quantum Cryptography (PQC) algorithms by 2030 [42], and has started a process to select PQC algorithms that are resistant against quantum computers [7].

According to the latest report on the NIST competition on PQC algorithms [7], three digital signature algorithms have been standardized.[2] All of them require longer public key (PK) compared to conventional algorithms such as ECDSA. The exact key size depends on the algorithm. However, in the worst case scenario (Dilithium-5), the PK size will grow with a factor of 81 compared to ECDSA keys. From a protocol perspective, the combination of the PK size and the digital signature size affects the total message size.

Vehicular communication is no exception to this threat of quantum computers as it relies on public key cryptography, specifically digital signature generation and verification using ECDSA. In fact, vehicles are durable goods which have lifetime over 20 years [62]. Therefore, robustness against cryptographic threats need to be guaranteed for the period of the vehicle's entire lifetime. This implies

[1]The capacity of quantum computers is expressed by physical and logical qubits. A physical qubit is "a physical device that behaves as a two-state quantum system, used as a component of a computer system", and a logical qubit is "a physical or abstract qubit that performs as specified in a quantum algorithm or quantum circuit" [84]. Due to the nature of physical qubits lacking stability, multiple physical qubits are used for error correction and fault tolerance to function as a logical qubit [84].

[2]This NIST report states that one key-encapsulation mechanism (KEM) algorithm (CRYSTALS-Kyber) and three signature algorithms (CRYSTALS-Dilithium, Falcon, and SPHINCS+) are standardized [7].

maintenance and upgrade of cryptographic algorithms over time. The PKI system for vehicular communication needs to take this point into account.

IEEE 1609.2 [79] and ETSI ITS 103 097 [33] specify the certificate format for vehicular communication. One notable point to highlight is that the IEEE 1609 committee has decided to define a customized certificate format for vehicular communication instead of reusing the conventional X.509 [52] standard. The ETSI ITS standard also adopted this IEEE 1609 standard as a baseline specification and made modifications, including the certificate definition. In other words, the certificate definitions in these two standards are similar.

In this context, we have identified an issue in the IEEE 1609.2-defined certificate format – it is not ready to migrate to PQC algorithms, contrary to X.509. To ensure seamless migration and transition to PQC algorithms, vehciular communication needs to be able to carry PKs for both the current algorithm (EDCSA) and the future one at the same time in a certificate, i.e. a *hybrid* certificate. The X.509 standard already addresses this migration issue with the use of an optional extension field to include a new PK, if necessary. However, there is no equivalent optional field defined in the certificate format defined by IEEE 1609.2. This is clearly an oversight by the IEEE 1609 committee given that this specification was first published in 2006 and threats by quantum computers were likely less prominent at that time. Therefore, we point out this omission in the standard and propose to correct this oversight [89].

This correction in the standard is an urgent matter given that retrofitting a new certificate format into already-deployed vehicles on the road will introduce significant challenges and issues to maintain compatibility with the legacy certificate format that has no forward compatibility. In this sense, we recommend that the IEEE 1609 and ETSI ITS standard committees address this issue soon.

Furthermore, we also point out negative implications of the introduction of *hybrid* certificates in vehicular communication as doing so will create significant issues to an extent that the vehicular communication itself will no longer be sustainable. As discussed earlier, the use of *hybrid* certificates is required to make the seamless transition from the current algorithms to the PQC algorithms. However, the large PK size in PQC algorithms effectively reduces the communication channel capacity. In other words, due to the addition of a large-size PK in the certificate and a digital signature, each V2X message will occupy the communication channel longer, effectively reducing the number of vehicles that can fit into the communication channel before it saturates. For example, our simulation shows that even the smallest PK size PQC algorithm (Falcon-512) will reduce the communication channel capacity by half when 30% of the vehicle population is replaced by PQC-ready vehicles that uses hybrid certificates. The end result is that the effective communication distance will

reduce by half if we assume the vehicle density for a given area is constant.

This observation has a significant implication on vehicular communication. The reduction in the effective communication distance affects the exchange of information about movements and the dissemination of safety and warning messages. Therefore, the increase of the PQC PK size and the signature size will strongly impact the communication and its effectiveness to achieve safety on the road.

There are three solutions to alleviate this concern. The first is to increase the channel bandwidth, the second is to improve the spectrum efficiency by using more complex modulation techniques, and the third is to minimize the increase of the PQC PK size. The first requires a change in the government policy on radio spectrum usage which is a time-consuming process which may or may not materialize. Also, universal harmonization of spectrum increase is required at global scale to make the solution viable. The second can affect the performance as higher-order modulation techniques are more vulnerable to changing radio environments. In addition, the available choices of modulation schemes are bounded by what the existing standards offer. The third requires further research to design PQC algorithms that minimize the PK size increase.

More generally, the design of new PQC algorithms needs to take its impacts on real-time systems into consideration, such as vehicular communication. The standardized algorithms by the NIST competition [7] thus far does not meet this need.

3.5 Certificate Digest Handling

Content in this section corresponds to the following paper in Part II:

- Yoshizawa, T., and Preneel, B. On Handling of Certificate Digest in V2X Communication. In 2022 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, pp. 160–165, 2022.

  – See p. 181

Vehicular communication is a real-time system. Vehicles reflect real-time change of their movement and status, and subsequently construct and transmit messages in the communication channel. Vehicles receiving these messages need to process them and take action (if necessary) within a specific time window. For example, the dissemination of dynamic information of moving vehicles,

such as their position, direction, and acceleration needs to be received and processed by the receiving vehicles within a fixed time window for vehicles to accurately maintain *situational awareness* regarding their dynamically-changing environment. Processing obsolete information is not only useless to accurately determine a vehicle's maneuver, but also it can be dangerous from the overall goal of achieving road safety if the information does no longer accurately reflect reality.

From this perspective, the security solution in vehicular communication as specified in the IEEE 1609.2 and ETSI ITS standards has mechanisms to make the communication as efficient as possible. One example in this context is to avoid repeating the same information in successive messages when possible. For example, Cooperative Awareness Message (CAM) in ETSI ITS EN 302 637-2 [28] and IEEE 1609.2 [79] allow transmitting vehicles to omit the certificate from these messages. According to an empirical study of CAM transmission in [12], typical CAM messages have a message length of between 200 to 800 bytes with an average of 350 bytes. Within these messages, approximately 100 to 150 bytes are certificates. In other words, between 29% to 43% of CAM message content remains static in all messages during the period a vehicle uses the same pseudonym certificate. Replacing the repetitive certificate in messages with a shorter information can immediately reduce the overall message length, thus improving the communication channel usage of these messages. In other words, according to the ETSI ITS standard, vehicles include the complete certificate only periodically, once per second. When CAM messages are transmitted more frequently, due to its transmission criteria as determined by the vehicle's movement, a certificate *digest* is included instead of the full certificate. A certificate digest is a hash of the certificate truncated to the least-significant 8 bytes. Therefore, replacing a certificate with an 8-byte digest results in the message size reduction of 42% at maximum.

The use of this certificate *digest* implies that receiving vehicles need to hold the full certificate in their internal memories and use it every time a *digest* is included in a CAM message in order to calculate and verify the digital signature in the message and determine whether the received message is genuine or not. However, there can be situations where a vehicle may not have the full certificate that corresponds to a received *digest*. Such a situation may arise when a transmitting vehicle just enters the communication range of a receiving vehicle, and the very first message the receiving vehicle receives contain a *digest*. In this case, the receiving vehicle needs to resolve this *unknown digest* to a complete certificate before it can verify the digital signature in the received message.

To address this needs, the CAM message header has an optional field to list one or more *unknown digest*. Including a *digest* in this optional header field indicates

that the transmitting vehicle of this CAM message requests other vehicles to provide the corresponding full certificate by responding to this request. Any of the surrounding vehicles within the communication range can respond to this request by transmitting the *certificate* that corresponds to the indicated *digest*. This resolution mechanism is called *Peer-to-Peer Certificate Distribution (P2PCD)* defined in IEEE 1609.2 Amendment 1 [80] and ETSI ITS EN 302 637-2 [28].

This resolution mechanism works in theory. However, when we take vehicle movements into account, it becomes clear that this mechanism is not very effective. In our paper [87], we showed our simulation results of this mechanism based on recreating real-world traffic. This real-world traffic data was collected as a part of the *Connected Corridor for Driving Automation* (Concorda) project [18] that took place between 2017 and 2020.[3] During this project, traffic data from Antwerp ring road was taken for the entire month of September 2019. We used this data to recreate the traffic flow and applied this P2PCD mechanism to evaluate its effectiveness.

Our simulation result confirms our suspicion that this mechanism is not effective, at least in the highway environment where vehicles move in relatively at high speed in a highly-fixed directional trajectory. As discussed earlier, the P2PCD mechanism is triggered when a vehicle receives a CAM message containing a certificate *digest*, and it does not internally hold the corresponding full certificate. Our simulation result highlights that a large majority (over 80% of the cases) for this condition occurs for traffic moving in the opposite directions on the highway, rather than vehicles moving in the same or similar direction. Furthermore, traffic moving in the opposite direction spends much less time within each other's communication range. The time two vehicles in opposite directions spend within each other's communication range is inversely proportional to the speed of these vehicles. For example, two vehicles moving in the opposite direction on a highway spend 5.4 seconds at 100 km/h with 300 meter communication range. Once they exit each other's communication range, it is unlikely that they will encounter each other again in the near future, e.g. 24 hours. In this sense, applying the P2PCD mechanism in every *unknown digest* situation, when the large majority of this situation occurs in vehicles moving in the opposite direction, is not a fruitful action to take.

As an alternative to triggering the P2PCD mechanism, simply "doing nothing" is a perfectly reasonable solution due to several reasons. First, given that vehicles periodically include the full certificate in the CAM message every second, it is likely that the full certificate will be available in the next 500 msec on average.

[3]We would like to thank Prof. Chris Tampère and Dr. Mohammad Ali Arman of the KU Leuven Mechanical Engineering department for kindly sharing the traffic data from this project.

Depending on the relative timing difference, to wait for this next message with a full certificate may be more efficient with lower usage of the communication channel than proactively resolving it using the P2PCD mechanism. Second, proactive resolution using P2PCD is only useful while the vehicle in question is within communication range. Therefore, especially in highway scenario where vehicles move at relatively high speed, vehicles in the opposite diction may go out of the communication range several seconds after the P2PCD mechanism is resolved. Our simulation result shows that approximately 80% of the *unknown digest* situation is a short-lived communication, triggering the P2PCD mechanism at every such event does not lead to an effective use of the communication channel.

Based on our simulation result and observation, we conclude that the P2PCD mechanism requires improvement by taking into consideration vehicle movement, such as relative differences of direction and speed. In other words, by triggering the P2PCD mechanism only for the traffic in the same or in a similar trajectory, the level of effectiveness of this mechanism will increase.

Chapter 4

Privacy Enhancement

4.1 Overview

In this chapter, we introduce our paper [91] by providing the overview of its background and content.

4.2 A New Beacon Scheme

Content in this section corresponds to the following paper in Part II:

- Yoshizawa, T., Singelée, D., and Preneel, B. A New Privacy Enhancing Beacon Scheme in V2X Communication. In Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, pp. 139–151, 2021.

  – See p. 163

The safety-related messages in vehicular communication are specified as Cooperative Awareness Message (CAM) in Europe as defined in ETSI ITS EN 302 637-2 [28] and Basic Safety Messages (BSM) in the US as defined in SAE J2735 [76]. These messages are transmitted periodically, between 1 to 10 messages per second. In the ETSI ITS standard [28], the triggering condition of CAM messages are defined as follows:[1]

[1]ETSI ITS defines both 802.11p-based and C-V2X-based access technologies that have different CAM transmission criteria. In the former, as the 802.11 technology does not explicitly

1. The minimum transmission interval (100 msec.) has elapsed since the last transmission, and any of the following conditions is met:
   (a) The change of direction from the last transmission exceeds more than 4 degrees, or
   (b) The distance from the position of the last transmission exceeds more than 4 meters, or
   (c) The acceleration change from the last transmission exceeds more than 0.5 meter/sec.
2. If none of the above condition is met, and the periodic transmission interval (1 sec.) has elapsed from the last transmission.

In other words, one can infer that vehicles transmit CAM messages more frequently when they are on the move, and less frequently when they are stationary (e.g. stopping at a red traffic light). This variable transmission criteria helps to optimize the use of communication channel.

One notable observation from these transmission criteria is that vehicles determine the CAM message transmission strictly based on their own movements. In other words, they do not take other factors into consideration for CAM message transmission. We consider that it will benefit and optimize communication channel usage even further if vehicles take other factors into consideration. Doing so likely leads to an enhanced level of privacy for vehicle owners.

From this perspective, we propose a new decision criterion for CAM transmission – presence of other vehicles. In other words, if a vehicle discerns there is no or few vehicles on the road, disseminating CAM messages may not help achieve anything from a road safety perspective. On the other hand, voluntarily disseminating vehicle's information irrespective of other vehicles' presence may lead to a compromise of privacy of the vehicle and its owner. This is especially relevant in CAM messages because they are broadcast-based communication and sent in clear (i.e. no encryption is applied). Therefore, any entity, malicious or not, with appropriate hardware and software to receive these messages can decode the message content.

Therefore, it makes sense to try to limit, or minimize, such voluntary sharing of vehicle's movement-related information when it is not necessary or does not achieve road safety.

---

define congestion control mechanism, transmitting entities are required to observe a minimum transmission interval called De-centralized Congestion Control (DCC). In the case of C-V2X, the lower layer defines the radio resource allocation, hence this extra transmission interval is not necessary.

Traffic pattern and density varies in factors such as location, time, and type of area. For example, the number of vehicles within a given area (e.g. 1 square kilometer) is likely higher on busy highways in urban areas during rush hour. On the other hand, there may be no cars on the road at 3 AM on Sunday morning on a local street in a rural area. Therefore, if the CAM transmission criteria takes these environmental conditions into account, vehicles may be able to switch off CAM transmission to limit unnecessary dissemination of vehicle information.

In our paper [91], we proposed a scheme to check the number of vehicles on the road, and determine whether to switch on or off CAM transmissions. If a vehicle detects that there is a sufficient number of vehicles within the communication range (based on a threshold parameter), then this vehicle start transmitting CAM messages. If, on the other hand, there are fewer vehicles than a fixed threshold, then it stops transmitting CAM messages. This check is done by vehicles sending a *beacon* message periodically. This *beacon* message consists of static information only ("I am here."), thus does not expose any information unique to a vehicle. The absence of vehicle-specific data in this beacon message implies that it is not possible to identify how many vehicles are actually present, or if these messages are sent by real vehicles as opposed to fake vehicles. In order to account for potential adversaries transmitting this fake *beacon* message to trigger other vehicles to switch on CAM messages, our mechanism also includes a probabilistic *testing phase* to selectively try out CAM transmission to see if there is indeed a sufficient number of vehicles present or not by verifying the genuine CAM messages and counting the number of unique vehicles.

This further implies that vehicles periodically monitor the communication channel and test this threshold and move to the *testing phase* to determine if the current behavior (i.e. CAM transmission on or off) needs to be changed or not. It further implies that, if the change of behavior is needed, this transition needs to occur smoothly with sufficient level of confidence. To do so, our scheme also defines additional threshold and timer values.

We conducted a simulation to test our proposed scheme and discussed our finding in [91]. Our simulation includes both large-city and small-city environments. The simulation results indicate the effectiveness of our proposed scheme in reducing CAM transmission when the surrounding environment indicates it is not necessary. This way, our scheme effectively limits the potential exposure of privacy-related information to adversaries who can collect and analyze unprotected broadcast-based CAM messages.

There are multiple benefits in our scheme when it is applied to real-world situations. First, as discussed earlier, our beacon scheme can adapt to the driving environment and does so seamlessly. For example, when a vehicle

travels from a busy metropolitan area during the day to a sparse rural area at night, our beacon scheme adjusts its CAM and BSM transmission behavior that best fits to the environment the vehicle find itself in while minimizing voluntary sharing of privacy-related information. Second, in the early days of vehicular communication technology, the proportion of V2X-capable vehicles on the road is relatively small. During this period, the effectiveness of CAM or BSM messages is limited given that only a small proportion of vehicles on the road supports this new technology. In this situation, it may be more accurate to characterize the message dissemination by these V2X-capable vehicles in the start-up phase as a voluntary sharing of their information rather than achieving the intended goal of improving road safety. In this sense, our beacon scheme is useful to seamlessly transition from the early technology introduction period to a larger-scale adoption of this technology.

Chapter 5

Closing Discussion

5.1 Discussion

We conclude this thesis by reviewing the research outputs as a whole and discuss how our research questions we identified in Sec. 1.3 are answered in our research outputs. Then we state future work and capture some key observations we have made throughout our research work presented in this thesis.

5.1.1 Answers to the Research Questions

In this section, we discuss how each of the research question identified in Sec. 1.3 are addressed in this thesis. The referenced section numbers refer to the sections in Part I and the page numbers refer to the paper in Part II, respectively.

1. *Are the existing standards, specifically regarding the certificate management system based on the PKI paradigm, sufficient to realize the overall objective of improving road safety and preserve users' privacy?*

   Answer: We believe that the PKI-based security solution and periodic pseudonym change for privacy protection, as defined by IEEE 1609.2 and ETSI ITS, are necessary but not sufficient as an effective solution by themselves. They merely serve as *baseline frameworks* toward achieving the stated goal, but lack in specific scheme definition, leaving many details as implementation-specific matter which results in a varying level of

effectiveness in practice. In other words, both of these standards fall short of specifying effective and complete solution.

We propose two solutions to address this area: one covers security ([88] in Sec. 3.3, p. 221) and another one privacy ([91] in Sec. 4.2, p. 163). We defer detail discussion on these solutions under question #4 below.

2. *Are there areas where these standards may cause negative impacts on the intended road safety?*

   Answer: Our paper [87] discussed in Sec. 3.5 (p. 181) addresses this question. In this paper, we showed that the P2PCD mechanism as defined in both the IEEE 1609.2 and ETSI ITS specifications are ineffective and only results in using additional communication channel and computing resources especially in highway traffic scenario. Based on the simulation results, we show that ineffective and unnecessary channel usage and processing can be avoided by vehicles being aware of the environment (e.g. current average speed and its variations) and refrain from requesting P2PCD resolution with other vehicles. Doing so reduces the communication channel usage and avoids unnecessary processing in all vehicles involved, both sending and receiving requests and responses. The benefit of alleviating vehicles from these unnecessary processing will be further pronounced as the traffic volume increases. Reducing unnecessary channel usage and processing will help ensure that these resources are available for processing high priority events such as communicating emergency situations in De-centralized Environmental Notification Messages (DENM).

3. *What are the key gaps and issues in these standards? For these gaps and issues, what are possible solutions to address them?*

   Answer: Our two papers discussed in Sec. 3.2 and Sec. 3.4 address this question. The paper [86] discussed in Sec. 3.2 (p. 199) demonstrates that misbehavior resolution mechanism as is currently specified in ETSI ITS standard does not work, most notably in cross-border scenarios where vehicles managed by different PKI systems co-exist on the road. This issue is introduced due to the architectural simplification of IEEE 1609.2 PKI system design upon incorporating it into the ETSI ITS standard. Our proposed solution effectively addresses this issue by introducing a new information element (IE) in the certificate definition. To put it in another way, this type of issue arises due to the standards' view being limited to a single PKI system rather than expanding their scope to multiple PKI systems and interactions between them.

The paper [89] discussed in Sec. 3.4 (p. 245) highlights the absence of forward compatibility in the certificate format for the future migration of PQC signature algorithm. This issue is commonly applicable to both IEEE 1609.2 and ETSI ITS standards.

Some other outstanding issues that we discussed in our survey paper [90] but not covered in our solution papers include: (1) potential new approaches on enhancing privacy protection when confidentiality protection cannot be used, (2) considerations on differentiated privacy treatment based on vehicle types and ITS-S types, e.g. privately-owned vs. commercial vehicles, vehicle vs. RSU vs. VRU, (3) certificate management for non-vehicle ITS-S types, i.e. RSUs and VRUs, (4) interactions between multiple PKI systems, (5) separation of pseudonym certificates for different communication types, e.g. broadcast vs. unicast.

4. *Are there further enhancements to supplement the existing functionalities in the standards? If so, what are they and how can they improve the security and privacy of vehicular communication?*

Answer: As discussed under question #1, we have authored two papers that enhance security and privacy aspects.

From a security perspective, the use of pseudonym certificates implies the potential need of revoking them if and when it becomes necessary. One example is preventing misbehaving vehicles from negatively influencing other vehicles on the road. Promptly evicting such vehicles, malicious or not, from the communication channel is important from a road safety perspective. However, both active (CRL-based) and passive revocation approaches have their own issues.

Historically, the CRL-based revocation approach has had fundamental issues which have not been resolved yet as we discussed in [92]. The passive revocation approach suffers from a different issue; it leaves a significant time gap if the interval of a vehicle requesting additional pseudonym certificates to the PKI system is in the order of days or longer. If vehicles are pre-loaded with pseudonym certificates for an extended period (e.g. three years [41] or five years [82]), then passive revocation will not be triggered in the order of years as the worst case scenario. During this period, revoked vehicles continue to use their pseudonym certificates until they run out of valid certificates; this can take several years depending on the preloading scheme and the relative timing of a revocation event. To address this issue, we have proposed a solution in our paper [88] discussed in Sec. 3.3 (p. 221).

In this paper, we re-frame the activation semantics discussed in the IFAL scheme [82] to a shorter period, e.g. daily. Further, digital signature

generation is characterized as *signature-as-a-service* which the vehicle's HSM provides to the OBU. As a result, this activation scheme effectively becomes a procedure a vehicle triggers daily in which a vehicle requests a permission to continue to operate *normally*. If the PKI system has revoked this vehicle's certificates, then this activation procedure fails, resulting the vehicle no longer able to generate valid digital signatures, effectively denying the vehicle from transmitting valid messages. With this scheme, revoked vehicles stops transmission within 24 hours at maximum rather than days, months, or years.

From a privacy perspective, the standards specify transmitting CAM / BSM messages under all circumstances without considering its meaningfulness. To address this point, we proposed that vehicles do not necessarily transmit CAM messages when it is deemed unnecessary ([91] in Sec. 4.2, p. 163). By monitoring the environment and transmitting CAM messages only when it is truly meaningful to do so, potential leakage of privacy-related information and tracking of vehicles by adversaries can be minimized. We also stress that our proposed scheme is equally effective in the early days of V2X technology introduction in which the vehicle population supporting V2X technology is low.

5.1.2 Adversarial Assumptions (Attacker Models)

Our published papers in Part II identify issues and propose new approaches or solutions, except for the two survey papers [85, 90]. These solution papers are [86, 87, 88, 89, 91]. Each of these papers addresses distinct issues identified in the relevant standards as described in our survey paper [90]. As a result, these five papers are complementary to each other.

Among these papers, two of them ([91] and [88]) involve adversaries; the other three ([86, 87, 89]) do not. In this respect, the first two require clarifications regarding their adversarial assumptions. As each paper addressed distinct issues separately, our assumptions on adversaries (*attack models*) do not necessarily coincide in these papers.

Our proposed solution in [91] (Sec. 4.2) assumes that adversaries do not have access to valid private keys and certificates, thus cannot generate valid messages. The reason for this assumption is that active and highly intrusive attacks such as compromising an in-vehicle HSM is significantly more difficult to achieve successfully due to the security properties of the hardware-based security device. On the one hand, we do not necessarily exclude the possibilities of such attacks to occur. On the other hand, due to this difficulties to achieve successful attacks on such devices, we consider prevalent and wide-scale attacks that affect large

numbers of vehicles simultaneously is low. Considering the nature of moving vehicles, encountering many such compromised vehicles over time and space is unlikely. Based on this assumption, our proposed scheme in [91] assumes that adversaries within the immediate communication range from a given vehicle can only transmit beacon messages at most in order to entice vehicles to transmit CAM messages and capture these messages or track vehicles based on the message content but cannot transmit valid CAM messages.

Contrary to this assumption, the *attack model* in [88] (Sec. 3.3) is based on a different assumption. The scheme presented in this paper re-frames the activation semantics in such a way that vehicles regularly and periodically contact the PKI system to ensure that their certificates are not revoked. Doing so minimizes the time gap in the passive revocation mechanism as the sole revocation mechanism of pseudonym certificates in the ETSI ITS standard. In this context, this proposed scheme assumes that vehicles can be compromised for *any* reason, implying that adversaries may be able to compromise an on-board HSM, resulting in accessing private keys. In addition, contrary to the scenario in [91] (Sec. 4.2), the attack is specific to a single vehicle only within the scope of this paper. Therefore, the scope of impact from the scenario in [91] is significantly localized to a single vehicle compared to possibly large number of compromised vehicles in [88].

5.2 Future Work

Several areas can be considered as possible topics for further research. First, this thesis addresses a subset of gaps and issues identified in [90], leaving other unaddressed areas open. Closing this loop by investigating and proposing possible solutions for these open areas is an immediate research direction. One notable example is to define a viable migration road map to new PQC signature algorithms that can suit real-time systems such as V2X communication when they become standardized.

Second, we do not consider that the gaps and issues identified in [90] are exhaustive. Therefore, expanding the scope of analysis by investigating other relevant standard specifications may reveal additional issues. Identify and addressing those additional issues can be an interesting research work as an extension of the work presented in this thesis.

Third, future trends such as Cooperative Connected Automated Mobility (CCAM) – a combination of autonomous vehicles (AVs) enhanced with their communication capabilities – may present new challenges. Because higher AV categories (SAE level 4 or 5) may not require human driver's constant attention,

or no driver at all, potential negative consequence due to insufficient security can be even more disastrous than those of lower level autonomy. In this respect, security and privacy aspects will be even more significant in the AV context. In other words, AVs present a new and unique operating environment, which likely require new approaches from security and privacy perspectives of the V2X communication. Identifying them and designing solutions against them will be an important new research area in order to ensure AVs are safe, secure, and reliable in the real world.

5.3 Closing Remarks

As closing remarks, we discuss some key observations we have made through our research work presented in this thesis.

First and foremost, we assert that the balance between safety and privacy is not sufficiently addressed in the relevant standards; some of their solutions can make road traffic more dangerous, completely negating the intended outcome to make roads safer with the use of communication between vehicles. As discussed in Sec. 6.5 in [90], the Emergency Electronic Brake Light (EEBL) as defined in DENM message is a prime example to illustrate this point.

According to the definition of privacy properties in Sec. 1.2, the *unobservability* property requires that receiving vehicles of an EEBL message cannot determine which vehicle has transmitted a particular message. As a result, this property makes it impossible for the receiving vehicles to determine whether to brake or not.[1] If these standards are applied to the Level 4 or Level 5 AVs, making a wrong decision by an AV significantly increases the chance of an accident, e.g. colliding to the vehicle ahead of it by not braking when it is necessary, or braking when it is unnecessary and forcing a trailing vehicle to brake and collide with it. In other words, from a road safety perspective, vehicles need to be able to identify a vehicle from a specific message in order to determine a safe maneuver under certain situations. In this sense, too strong a focus on privacy aspect will inhibit road safety.[2]

[1] ETSI TS 102 940 [27] Clause 4.3.7.2 (Confidentiality and Privacy) states *"It is assumed that each ITS application uses its own identifiers that cannot be linked to each other. In particular, DENM and CAM originating from the same vehicle should not be linkable."* On the other hand, TS 101 539 [24] Clause 5 (Road Hazard Signalling application description) states *"The RHS application may provide specific CAM interval adjustment requests to the CA basic service (see informative annex F) in order to improve the confidence level at the receiving ITS-S side."* These two statements are directly contradicting each other.

[2] In practice, AVs will likely combine data from multiple sources upon determining their maneuver. Such data sources include camera, rader, lidar, GPS, etc. In this sense, V2X

A related question that is not addressed by the existing standards are important and practical questions such as privacy protection against potentially overruling conditions such as emergency situations. This point relates to the EEBL example above. Is privacy protection in V2X communication uniformly applicable under any and all circumstances, or should the level of privacy protection be lowered under certain conditions? If the latter prevails, under what circumstances can privacy protection be diminished and to what extent? This is not an easy question to answer as it has significant implications on road safety. However, one thing is clear: under no circumstances, the use of vehicular communication should compromise road safety.

In Sec. 5.1.2, we discussed differences in adversary types in two of our papers [88, 91]. We also note that security related standards often do not explicitly state this aspect in their specifications. In this sense, stating this aspect as a mandatory element in the specification would help to clearly identify the types of threats the security solution intends to protect from. In some cases, more than one model may be required depending on the problem scope the solution addresses.

Another key observation in the ETSI ITS standard is the consequence of the architectural simplification of the PKI system from its counterpart in the IEEE 1609.2 standard, inadvertently creating new issues as a result. We believe this simplification is a conscious decision by ETSI ITS, and we consider there is value in doing so. However, it is clear that this simplification broke at least one of the existing functionalities in the IEEE 1609.2 architecture as we discussed in our paper [86]. From this example, we learn an important lesson: changes at the fundamental architectural level require thorough evaluation of their impacts on the overall system and its functionalities. In addition, as stated in Sec. 5.1.1, limited perspectives of these standards to a single PKI system leads to the lack of attention and considerations on necessary interactions between multiple PKI systems under various scenarios.

Yet another important observation in the existing standards is that they are written predominantly from the vehicle-centric perspective, and it leaves other ITS types in the dark from the certificate management perspective. This observation equally applies to both the IEEE 1609.2 and ETSI ITS standards. The question in this regard is whether there is any difference in the way how non-vehicle ITSs are managed by the PKI system, and what those differences are if it is the case. With the recent addition of new participants to the ITS system such as VRUs as defined in TR 103 300-1 [31], the absence of specifications in certificate management for these non-vehicle ITS types will become a significant

communication becomes one of these data sources. However, data from any given source should not contribute to potentially make “wrong maneuver” as a result.

issue upon deploying such devices.[3]

In addition, one significant issue that we do not have answer for at the time of this writing is the absence of viable migration road map toward PQC signature algorithms from the perspective of real-time systems such as V2X communication and other resource-constrained IoT devices. Unless a suitable new algorithm emerges for such operating environments, systems that fall into these categories will potentially be left behind from the PQC migration. Such situation may become inevitable for many systems and devices due to various constraints such as physical or performance limitations of devices, and difficulties in conducting field replacement of current deployments.

Finally, we acknowledge that there exists an unwritten but reasonably well-understood demarcation point where standardization stops and implementation specifics begin. However, standards that involve CPS systems such as vehicular communication likely may cause significant impacts on reality. Therefore, leaving many areas to implementation-dependent choice will result in varying level of effectiveness in practice. Potential consequence due to sub-optimal implementations may result in physical damages, injury, or even death. This is exactly the opposite of what ITS systems intend to achieve. In this sense, CPS-related standards such as ITS need to go a step further to ensure the intended road safety is achieved and prevent negative consequences.

[3]ETSI EN 302 665 [20] (the latest version: Sept. 2010) Clause 4.5.1 defines four ITS device types (*sub-systems*). One of them is a hand-held device called *Personal ITS sub-system.* The use of such ITS device type became realistic in recent years due to the technological advancement and subsequent ubiquity of smartphones. From a practical perspective, it is the only viable platform to deploy VRU services as we consider it is unrealistic to expect consumers to purchase a dedicated device for the sole purpose of ITS.

Chapter 6

Conclusion

Two fundamental characteristics of vehicular communications are: (1) dynamic topology change due to moving vehicles, and (2) the use of direct communication among vehicles on the road as the main scenario for realizing safety-related services. These characteristics imply that the set of vehicles within the communication range of one vehicle's reference point constantly changes. Thus the communication in this operating environment necessarily relies on predominantly broadcast mode in which transmitting vehicles are not aware of the exact constituents of receiving vehicles and do not use message confidentiality (i.e. encryption). The use of confidentiality is limited to unicast mode for which the applicable use cases in vehicular communication are limited such as remote driving or platooning. In this paradigm, the only security mechanism in place is the use of digital certificates to guarantee the transmitting vehicles' authenticity and message integrity by verifying the certificate chain and the digital signature attached to these messages. From a security perspective, it is the only line of defense. This paradigm sets itself apart from other wireless communication systems, such as cellular systems.[1]

In this thesis, we analyzed existing vehicular communication standards from security and privacy perspectives, and identified issues and gaps as the result of our detailed analysis. Our survey paper [90] represents the culmination of our analysis and describes these open issues and gaps. As this paper shows, there are number of open areas, some of which are questions at the fundamental level, including achieving a good balance between conflicting requirements of

[1] Communication in cellular systems takes place over the network infrastructure based on a unicast communication mode. Although cellular systems support broadcast and multicast based services, their actual deployment and usage are limited.

road safety and privacy protection. Leaving these issues as an implementation-dependent matter will most likely result in ineffective solution in reality. In this sense, we consider that standards (mainly IEEE 1609.2 and ETSI ITS) still require work at some fundamental levels.

As an offspring to our analysis, we have published several research papers that focus on some of these key issues related to security and privacy aspects. In some of these papers, we proposed alternative solutions or new approach to address these issues. These papers include [86, 87, 88, 89, 91].

In summary, this thesis can be characterized as a culmination of enhancements to improve the existing standards from both security and privacy perspective. At the same time, among the issues and gaps we have identified in [90], the above-mentioned solution papers represent only a small subset. In this sense, there are still many open areas to be addressed.

The combination of AV and communication capabilities, the so-called connected autonomous vehicle, or Cooperative Connected Automated Mobility (CCAM), as a more general term will introduce new technical challenges in many aspects. Security and privacy in this context will also need to evolve by addressing new challenges to make this reality while improving road safety.

Bibliography

[1] 3GPP. TS 33.185, Security Aspect for LTE Support of Vehicle-to-Everything (V2X) Services, v15.0.0. Technical report, 3rd Generation Partnership Project, 06 2018.

[2] 3GPP. TS 23.285, Architecture Enhancements for V2X Services, v15.3.0. Technical report, 3rd Generation Partnership Project, 03 2019.

[3] 3GPP. TS 23.285, Architecture Enhancements for V2X Services, v16.2.0. Technical report, 3rd Generation Partnership Project, 12 2019.

[4] 3GPP. TS 23.287, Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services, v0.2.0. Technical report, 3rd Generation Partnership Project, 03 2019.

[5] 3GPP. TS 23.287, Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services, v.17.2.0. Technical Specification (TS), 3rd Generation Partnership Project, 12 2021.

[6] Agencia Española Protección Datos (AEPD). 10 Misunderstandings Related to Anonymisation. `https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf`, 03 2021.

[7] Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, and Daniel Smith-Tone. NIST IR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. *US Department of Commerce, NIST*, 2022.

[8] Messaoud Babaghayou and Nabila Labraoui. Transmission Range Adjustment Influence on Location Privacy-Preserving Schemes in VANETs. In *2019 International Conference on Networking and Advanced Systems (ICNAS)*, pages 1–6. IEEE, 2019.

[9] Alastair R Beresford and Frank Stajano. Mix Zones: User Privacy in Location-Aware Services. In *IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second*, pages 127–131. IEEE, 2004.

[10] Daniel J Bernstein and Tanja Lange. Post-Quantum Cryptography. *Nature*, 549(7671):188–194, 2017.

[11] Benedikt Brecht, Dean Therriault, André Weimerskirch, William Whyte, Virendra Kumar, Thorsten Hehn, and Roy Goudy. A Security Credential Management System for V2X Communications. In *IEEE Transactions on Intelligent Transportation Systems*, volume 19, pages 3850–3871. IEEE, 2018.

[12] C2C-CC. TR2052, Survey on ITS-G5 CAM Statistics. Technical report, Car 2 Car Communication Consortium, 12 2018.

[13] Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Walter Lioen, Peter L. Montgomery, Brian Murphy, Herman Te Riele, Karen Aardal, Jeff Gilchrist, Gérard Guillerm, Paul Leyland, Jöel Marchand, François Morain, Alec Muffett, Chris & Craig Putnam, and Paul Zimmermann. Factorization of a 512-bit RSA Modulus. In *Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings 19*, pages 1–18. Springer, 2000.

[14] L Chen, S Jordan, Y Liu, D Moody, R Peralta, R Perlner, and D Smith-Ton. NIST IR 8105, Report on Post-Quantum Cryptography. NIST (2016). *US Department of Commerce, NIST*, 2016.

[15] Federal Communications Commission. Dedicated Short Range Communications (DSRC) Service. `https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service`.

[16] Federal Communications Commission. FCC Allocates Spectrum in 5.9 GHz Rrange for Intelligent Transportation Systems Uses. `https://transition.fcc.gov/Bureaus/Engineering_Technology/News_Releases/1999/nret9006.html`.

[17] Federal Communications Commission. STATEMENT OF CHAIRMAN AJIT PAI Re: Use of the 5.850-5.925 GHz Band, ET Docket No. 19-308. `https://docs.fcc.gov/public/attachments/FCC-19-129A2.pdf`.

[18] Concorda. Connected Corridor for Driving Automation. `https://connectedautomateddriving.eu/project/concorda`.

[19] Donald Eastlake 3rd. RFC 6066, Transport Layer Security (TLS) Extensions: Extension Definitions. Standards track, IETF, Jan. 2011.

[20] ETSI. EN 302 665: Intelligent Transport Systems (ITS); Communications Architecture; V1.1.1. Standard, European Telecommunications Standards Institute (ETSI), 09 2010.

[21] ETSI. TS 102 731: Intelligent Transport Systems (ITS); Security; Security Services and Architecture; V1.1.1. Standard, European Telecommunications Standards Institute, 09 2010.

[22] ETSI. TS 102 942: Intelligent Transport Systems (ITS); Security; Access Control Technical Specification; V1.1.1. Standard, European Telecommunications Standards Institute, 06 2012.

[23] ETSI. TS 102 943: Intelligent Transport Systems (ITS); Security; Confidentiality Services; V1.1.1. Standard, European Telecommunications Standards Institute (ETSI), 06 2012.

[24] ETSI. TS 101 539-1: Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) Application Requirements Specification; V1.1.1. Standard, European Telecommunications Standards Institute, 08 2013.

[25] ETSI. TR 103 415: Intelligent Transport Systems (ITS); Security; Pre-standardization Study on Pseudonym Change Management; V1.1.1. Standard, European Telecommunications Standards Institute, 04 2018.

[26] ETSI. TS 102 940: Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management; V1.3.1. Standard, European Telecommunications Standards Institute, 04 2018.

[27] ETSI. TS 102 940: Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management; V2.1.1. Standard, European Telecommunications Standards Institute, 07 2018.

[28] ETSI. EN 302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, V1.4.1. Standard, European Telecommunications Standards Institute, 04 2019.

[29] ETSI. EN 302 637-3: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service; V1.3.1. Standard, European Telecommunications Standards Institute, 04 2019.

[30] ETSI. TR 103 460: Intelligent Transport Systems (ITS); Security; Pre-Standardization Study on Misbehaviour Detection; Release 2; V2.1.1. Standard, European Telecommunications Standards Institute, 10 2020.

[31] ETSI. TR 103 300-1: Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) Awareness; Part 1: Use Cases Definition; Release 2; V2.2.1. Standard, European Telecommunications Standards Institute (ETSI), 04 2021.

[32] ETSI. TS 102 941: Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; V2.1.1. Standard, European Telecommunications Standards Institute, 10 2021.

[33] ETSI. TS 103 097: Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats; Release 2; V2.1.1. Standard, European Telecommunications Standards Institute, 10 2021.

[34] ETSI. TS 103 300-2: Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) Awareness; Part 2: Functional Architecture and Requirements Definition; Release 2; V2.2.1. Standard, European Telecommunications Standards Institute (ETSI), 04 2021.

[35] ETSI. TR 103 949: Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS Migration Study, V1.1.1. Standard, European Telecommunications Standards Institute, 05 2023.

[36] ETSI. TS 103 300-3: Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) Awareness; Part 3: Specification of VRU Awareness Basic Service; Release 2; V2.2.1. Standard, European Telecommunications Standards Institute (ETSI), 02 2023.

[37] ETSI. TS 103 759: Intelligent Transport Systems (ITS); Security; Misbehaviour Reporting Service; Release 2, V1.1.1. Standard, European Telecommunications Standards Institute, 01 2023.

[38] Antonio E. Fernandez, Mikael Fallgren, and Nadia Brahmi. 5GCAR Scenarios, Use Cases, Requirements and KPIs. *Fifth Generation Communication Automotive Research and innovation, Tech. Rep. D*, 2, 2019.

[39] European Union Agency for Cybersecurity (ENISA). Pseudonymisation Techniques and Best Practices, Recommendations on shaping technology according to data protection and privacy provisions. `https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices/@@download/fullReport`, 11 2019.

[40] European Union Agency for Cybersecurity (ENISA). Deploying Pseudonymisation Techniques, The case of the Health Sector. https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques/@@download/fullReport, 03 2022.

[41] Laurent Gallo, Thierry Lejkin, Bruno Tossou, and Bernadette Villeforceix. Initial Design of 5G V2X System Level Architecture and Security Framework. *Fifth Generation Communication Automotive Research and Innovation, Tech. Rep. D*, 2, 2018.

[42] Michael Gardiner, Alexander Truskovsky, George Neville-Neil, and Atefeh Mashatan. Quantum-Safe Trust for Vehicles: The Race is Already On. *Communications of the ACM*, 64(9):54–61, 2021.

[43] Peter Gutmann. Engineering Security. https://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf, April 2014.

[44] Phillip Hallam-Baker. RFC 7633, X.509v3 Transport Layer Security (TLS) Feature Extension. Standards track, IETF, Oct. 2015.

[45] Dick Hardt. RFC 6749: The OAuth 2.0 Authorization Framework, Oct. 2012.

[46] Leping Huang, Kanta Matsuura, Hiroshi Yamane, and Kaoru Sezaki. Enhancing Wireless Location Privacy Using Silent Period. In *IEEE Wireless Communications and Networking Conference, 2005*, volume 2, pages 1187–1192. IEEE, 2005.

[47] IBM. IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two. https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two, Nov 2022.

[48] IEEE. IEEE Standard 802.11-2016 - IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Technical report, Institute of Electrical and Electronics Engineers, Piscataway, NJ, United States, 2016.

[49] Vehicular Technology Society IEEE Standards Association. IEEE Std. 1609.2.1-2020, Standard for Wireless Access in Vehicular Environments (WAVE) — Certificate Management Interfaces for End Entities. Technical specification, IEEE, 2020.

[50] ISO. Health Informatics — Pseudonymization. Standard ISO 25237:2017, International Organization for Standardization (ISO), 2017.

[51] ISO. Road Vehicles — Cybersecurity Engineering. Standard ISO/SAE 21434, International Organization for Standardization (ISO), 2021.

[52] ITU-T. Recommendation ITU-T X.509, Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks. Standard, International Telecommunication Union - Telecommunication, 2019.

[53] Jaehoon Paul Jeong, Nabil Benamar, Sandra Cespedes, Jerome Haerri, Dapeng Liu, Tae (Tom) Oh, Charles E. Perkins, Yiwen Chris Petrescu, Alexandre Shen, and Michelle Wetterwald. IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases, draft-ietfipwave-vehicular-networking-08.pdf. IETF draft, Internet Engineering Task Force, 03 2019.

[54] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L Montgomery, Dag Arne Osvik, Herman Te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768-bit RSA Modulus. In *Advances in Cryptology–CRYPTO 2010: 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings 30*, pages 333–350. Springer, 2010.

[55] Chengzhe Lai, Rongxing Lu, Dong Zheng, and Xuemin Sherman Shen. Security and Privacy Challenges in 5G-enabled Vehicular Networks. *IEEE Network*, 34(2):37–45, 2020.

[56] Brigitte Lonc, Alexandre Aubry, Hafeda Bakhti, Maria Christofi, and Hassane Aissaoui Mehrez. Feasibility and Benchmarking of Post-Quantum Cryptography in the Cooperative ITS Ecosystem. In *2023 IEEE Vehicular Networking Conference (VNC)*, pages 215–222. IEEE, 2023.

[57] John Preuß Mattsson, Ben Smeets, and Erik Thormarker. Quantum Technology and Its Impact on Security in Mobile Networks. *Ericsson Technology Review*, 2021(12):2–12, 2021.

[58] Tero Mononen, Tomi Kause, Stephen Farrell, and Carlisle Dr. Adams. RFC 4210, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP). Standards track, IETF, Sept. 2005.

[59] Michele Mosca. Cybersecurity in an Era with Quantum Computers: Will We be Ready? *IEEE Security & Privacy*, 16(5):38–41, 2018.

[60] Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams. RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Standards track, IETF, June 1999.

[61] National Institute of Standards and Technology (NIST). NIST Announces First Four Quantum-Resistant Cryptographic Algorithms. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms, 07 2022.

[62] Masahiro Oguchi and Masaaki Fuse. Regional and Longitudinal Estimation of Product Lifespan Distribution: A Case Study for Automobiles and A Simplified Estimation Method. *Environmental Science & Technology*, 49(3):1738–1743, 2015.

[63] The European Parliament and The Council of The European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council. *Official Journal of the European Union*, 679, 2016.

[64] Eric Perraud and Kurt Eckert. Test Case Definition and Test Site Description Part 1. *5G CroCo*, 2, 2019.

[65] Alexandre Petrescu, Nabil Benamar, Jerome Haerri, Jong-Hyouk Lee, and Thierry Ernst. Transmission of IPv6 Packets over IEEE 802.11 Networks Operating in Mode Outside the Context of a Basic Service Set (IPv6-over-80211-OCB)", draft-ietf-ipwave-ipv6-over-80211ocb-36.pdf. IETF draft, Internet Engineering Task Force, 04 2019.

[66] Andreas Pfitzmann and Marit Hansen. A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf, 2010.

[67] John Proos and Christof Zalka. Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves. *arXiv preprint quant-ph/0301141*, 2003.

[68] Han Qiu, Meikang Qiu, and Ruqian Lu. Secure V2X Communication Network Based on Intelligent PKI and Edge Computing. *IEEE Network*, 2019.

[69] SAE. J2735, Surface Vehicle Standard, V2X Communications Message Set Dictionary. Standard SAE J2735:2006, SAE International, 2006.

[70] SAE. J2735: Dedicated Short Range Communications (DSRC) Message Set Dictionary. Standard SAE J2735:2009, SAE International, 2009.

[71] SAE. J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. Standard SAE J3061:2016, SAE International, 2016.

[72] SAE. J2945/2: Dedicated Short Range Communications (DSRC) Performance Requirements for V2V Safety Awareness. Standard SAE J2945/2:2018, SAE International, 2018.

[73] SAE. J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. Standard SAE J3016:2018, SAE International, 2018.

[74] SAE. J2945/1: On-Board System Requirements for V2V Safety Communications. Standard SAE J2945/1:2020, SAE International, 2020.

[75] SAE. J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. Standard SAE J3061:2021, SAE International, 2021.

[76] SAE. J2735: V2X Communications Message Set Dictionary. Standard SAE J2735:2022, SAE International, 2022.

[77] Peter W Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM review*, 41(2):303–332, 1999.

[78] IEEE Computer Society. IEEE Std. 802.11p-2010, Standard for Information Technology - Telecommunication and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. Technical specification, IEEE, 2010.

[79] IEEE Vehicular Technology Society. Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Services. Technical specification, Institute of Electrical and Electronics Engineers, Piscataway, NJ, United States, 03 2016.

[80] IEEE Vehicular Technology Society. IEEE 1609.2a-2017, Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages Amendment 1. Technical specification, IEEE, 2017.

[81] Syrma SGS Technology. Automotive ECU: Core Component for Connected Cars. `https://www.syrma.com/ecu/`.

[82] Eric Verheul, Christopher Hicks, and Flavio D Garcia. IFAL: Issue First Activate Later Certificates for V2X. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 279–293. IEEE, 2019.

[83] Wikipedia.org. CAN Bus. `https://en.wikipedia.org/wiki/CAN_bus`.

[84] Wikipedia.org. Physical and Logical Qubits. `https://en.wikipedia.org/wiki/Physical_and_logical_qubits`.

[85] Takahito Yoshizawa and Bart Preneel. Survey of Security Aspect of V2X Standards and Related Issues. In *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 1–5. IEEE, 2019.

[86] Takahito Yoshizawa and Bart Preneel. Misbehaviour Reporting in ETSI ITS Standard Considered Broken. In *2022 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 144–150. IEEE, 2022.

[87] Takahito Yoshizawa and Bart Preneel. On Handling of Certificate Digest in V2X Communication. In *2022 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 160–165. IEEE, 2022.

[88] Takahito Yoshizawa and Bart Preneel. A New Approach to Pseudonym Certificate Management in V2X Communication. In *2023 IEEE Conference on IEEE Vehicular Networking Conference (VNC)*, pages 25–32. IEEE, 2023.

[89] Takahito Yoshizawa and Bart Preneel. Post-Quantum Impacts on V2X Certificates – Already at the End of the Road. In *2023 IEEE Conference on IEEE Vehicular Technology Conference (VTC)*, pages 1–6. IEEE, 2023.

[90] Takahito Yoshizawa, Dave Singelée, Jan Tobias Mühlberg, Stéphane Delbruel, Amir Taherkordi, Danny Hughes, and Bart Preneel. A Survey of Security and Privacy Issues in V2X Communication Systems. *ACM Computing Surveys (CSUR)*, 55(9):1–36, 2023.

[91] Takahito Yoshizawa, Dave Singelée, and Bart Preneel. A New Privacy Enhancing Beacon Scheme in V2X Communication. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology, LNCS 13140*, pages 139–151. Springer, 2021.

[92] Takahito Yoshizawa, Dave Singelée, and Bart Preneel. Certificate Revocation - Is There A Way Forward? In *submitted to Applied Cryptography and Network Security (ACNS 2024)*.

Part II

Publications

List of Publications

The following list itemizes the publications as the culmination of the research work toward the PhD. Only the relevant publications are included in this thesis as indicated by the page number under the reference. Others published during this period but not directly related to this thesis are mentioned with reference only.

International journals

1. Xiaoting Huang, Takahito Yoshizawa, Sheeba Backia Mary Baskaran, Authentication Mechanisms in the 5G System. Journal of ICT Standardization, Vol. 9, No. 2, pp. 61–78, 2021.

2. Takahito Yoshizawa, Dave Singelée, Jan Tobias Mühlberg, Stephane Delbruel, Amir Taherkordi, Danny Hughes, Bart Preneel, A Survey of Security and Privacy Issues in V2X Communication Systems. ACM Computing Surveys (CSUR), Vol. 55, No. 9, pp. 1–36, 2023.

    - See p. 79

3. Roozbeh Sarenche, Farhad Aghili, Takahito Yoshizawa, Dave Singelée, DASLog: Decentralized Auditable Secure Logging for UAV Ecosystems. IEEE Internet of Things Journal (early access), pp. 1–21, 2023.

International Conferences and Workshops with Proceedings

1. Takahito Yoshizawa, Bart Preneel, Survey of Security Aspect of V2X Standards and Related Issues. In 2019 IEEE Conference on Standards for

Communications and Networking (CSCN), IEEE, pp. 1–5, 2019.

• See p. 147

2. Takahito Yoshizawa, Sheeba Backia Mary Baskaran, and Andreas Kunz, Overview of 5G URLLC System and Security Aspects in 3GPP. In 2019 IEEE Conference on Standards for Communications and Networking (CSCN), IEEE, pp. 1–5, 2019.

3. Takahito Yoshizawa, Bart Preneel, Verification Schemes of Multi-SIM Devices in Mobile Communication Systems. In Proceedings of the 18th ACM Symposium on Mobility Management and Wireless Access (MobiWac), pp. 91–97, 2020.

4. Takahito Yoshizawa, Dave Singelée, Bart Preneel, A New Privacy Enhancing Beacon Scheme in V2X Communication. In Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, pp. 139–151, 2021.

• See p. 163

5. Takahito Yoshizawa, Bart Preneel, On Handling of Certificate Digest in V2X Communication. In 2022 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, pp. 160–165, 2022.

• See p. 181

6. Takahito Yoshizawa, Bart Preneel, Misbehaviour Reporting in ETSI ITS Standard Considered Broken. In 2022 IEEE Conference on Standards for Communications and Networking (CSCN), IEEE, pp. 144–150, 2022.

• See p. 199

7. Takahito Yoshizawa, Bart Preneel, A New Approach To Pseudonym Certificate Management in V2X Communication. In 2023 IEEE Conference on IEEE Vehicular Networking Conference (VNC), IEEE, pp. 25–32, 2023.

• See p. 221

8. Takahito Yoshizawa, Bart Preneel, Post-Quantum Impacts on V2X Certificates – Already at The End of The Road. In 2023 IEEE Vehicular Technology Conference (VTC), IEEE, pp. 1–6, 2023.

• See p. 245

9. Takahito Yoshizawa, Dave Singelée, Bart Preneel, Certificate Revocation - Is there A Way Forward? Submitted to Applied Cryptography and Network Security (ACNS), 2024

10. Takahito Yoshizawa, Bart Preneel, Open Questions in VRU Standards from Security and Privacy Perspectives. Accepted by IEEE Conference on Standards for Communications and Networking (CSCN), 2023

Publication

A Survey of Security and Privacy Issues in V2X Communication Systems

Publication Data

Yoshizawa, T., Singelée, D., Mühlberg, J. T., Delbruel, S., Taherkordi, A., Hughes, D., and Preneel, B. A Survey of Security and Privacy Issues in V2X Communication Systems. ACM Computing Surveys (CSUR) Vol. 55, No. 9, pp. 1–36, 2023.

Contributions

- Principal author.

A Survey of Security and Privacy Issues in V2X Communication Systems

Takahito Yoshizawa[1], Dave Singelée[1], Jan Tobias Mühlberg[2], Stéphane Delbruel[3], Amir Taherkordi[4], Danny Hughes[2], and Bart Preneel[1]

[1] KU Leuven, ESAT/COSIC, Leuven, Belgium
[2] KU Leuven, imec-DistriNet, Leuven, Belgium
[3] LaBRI, University of Bordeaux, Bordeaux, France
[4] Informatics Department, University of Oslo, Oslo, Norway

Abstract. Vehicle-to-Everything (V2X) communication is receiving growing attention from industry and academia as multiple pilot projects explore its capabilities and feasibility. With about 50% of global road vehicle exports coming from the European Union (EU), and within the context of EU legislation around security and data protection, V2X initiatives must consider security and privacy aspects across the system stack, in addition to road safety. Contrary to this principle, our survey of relevant standards, research outputs, and EU pilot projects indicates otherwise; we identify multiple security and privacy related shortcomings and inconsistencies across the standards. We conduct a root cause analysis of the reasons and difficulties associated with these gaps, and categorize the identified security and privacy issues relative to these root causes. As a result, our comprehensive analysis sheds lights on a number of areas that require improvements in the standards, which are not explicitly identified in related work. Our analysis fills gaps left by other related surveys, which are focused on specific technical areas but not necessarily point out underlying root issues in standard specifications. We bring forward recommendations to address these gaps for the overall improvement of security and safety in vehicular communication.

1 Introduction

1.1 Overview

Vehicular communication has gained momentum in the past years. It is expected that progress of this communication technology will have a major impact on the automotive industry and in particular on how vehicles are driven in society. Vehicle-to-Everything (V2X) communication is expected to bring numerous benefits. According to the assessment by National Highway Traffic Safety Administration (NHTSA) in the US [99], the adoption of Vehicle-to-Vehicle (V2V) technology is expected to improve the overall traffic safety by preventing 439,000 to 615,000 accidents, saving 987 to 1366 lives, and eliminating 537,000 to 746,000 property damage incidents per year. A report by the European Commission (EC) [11] states that the overall benefits of deploying Cooperative Intelligent Transport System (C-ITS) include reduced travel times, increased efficiency, reduced accident rates, and savings in fuel consumption.

The first standardized V2X technology is based on IEEE 802.11p (IEEE 802.11 Outside the Context of Basic Service Set (OCB) mode). In the US, the V2X system using 802.11 OCB mode is called Dedicated Short-Range Communication (DSRC) and its upper layer is called Wireless Access in Vehicular Environment (WAVE) as specified in the IEEE 1609 series and the SAE International (SAE) standard J2735 [117] (formerly the Society of Automotive Engineers). In Europe, ITS systems based on IEEE 802.11 OCB mode are called Intelligent Transport System G5 (ITS-G5), and its upper layer is referred to as C-ITS. Detailed descriptions of these standards and how they relate to each other are discussed in [135]. An overview of the V2X communication system is shown in Figure 1. V2X is a collective term which includes multiple communication modes:

- Vehicle-to-Vehicle (V2V): direct communication between vehicles.
- Vehicle-to-Infrastructure (V2I): communication between a vehicle and the infrastructure such as traffic light.
- Vehicle-to-Person/Pedestrian (V2P): between a vehicle and other road users such as pedestrians or cyclists.
- Vehicle-to-Network (V2N): between a vehicle and network entities via a mobile network base station.
- Infrastructure-to-Network (I2N): between an infrastructure and network entities via a mobile network.

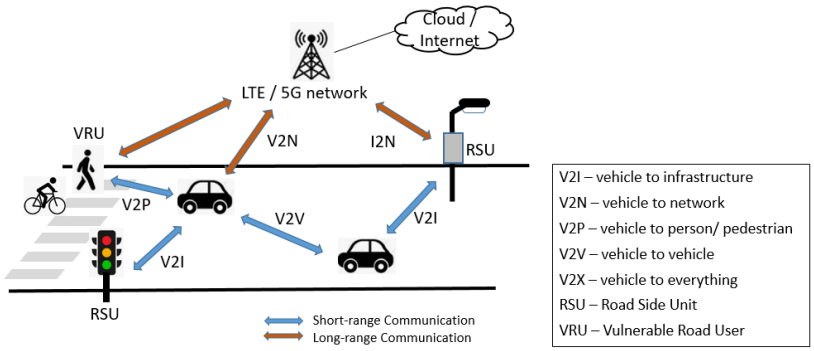


Figure 1: Overview of V2X Communication System

Meanwhile, modern vehicles are equipped with increasing number of Electronic Control Units (ECUs), embedded computers with the power to sense and actuate within the vehicle. Today, standard automobiles have more than 80 ECUs; luxury ones have as many as 150 ECUs [128, 93]. Their software size amounts to 100 million lines of code (LoC), far exceeding that of the space shuttle (400,000 LoC), F35 fighter jet (23 millin LoC) and even the Hadron Collider (50 million LoC) [129]. The increased complexity of vehicular ICT—ECUs, connectivity, overall software size—implies an overall increasing digital attack surface and thereby increasing security and privacy risks. Contrary to this point, the Controller Area Network (CAN) bus in vehicles does not support protection against cyberattacks; it does not support authentication and message integrity functionalities [96]. In fact, the CAN design is based on the assumption that it operates in a friendly environment where no security threats exist [14]. Yet, real-life attack scenarios around CAN communication and software defects in ECUs and their consequence as potential road hazard raise immediate concerns [82, 24, 94, 96]. Even if a relatively small number of vehicles on the road are directly affected by an attack, the consequences for road safety and national infrastructures can be devastating [133]. Therefore, vehicular communication technologies need to be secure, robust, and resilient to be truly beneficial. In this sense, including security and safety requirements from the initial stage of the system design is essential [96]. Ensuring secure communication requires at least mechanisms for authentication and integrity protection, which allows communicating parties to verify each other's identity, and the authenticity of messages: a vehicle is indeed a vehicle and a traffic light is indeed a traffic light, and communication between these entities cannot be spoofed or otherwise manipulated. In addition, protecting the *privacy* of vehicle owners is equally important. If no privacy protections are implemented on top of authenticated communications, vehicles can be tracked remotely,

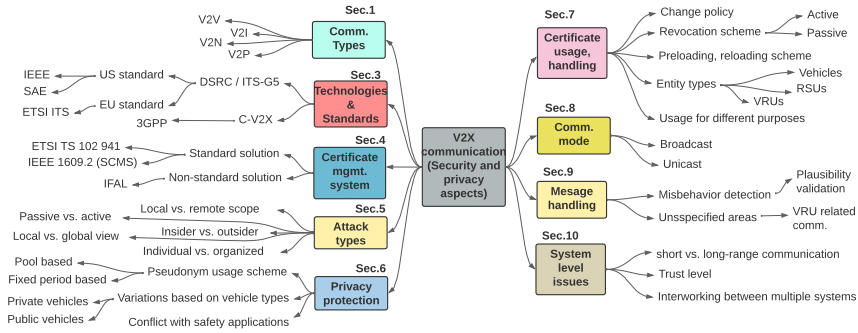


Figure 2: Overview of Security and Privacy Aspects in V2X Systems.

and information about drivers and their personal behaviour can be inferred by authorities, infrastructure operators and adversaries. In the V2X context, privacy-preserving technologies rely on the use of pseudonymous identities. These schemes come with their own security and safety challenges [116, 86], and a number of proposals to mitigate these challenges have been published [95, 18, 87], but not necessarily adopted by standardizing bodies.

This article surveys recent efforts in research and standardization regarding security and privacy aspects of V2X communication. We aim to provide a comprehensive overview of these aspects from the perspective of the ETSI ITS specifications, and link this to the objectives and results of recent research, development, and integration actions, specifically in the European Union but with links to other markets and political bodies. As a key contribution, our survey highlights a range of shortcomings and imprecisions in ongoing standardization efforts, and points towards potential solutions and open research questions regarding these security and privacy issues. As such, our article targets policy makers, researchers, and standardization engineers. Specifically for these actors, we provide the background to assess the novelty and relevance of research, and a medium to identify domains of research with a potentially high impact on upcoming standardization or regulatory efforts. Figure 2 gives an overview of these domains and links them to the structure of this article.

1.2 Methodology and Contributions

In this article, and in reference to related work summarized in Sec. 2, we focus on security and privacy aspects of European Union (EU) initiatives across a range of European pilot activities, such as past or present V2X-related EU projects,

and analyse ETSI ITS specifications from security and privacy perspectives. Our focus on EU standard and projects is due to several reasons: (1) Europe is the largest exporter of vehicles equipped with communication technologies as many major vehicle manufacturers are based in Europe, (2) covering relevant projects in other regions such as the US will diminish the focused analyses, and (3) including analysis of other regions will likely result in excessively long paper while adding relatively marginal additional benefit.

As a result, we identify a number of gaps in the ETSI ITS standards which stem from incoherent and inconsistent specifications. Based on our root cause analysis of the reasons and difficulties associated with these gaps, we provide recommendations based on our findings. We also identify previously unreported security and privacy issues resulting from recent trends driven by C-V2X such as the convergence of vehicular communication and mobile systems; one notable example being the absence of security and privacy considerations in the integration of smartphone in the ITS system in V2P scenarios. For many of these issues, existing literature offers either no solution or inadequate ones. When applicable, we propose ideas for potential solutions as an agenda for future analysis and investigation. We believe our findings are fundamental and essential to ensure that V2X communication is secure and protect user privacy.

We focus primarily on the EU initiatives in this paper. However, subtle but important contrast emerges as we put differences of the solutions between the EU and the US in perspective because the security and privacy solutions in two systems are similar in high level but different in details. For this reason, we discuss the similarities and differences between the two standards as the foundation of our discussion. When terminologies are different between the systems, we use the EU terminology unless it is necessary to explicitly describe the US system.

1.3 Document Organization

This paper is organized as follows. We first set a baseline of the discussion by summarizing the related survey papers and EU projects in Sec. 2, describing the overview of V2X technologies and their standards in Sec. 3. Then, we discuss their security management systems in Sec. 4. In Sec. 5, we discuss threat model that we use as a base of our analysis. Starting from Sec. 6 and up to Sec. 10, we examine details of specific security aspects and gaps. In Sec. 11, we present our root cause analysis of key gaps that need further study and research, and put forward recommendations. We conclude our study in Sec. 12. As a guide for the rest of this paper, Figure 2 provides an illustration of the various security and privacy protection-related aspects covered in this paper.

2 Related Work

We first review related work of V2X communication.[5] In the past years, a number of survey papers on security and privacy aspects of V2X have been published. The purpose of this section is to highlight the differences of our work compared to them. These survey papers can be categorized into three groups: ① discussion and solutions for generic vehicular network, ② surveys that cover both DSRC and C-V2X based solutions, and ③ surveys that focus specifically on C-V2X solutions.

In the first group, Hasan et al. [69], van der Heijden et al. [130], and Bißmeyer [15] exclusively focus on misbehaviour detection. In [69], a large part of this survey is dedicated to the discussion on attack and misbehaviour detection mechanisms by classifying and comparing numerous proposals on this subject. Survey in [130] provides in-depth analysis of detection mechanisms, and classify them into two-dimensions. The first dimension is *node-centric vs. data-centric*; the second dimension is *autonomous vs. collaborative*. Based on this classification, misbehaviour detection mechanisms can be categorized into one of the four types. The work in [15] focuses in two main areas: 1) misbehaviour detection, and 2) attacker identification in both local short-term and central long-term scope.

The survey by Badea and Stanciu [12] has a limited focus on security and privacy aspects. The only security related topic is on specific use cases and scenarios such as car sharing. Similarly, Ometov and Bezzateev [103] is not a survey; it is a proposal to apply multi-factor authentication (MFA) in V2X communication. This solution uses reversed Lagrange polynomial from Shamir's secret sharing schema as the building block. Wang et al. [134] focus specifically on the certificate revocation schemes in V2X communication. They analyse and classify them based on location where the revocation information has been placed. The entire revocation process is then divided into three stages: 1) resolution, 2) distribution, and 3) the use of revocation information.

In the second group, Huang et al. [72] treat both security and privacy topics although it is a small part of their paper as the content provides overview of 3GPP specifications on both LTE and 5G-based C-V2X rather than a survey. For security aspect, they discuss basic security services and attack types in vehicular networks, then categorize security solutions from two perspectives: 1) cryptography-based schemes, and 2) trust-based schemes. For privacy solutions, they categorize them into two types: 1) identity privacy preservation, and 2) location privacy preservation. Alnasser et al. [9] analyse security threats

[5] An extended version of this section is available in the online supplemental material, including both relevant survey papers and EU projects.

and solutions for both DSRC and LTE-based C-V2X. Their threat analysis includes availability, integrity, confidentiality, authenticity, and non-repudiation aspects. Then, they categorize security solutions including cryptography-based, behaviour/trust-based, and identity-based solutions. Ghosal and Conti [67] provide overview and background of both DSRC/WAVE and 3GPP-based LTE and 5G C-V2X systems, then discuss security challenges by analysing various attack types and how they impact V2X communication. Later, they examine techniques and solutions in specific areas, including symmetric key cryptography, privacy preservation, message authentication.

In the third group, Cao et al. [19] cover overall 5G system security and related topics rather than focusing on 5G-based C-V2X. They describe security and privacy aspects of other vertical applications such as IoT, device-to-device (D2D), and 5G-specific topics such as network slice. Only one section (Sec.VI) is dedicated to security in both LTE and 5G-based C-V2X solutions. In it, security requirements, solutions, and open issues are discussed. Muhammad and Safdar [95] focus specifically on the authentication mechanism in the context of LTE C-V2X. They enumerate attack types and describe their relevance and corresponding countermeasures. They discuss multiple proposed authentication solutions and analyse how they can meet the needs of C-V2X communication. Lu et al. [87] focus on security and privacy aspects of LTE and 5G-based C-V2X. Their survey is on challenges in trust, security, and privacy-related issues in C-V2X, followed by discussions on strategies to resolve them. The discussion in Lai et al. [85] rather narrowly focuses on a specific C-V2X scenario (platooning) rather than more general V2X communication. They propose security solutions, including privacy-preserving platoon group set up, distributed group key management, and cooperative message authentication. Marojevic [91] focuses on LTE-based C-V2X, discusses its threat scenarios, lists out associated security requirements, and proposes research directions to satisfy these requirements, along with the needs of further standardization to ensure security mechanisms are in place. In summary, the examined surveys can be characterized as follows:

- Analysis of relevant threat scenarios and attack types and their impacts to V2X communication,
- Discussion of issues, challenges, and requirements on specific security areas,
- Discussion on approaches and strategies to address stated issues and requirements,
- Description and comparison of existing proposed solutions on specific security areas,

- A new proposal on specific security or privacy area.

In contrast to these surveys, as articulated in Sec. 1.2, our unique contribution in this paper is to point out fundamental issues and gaps in the ETSI ITS standards and unreported security and privacy issues that have not been discussed in the existing survey papers.

3 V2X Technologies

In this section, we discuss the two competing V2X standards, the first one being specified by the IEEE and the second by the 3GPP. We introduce these two main competing standards and highlight their differences as we set the context of the standardization in order to explore their respective security aspects and how they differ further in our survey. The discussion on their shared features being out of scope of this survey, we recommend for readers desirous to explore this path a previous study by Yoshizawa et al. [135] focusing on the similarities of these two standards and possible hints on their cohabitation.

3.1 IEEE Standard

In 2010, IEEE approved the amendment IEEE 802.11p designed to standardize vehicular communication system. The following publication of the IEEE 802.11 standard in 2016 [29] incorporated the amendment IEEE 802.11p. This amendment also specifies a new operation mode dubbed *Outside Context of a Basic Service Set* (OCB) mode for each 802.11p compliant device to be set to. OCB mode does not need authentication nor association and the only parameter to set is the central channel frequency and the channel bandwidth to communicate. Overall, this amendment concerns the PHY and MAC layers for WLAN-based V2X communications. To build it up towards the applicative layer, the IEEE 1609 standard known as *wireless access in vehicular environments* (WAVE) was developed by IEEE, while in Europe the ETSI committee on *Intelligent Transportation Systems* (ETSI ITS) worked on top of IEEE 802.11p towards standardising applications and a security framework. There are two initiatives benefiting from this work: SAE [117] is known as *Dedicated Short-Range Communications* (DSRC), and ETSI ITS-G5. Both of them define the upper layer protocols that operate on top of the 802.11 OCB mode. The intended application is short-range communication sufficient for direct communication involving both V2V between vehicles and V2I between vehicles and *Road Side Units* (RSUs).

3.2 3GPP Standard

Since 2014, the 3rd Generation Partnership Project (3GPP) has worked on standardizing vehicular communication based on previously standardised 4G LTE, and later on included 5G mobile cellular connectivity. This standardisation effort begun with the Proximity Services (ProSe) functionality published in Release-12 which was originally designed for public safety communication. Later in Release-13, support of direct communication between vehicles (D2D) was added. To expand ProSe capabilities towards D2D communications in a cellular environment, a new interface called PC5 was defined in 3GPP TS 23.285 [2] for the LTE system. The equivalent functionality for the 5G system is in 3GPP TS 23.287 [4]. The PC5 interface, also denoted *sidelink*, facilitates a new communication path in addition to the existing *Uu* interface between the User Equipment (UE) and the base station (the terminologies in standard specifications for base station in LTE and 5G are *eNodeB* and *gNodeB*, respectively). This combination of short-range sidelink (PC5) and long-range *(Uu)* communications under the same system is considered complementary and enables a wide range of new types of use cases or services. This technological approach relying on 4G LTE or 5G V2X communications is combined under the 3GPP standard for Cellular V2X (C-V2X).

3.3 Differences between ITS-G5/DSRC and C-V2X

In this section, we highlight conceptual differences between the two competing key V2X standards. For the sake of clarity, the one carried by IEEE comprising IEEE 802.11 OCB mode along with DSRC/ETSI ITS-G5 will be designated using its ETSI denomination, i.e. ITS-G5, while the second defined by 3GPP will be specified under the term C-V2X.

Two Different Target Scenarios

The vehicular communication originally envisioned by the IEEE for the ITS-G5 was V2V where vehicles directly communicate with one another. Later on, communication that involves infrastructure, such as RSUs, was added. This type of communication is called V2I and in that scenario both V2V and V2I are designed from the point of view of the vehicle and its communications capabilities.

When the C-V2X concept emerged, it envisioned a scenario introducing two distinct new communication paradigms. One is the involvement of the cellular mobile network (V2N); the other is the involvement of pedestrians or cyclists

through the use of smartphones (V2P). The addition of V2N and V2P paradigms is a natural extension to vehicle communication in the context of cellular mobile networks as both short-range and long-range communications in the C-V2X are defined by the same standard body (3GPP).

Collectively, both ITS-G5-based systems and C-V2X-based systems use the term *V2X*. However, the target scenarios are different. In the first one, the focus is on short-range communications involving vehicles and RSUs. Within the context of ITS-G5-based systems, the *Intelligent Transport System - Stations* (ITS-S) consists of only two types: *On-Board Unit* (OBU) and RSU. Thus, only dedicated devices for ITS are envisioned to be part of the vehicular communication system. In this sense, the term *V2X* refers to V2V and V2I from the perspective of ETSI ITS-G5-based systems.

In the C-V2X-based system, inclusion of the mobile network (V2N) and pedestrians and cyclists (V2P) using a smartphone as a new type of ITS-S introduces new dimensions in the vehicular communication. Especially, introducing consumer devices within the family of ITS-S device types extend the range of communication options and use case scenarios. In this sense, the term *V2X* refers to V2V, V2I, V2N, and V2P from the perspective of C-V2X-based systems.

Specific Issues with ITS-G5

Several concerns have been reported regarding the use of ITS-G5/DSRC within the context of vehicular communication. For example, Klingler et al. [80] show that the use of unicast in IEEE 802.11p OCB mode leads to a *Head-of-Line blocking* as each unicast frame requires an acknowledgment from the receiving ITS-S. Absence of acknowledgment in unicast causes subsequent frames to be blocked from transmission, not only to a specific unicast communication but also to other outbound traffic from the ITS-S in question. To create this *Head-of-Line blocking* condition, only a minimally sophisticated attack is necessary as all it requires is to prevent the reception of an acknowledgment frame. Moreover, this condition can occur under the expected normal operating environment in vehicle communication where moving vehicles enters and exists other vehicles' communication range. This point implies that IEEE 802.11 OCB mode-based systems such as ETSI ITS-G5 and DSRC are suitable only for strictly broadcast-based communication in the V2X environment.

Another issue of with 802.11 OCB mode is the lack of reliability and performance in V2X environment. A formal analysis by Ma et al. [88] shows that 802.11 OCB based system is not able to guarantee high reliability due to potential frame collisions and severe channel fading condition. The exponential back-

off mechanism used in 802.11 to address frame collision and degraded radio condition has negative performance implications with increasing traffic load. This problem is pronounced further in dynamically moving vehicle environment. In addition, hidden terminal problem is more severe in broadcast than that in unicast. In other words, both broadcast and unicast modes have issues in 802.11-based systems in V2X environment. This is in contrast to the conventional WLAN environment where wireless devices are likely more static compared to vehicles moving at high speed. On the contrary, in mobile systems (e.g. 4G LTE) radio resource is managed by the network. While various cellular protocols use time slotting or time sync to prevent the above-mentioned performance issue, latency comes however at a price.

3.4 ISO Standard

International Standard Organization (ISO) specifies several vehicle-related standards. ISO 26262 [75] defines functional safety of electrical and electronic devices for the automotive industry. It adapts the International Electrotechnical Commission (IEC) 61508 standard, a functional safety standard that defines safety life cycle of electronic systems and products for all industries. It is a risk-based safety standard; vehicles assess the risk of possible hazardous situations and mitigate their impacts to avoid systematic failure of vehicles. It was first published in 2011 and was revised in 2018 [75] in which cybersecurity aspects are added in a limited scope by covering only the interface from functional safety to cybersecurity [121].

ISO/SAE 21434 [76] specifies cybersecurity standard for road vehicles. It started in 2016 as a joint work of ISO and SAE. It is based on SAE J2735 [117]; ISO/SAE 21434 defines a process and minimum criteria for cybersecurity engineering through all phases of product life cycle to prevent cyberattack on vehicles [89]. By complying to this standard, the whole automotive industry follows the uniform cybersecurity development process through the vehicle development life cycle. An analysis by Macher et al. [89] indicates that ISO/SAE 21434 leaves a gap as it stays at an abstract level and is not intended to provide answer to specific implementation details, methods, guidelines, or best practice, and does not present a “silver-bullet” per se. In addition, cybersecurity for autonomous vehicles and non-vehicles such as RSU are outside the scope of this standard.

ISO 39001 [77] is a management system standard for Road Traffic Safety (RTS). It was first published in 2012. Its goal is to improve organizations’ traffic safety, and it is targetted for organizations that have a process to improve traffic safety. Organizations that adhere to ISO 39001 can obtain certification of compliance.

4 Security Management System Overview

In this section, we first revisit the security related standards in both the EU and the US. Then we review the security management system defined in these specifications. Both the EU and the US systems are based on a Public Key Infrastructure (PKI) [7]. These ITS security management systems particularly focus on how to manage the certificates for the ITS-Stations (ITS-S). This section highlights the similarities and differences between security management systems in the EU and the US as a baseline for the discussion in the following sections.

4.1 ETSI C-ITS and IEEE 1609.2

The most notable security-related ITS specifications are listed in Table 1. The certificate management system adopted in the US is specified in IEEE 1609.2 [127]. It is called Security Credential Management System (SCMS). A comprehensive and detailed description of the SCMS is found in Brecht et al. [18]. The ETSI ITS standard covers a range of aspects across separate documents. Among them, ETSI TS 102 940 [52] defines the overall architecture of C-ITS security management system. Figure 3 illustrates the overall security management system and the relationship among the entities within the system, including the definition of reference points (e.g. S1, S2), following [52]. Key entities include:

- Root CA (RCA) — This entity is the root of trust of the entire ITS certificate management system. One or more RCA issues certificates to the EA and AA.
- Enrollment Authority (EA) — This entity accepts enrollment requests from the ITS-S and issues enrollment credentials that are used by the ITS-S to contact the AA.
- Authentication Authority (AA) — This entity verifies the successful enrollment based on the enrollment credential issued by the EA, and issues one or more Authorization Certificates, which is also referred to as an Authorization Ticket (AT). The AT is equivalent to a pseudonym certificate in general term.
- ITS Station (ITS-S) — This entity is the end device and the user of ATs issued by the AA. It includes multiple types of devices such as an On-Board Unit (OBU) in the vehicle, a Road Side Unit (RSU), and other types of devices that are engaged in the V2X communication.

Table 1: US and EU ITS Specifications (Security Specific)

Spec #	Title	Latest Version	Ref.
	US Specification (IEEE)		
IEEE 1609.2	IEEE Standard for Wireless Access in Vehicular Environments— Security Services for Applications and Management Messages	2016, January	[127]
	EU Specifications (ETSI)		
TS 102 731	Intelligent Transport System (ITS); Security; Security Services and Architecture	V.1.1.1, 2010-09	[43]
TS 102 940	Intelligent Transport System (ITS); Security; ITS Communications security architecture and security management	V.2.1.1, 2021-07	[52]
TS 102 941	Intelligent Transport System (ITS); Trust and Privacy Management	V.2.1.1, 2021-10	[56]
TS 102 942	Intelligent Transport Systems (ITS); Security; Access Control Technical Specification	V.1.1.1, 2012-06	[44]
TS 102 943	Intelligent Transport Systems (ITS); Security; Confidentiality services	V.1.1.1, 2012-06	[45]
TS 103 097	Intelligent Transport Systems (ITS); Security; Security header and certificate formats	V.2.1.1, 2021-10	[57]

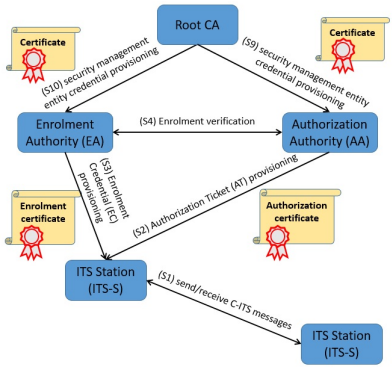


Figure 3: Overview of Security Management System

4.2 Differences between ETSI C-ITS and IEEE 1609.2

In this section, we describe differences in the security management systems between ETSI ITS and IEEE 1609.2 [127] (SCMS [18]).

Architectural Principles of Security Management

The SCMS architecture [18] ensures strong privacy protection of vehicle owners by enforcing strict separation of vehicle information and the network entities under different organizations. This architecture allows no single entity in the security management system to have access to information sufficient to identify a vehicle: identifying a vehicle in SCMS requires multiple management entities under different organizations to collude. To achieve this goal, this architecture includes purpose-specific entities such as Registration Authority (RA) and a pair of Linkage Authorities (LAs). This level of functional and ownership separation is beyond the extent of ETSI ITS certificate management system [52]. To achieve the similar level of functional separation in ETSI ITS as in the SCMS, extra design and implementation steps are required beyond the scope of the ETSI ITS standard.

Revocation of ITS-S Certificates

The SCMS supports *active revocation* of pseudonym certificates. *Active revocation* means that the certificate management system revokes the pseudonym certificates of a vehicle by issuing a Certificate Revocation List (CRL). The SCMS defines separate entities dedicated for this task, such as Misbehaving Authority (MA) and a pair of LAs. When a vehicle observes misbehavior of another vehicle, the former reports to the MA by including the latter vehicle's *linkage value* which is included in its pseudonym certificate. Then the MA determines whether misbehavior exists or not by correlating multiple reports and verifying the alleged misbehavior.

Upon confirming the positive misbehavior, the MA resolves the reported *linkage value* to two *linkage seeds* by contacting the Pseudonym CA (PCA), the RA, and the LAs. The MA contacts these three entities in a serial manner in this process as each entity has only limited information that collectively triggers the LAs to retrieve the correct *linkage seeds* of the to-be-revoked vehicle.

After the *linkage seeds* are obtained from the LAs, the MA creates an entry in the CRL by including the tuple of (*linkage seeds*, current time period, and the number of simultaneously active pseudonyms). As vehicles receive the CRL, they use this tuple and reconstruct a set of *linkage values* that correspond to all pseudonym certificates of the revoked vehicle. This way, vehicles can identify revoked certificates by comparing the *linkage value* within the certificate in the received messages against the values reconstructed out of the CRL. This way, the number of simultaneously valid certificates or future certificates preloaded

to vehicles does not impact the CRL size (cf. Sec. 7.3). We refer the reader to [18] for further details.

ETSI ITS does not define *active revocation* of certificates. Instead, it solely relies on a *passive revocation* mechanism. *Passive revocation* is accomplished by denying further allocation of certificates to a vehicle when the system determines that the vehicle needs to be revoked. This rejection occurs at the time when the vehicle attempts to obtain additional pseudonyms from the certificate management system.

Certificate Issuing and Usage Schemes

Annex 2 in the 5GCAR D4.1 document [65] describes the security architecture of the US and the EU certificate management systems. In the US system, the certificate management system (more specifically the RA and PCA collectively) generates three-years worth of certificates and preload them to a vehicle, containing 20 pseudonym certificates per week to a vehicle [18, 65]. This pseudonym size is derived from C2C-CC recommendation [16] as stated in SCMS [18].

An ETSI report on pseudonym change management in TR 103 415 [51] lists six different types of pseudonym management schemes. Given the nature of a pre-standard report, it does not yet specify exact details in this area. It indicates that the pseudonym pool size in referenced schemes varies between 10 to 100 depending on the scheme. The underlying mechanism is that a vehicle cycles through a set of certificates for a fixed duration of a week. The smallest size of 10 is the proposal from SCOOP@F project [122] and the largest pool size of 100 is the recommendation by EC's security policy and governance frame work [27] and certificate policy [28]. One exception is Issue First Activate Later (IFAL) scheme [131] which strictly uses only one pseudonym at a time without reuse.

Neither the aforementioned 5GCAR D4.1 document [65], SCMS [18], nor the ETSI ITS specifications [52, 56] explicitly specify the change period of one certificate from another within a one-week period. This period influences a vehicle's vulnerability to tracking and identification. Multiple schemes may be employed for this purpose; this period may be static for all vehicle types under all circumstances, or may vary depend on vehicle types and specific circumstances.

5 Attack Types and Threats

Before we discuss individual security and privacy-related issues in the subsequent sections, we first identify attack types and their resulting threats. Table 2 captures our view on this point. This table is not intended to be exhaustive; in fact, there may be new types of attacks we are not aware of today but become possible in the future. However, it is important to be cognizant to this important aspect.

Table 2: Attack Types and Threats

Attack types	Attack Description	Resulting Threats
Passive vs. *Active*	*Passive*: monitor communication channels and obtain information from it. *Active*: send disruptive messages to the communication channels or breaks in a system.	*Passive*: collected data can identify or trace vehicles. *Active*: disruptive messages may cause accidents, or intrude the system resulting in information loss or system malfunction.
Local vs. *Remote* scope	*Local*: passively monitor or actively send disruptive messages at a specific location to its immediate area. *Remote*: passively monitor or actively send disruptive messages to/from one or more remote locations.	*Local*: the scope and impact of data collection and disruptive messages is limited to a specific area only. *Remote*: the scope and impact of data collection and disruptive messages spans farther to wider areas.
Local vs. *Global view*	*Local view*: data collection in a limited scope, e.g. using a single or small number of devices in a limited area. *Global view*: data collection and aggregation from large number of devices in a wide area.	*Local view*: obtains traffic flow or pattern within a limited area. *Global view*: obtains traffic flow or pattern in a wide area, such as entire country.
Insider vs. *Outsider*	*Insider*: an employee of RSU infrastructure system steals data or disrupts its operation. *Outsider*: a hacker builds a device that sends messages as a fake vehicle, or breaks in a system.	*Insider*: loss or leak of data that are otherwise available only to insiders. *Outsider*: disruptive messages from a fake device cause negative consequence such as accidents.
Individual vs. *Organized*	*Individual*: a motivated hacker with limited budget and materials with an intent to disrupt communication. *Organized*: an organized group (e.g. nation state) with unlimited resources with large budgets, facilities, and materials with intentions to disrupt an enemy nation.	*Individual*: limited impact relative to the effect a single individual can cause, e.g. a small number of fake devices. *Organized*: more organized and larger-scale attacks possible using a dedicated infrastructure.

Different types of adversaries have different motivations and goals. An individual hacker may have fun out of disrupting society, and would likely be satisfied to see the resulting chaos in reality. On the other hand, a large organized crime

group may aim to disrupt peace in an enemy nation with an intention to cause chaos, physical and material damages, and panic. In both cases, adversaries' motivations and goals are related to the aspects of the CIA triad [33].

- Reduced confidentiality: as a result of compromising privacy of vehicle owners by tracking and identifying vehicles.
- Reduced system integrity: by making it untrustworthy, e.g. by introducing fake vehicles injecting false messages.
- Reduced system availability: by disrupting the objective to promote road safety, such as by creating denial-of-service (DoS) situation.

6 Security Issue: Privacy Protection

One of the goals of the security management system in V2X communication is privacy protection, i.e. protecting the vehicle owners' privacy as required by relevant regulations. In the EU, these are GDPR [107], Network and Information System (NIS) Directive [36], the Cybersecurity Act [6], and the ePrivacy Directive [106]. Thus, user privacy protection is a requirement for V2X communications. Privacy protection technologies aim to prevent attacks or to confuse attackers who attempt to track vehicles by intercepting communications or tracing V2X interactions. A range of privacy protection strategies have already been developed and partially standardized. It is important to ensure that these privacy-preserving approaches do not impede safety functions which rely on vehicular communications.

A key strategy to achieve privacy protection is to rely on periodically changing pseudonyms for all communication involving vehicles. To provide pseudonyms to vehicles, certificate management systems such as SCMS [18] have been designed for the US based on PKI [7] (cf. Sec. 4.2). The EU security architecture is based on the same approach. Privacy protection includes the following concepts as defined by Pfitzmann and Hansen [109]:

- Anonymity: *"Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set."*
- Pseudonymity: *"Pseudonymity is the use of pseudonyms as identifiers"*
- Unlinkability: *"Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the*

attacker cannot sufficiently distinguish whether these IOIs are related or not."

- Unobservability: *"Unobservability of an item of interest (IOI) means (i) undetectability of the IOI against all subjects uninvolved in it and (ii) anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI."*

Protecting the vehicle owners' privacy is a meaningful goal. However, there are several scenarios worth considering for the applicability of privacy protection. They appear to directly conflict with the privacy protection requirement.

6.1 Privacy and Vehicle Operation

Vehicles with no malicious intent store certificates from other vehicles as a part of their normal operation. How long vehicles store these certificates have implications on privacy of vehicle owners. Vehicles store other vehicles' certificates for several reasons. First, verification of sender's authenticity requires verifying the entire certificate chain from up to the RCA. However, messages may not necessarily contain all certificates in the chain. Therefore, once a vehicle obtains the entire certificate chain for a given AT, it needs to keep this set for future references. Second, some message types (i.e. CAM, cf. Sec. 6.4) do not always contain an AT in every message. This implies that receiving vehicles need to store a copy of this AT to verify the message integrity as long as the transmitting vehicle uses the said AT. Therefore, the difference between malicious and benign devices are subtle: presence or absence of malicious intent to use collected information. In this sense, privacy protection implicitly includes protection against benign vehicles also. We consider this is a fundamental constraint of the certificate-based message verification in broadcast-mode. This point raises a question: when does a benign vehicle deletes *old and stale* ATs that has been stored in it but no longer used due to, either the AT-owner vehicles changed their ATs, or they moved out of the communication range from the vehicle. Another question is a requirement to retain received ATs for forensics purposes, such as investigating accidents. If such requirement exists, it may vary in countries or jurisdictions, thus likely not a one-size-fits-all answer. In this respect, these questions are implementation-dependent matter. Differences in these aspects likely influence the privacy of vehicle owners as how long privacy-related information is stored in other vehicles. The ETSI standard does not address either of these questions, leaving as an open issue in the standard.

6.2 Applicability of Privacy 1: Vehicle Types and Usages

There are multiple types of vehicles on the road, and the privacy requirements are not likely to be applied to all of them uniformly. ETSI TS 102 941 [56] specifies the privacy requirements for ITS. However, it does not consider the option to apply different privacy measures depending on the vehicle type.

First, not all vehicles are privately owned. Some special vehicles and non-passenger vehicles are owned by a company rather than by an individual. Trucks, delivery vans, and taxis fall into this category. These vehicles quite often have a company name or a logo written on the vehicle's body. Even a privately-owned vehicles may have a name, an address, an email address, and a telephone number written on the vehicle's body if its owner has a private business to advertise. In this sense, many vehicles voluntarily forfeit the privacy information. Although drivers or vehicle owners wish to protect their privacy, it is an imbalance between volunteering visible information and a need to prevent *remote* tracking. Second, some special vehicles, such as police cars, ambulances, and public transportation (e.g. buses), belong to various levels of government or public entities rather than an individual. Hence, in this case, different level of privacy protection may apply for these vehicles while considering their minimum level of protection against tracking.

According to ETSI TS 102 941 [56], OEMs are expected to assign a canonical permanent vehicle ID to each vehicle at the time of manufacturing. This permanent ID is what the privacy protection requirement intends to protect by using pseudonyms instead. However, OEMs do not know for what purpose any given vehicle will be used at the time of manufacturing. For example, for the exact same type vehicles, one of them may be used by an individual owner; another may be used by a business to which no particular individual is associated with. The former case requires more strict privacy protection than the latter. Therefore, it is likely that we need to rely on other mechanisms to determine what level of privacy a given vehicle requires. This type of consideration is not given in the ETSI ITS specifications.

Another related aspect is the change of vehicle ownership. When a vehicle is sold in the second market, the privacy-related information of the previous owner stored in the vehicle needs to be erased. This includes data such as unused ATs, navigation history, and Bluetooth-paired smartphone. The sales process of second-hand vehicles needs to include the necessary procedure to erase these data. As vehicles can be sold by owners rather than by auto dealers, it should be a simple process to trigger it through vehicle's user interface (UI).

6.3 Applicability of Privacy 2: Non-Vehicle ITS-S

There are different types of ITS-S, most prominently the vehicles, and the road-side RSU. ETSI ITS TS 102 940 [52] describes the overall certificate management system. However; the standard [52] only considers a vehicle-centric view of the system; it has no description on the certificate management for RSUs as another type of ITS-S.

As discussed in Sec. 6.2, privacy requirements are intended to protect the privacy of vehicle owners as private individuals. However, RSUs do not have any private owner or person associated with it. Therefore, it follows that RSUs do not need pseudonyms. The fact that privacy requirements may depend on the ITS-S type is not considered in the ETSI ITS specifications. How pseudonym certificates are managed for RSUs, or whether they are necessary for RSU at all, is not specified. See the related discussion in Sec. 7.5.

6.4 Privacy and Cooperative Awareness

Cooperative Awareness Messages (CAM), as specified in ETSI TS 302.637-2 [53], share basic attributes of the vehicles on the road. These attributes include the vehicle's position, speed, direction, acceleration, vehicle length and width, vehicle type, etc. Vehicles on the road periodically transmit CAM messages to mutually establish and maintain situational awareness in the vicinity. At the same time, vehicles change their pseudonyms periodically to preserve privacy and prevent tracking, as specified by EN 302 636-6-1 [48]. They also need to change their MAC address at the same time (and its IPv6 address in case of IP-based communication). This simultaneous changes of pseudonym, MAC and IPv6 address prevents adversaries and other vehicles from linking consecutive pseudonyms by either the MAC or IPv6 address.

Despite this privacy-protection scheme, broadcasting vehicle information in CAM can reveal sufficient information for receiving vehicles to identify the transmitting vehicle. For example, if there are only a few vehicles in the distinctive positions relative to the receiving vehicle (e.g. one in front and another behind), then the receiving vehicle can correlate the CAM messages with the vehicle by comparing the received position information against its own position. In another example, if a received CAM message indicates the transmitting vehicle is 15-meter long and there is only one 18-wheeler truck in the vicinity, it is also trivial to correlate this message to that vehicle. In fact, study by Escher et al. [40] found that additional information such as vehicle size *"enormously improves"* the pseudonym linkage, allowing tracking of up to 80% of vehicles. Further, the number of vehicles in the vicinity plays an

important factor. This study concludes that the location privacy will decrease despite the change of pseudonyms.

Further, if vehicles collect and store pseudonym changes from vehicles based on relative position information, share and collaborate this information in a wider-scale, for example by uploading it in a cloud storage, real-time tracking of vehicle movement, such as city-wide level or even larger scale, would become possible. This way, vehicle tracking may become similar to what already exists in real-time flight and ship tracking maps such as in [63, 90].

In this way, simply transmitting CAM messages including position information and other attributes already helps a receiving vehicle to identify the transmitting vehicle, which leads to a possible compromise of the privacy of the vehicle owner. ETSI TS 102 940 [52] Clause 4.3.1.3 states: *"... it is necessary to ensure that the data cannot be linked to any individual so that no personally identifying information is leaked by the CAM service."* If we take this requirement text literally, the CAM message itself does not reveal the personally identifying information. However, the content in the CAM message provides information that certainly helps to violate the principle of privacy protection by linking the transmitted message and the vehicle that transmitted it.

One possible approach to mitigate this situation is to enforce strict one-time use of pseudonym. However, it still does not guarantee the unlinkability property if series of pseudonym changes are observed by and shared with multiple vehicles through the cloud storage. This approach also increases the required number of pseudonyms per vehicle; it will stress the management system to generate and deliver pseudonyms and vehicles to store them. The pseudonym change scheme as specified in standards requires further research.

6.5 Privacy vs. Road Safety

Privacy protection is at odds with road safety. Consider a simple scenario where there are multiple vehicles in a multi-lane road as shown in Figure 4. Vehicle A suddenly applied a brake which triggers the broadcast of an emergency electronic brake light (EEBL) message to the surrounding vehicles. The EEBL message is one of the De-centralized Environmental Notification Messages (DENM) as defined in ETSI TS 302.637-3 [54]. In this case, Vehicle B, which is directly behind Vehicle A, needs to brake immediately to avoid an imminent collision. This is an essential requirement to reduce the number of road accidents. However, due to the privacy requirements, TS 102 940 [52] states that the pseudonym used in DENM must be different (unlinkable) from the one used in CAM. This way, the message origin of the EEBL is kept anonymous and unobservable, meaning that Vehicle B is neither expected to know which vehicle originated this

EEBL message, nor can it determine whether a specific vehicle (e.g. Vehicle A) transmitted this message or not. Therefore, it follows that all vehicles not only cannot determine whether to apply its brake or not, but also making a wrong decision can make the situation even more dangerous, e.g. Vehicle D or G applying a sudden braking for no apparent reason. At the same time, all DENM messages, including EEBL, include position information of the transmitting vehicle according to the specification in ETSI TS 302 637-03 [54]. This is a contradiction to the privacy requirement (cf. Sec. 6.4).

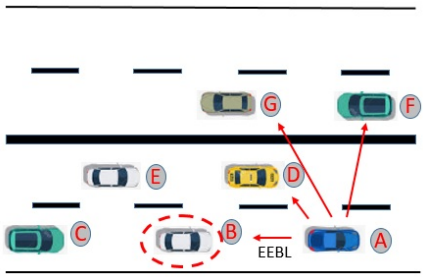


Figure 4: DENM and Privacy Requirement

This simple example illustrated above indicates that the privacy protection requirement is directly at odds with road safety. This leads to several issues:

- The privacy protection requirement hinders other vehicles to identify where a message comes from.
- Lack of this knowledge hinders surrounding vehicles to make right decisions to prevent an accident.

The analysis by Chator and Green [23] also identified these points in the security requirement in the ETSI ITS specifications; we agree with this analysis. Based on the discussion above, we conclude that the privacy requirement in ETSI ITS specifications needs to be reconsidered.

6.6 Privacy and Use of Unicast

Some use cases in the EU projects [30, 20, 21, 34, 5] are based on unicast communication between two endpoints. Some examples include remote driving or tele-operated driving use cases in the 5GCAR [61] and 5G CroCo project [108]. Unicast communication has an advantage over broadcast in that the former

can use confidentiality protection through encryption. This prevents passive observers from identifying the information transmitted by a vehicle. Although there are methods to apply confidentiality protection in broadcast, such as those proposed in [37, 66, 118, 68], the ITS specification (TS 102 943 [45]) does not require it to broadcast-based services such as CAM and DENM.

Despite the use of confidentiality protection, unicast communication conflicts with the privacy requirement. This applies to both internal and external threats. The internal threat refers to the leakage of private information between two endpoints of the communication; the external threat refers to the leakage of private information to another entity outside of these two endpoints.

First, we discuss the internal threat. If two entities establish a unicast communication, then by definition, both of them uniquely identify the other endpoint with the pseudonym, IP or MAC address of the other endpoint. In this case, applying a periodic pseudonym change is meaningful to protect the communication from eavesdroppers (i.e. protection against external threat). It makes it difficult for them to track unicast communication over a period longer than the pseudonym change cycle. However, it also means that the *linkability* of the old and the new pseudonym is voluntarily shared with the peer endpoint of the unicast communication. The peer vehicle can keep this information even after the unicast communication ends until the time that the vehicle changes its pseudonym again later. In addition, changing pseudonyms in the middle of unicast communication requires an explicit coordination between the two endpoints to maintain the communication. If this procedure fails for any reason, it can result in a negative consequence, such as a dropped communication.

The change of pseudonyms in unicast communication requires special handling, similar to Network Mobility (NEMO) in RFC 3963 [35]. It operates at the IP layer as described in ETSI EN 302 636-6-1 [48]. Therefore, an additional mechanism is needed to handle link layer address changes. 3GPP TR 33.836 [3] defines several variations of such explicit link layer address change notification. These schemes are workable solutions. However, as stated earlier, they fundamentally violate the *unlinkability* requirement between two endpoints in exchange for maintaining the unicast communication.

Second, from an external threat perspective, pseudonym changes in the ongoing unicast communication require confidentiality protection. Otherwise, it would be trivial for eavesdroppers to intercept the pseudonym change messages sent in clear and correlate the pseudonyms, hence violating the *unlinkability* requirement.

Another possible approach is simply avoiding the pseudonym change until the unicast communication is completed. This is especially meaningful if

confidentiality protection is not applied. In this case, both vehicles can change their pseudonyms as soon as the unicast communication ends. Doing so ensures that the *unlinkability* principle is maintained. This approach is also beneficial as it eliminates potential failure of pseudonym change and communication loss in the middle of unicast communication. Further consideration is needed to ensure reliable unicast communication while satisfying the privacy requirement.

7 Security Issue: Use of Certificates

Both the EU and the US systems are based on Public Key Infrastructure (PKI) [7] and use of certificates to manage the pseudonym usage. In this section, we focus specifically on aspects related to their usage. We will cover the actual issues and lack of definitions in the two competing standards (ITS-G5 and C-ITS) impacting certificate usage, renewal and revocation concerning vehicles, roadside infrastructures as well as pedestrians.

7.1 Certificate-Based Message Verification

In V2X communication, a certificate is attached to a message and receivers of this message use the public key in the certificate to verify the message's authenticity. The PKI in charge of managing certificates [7] requires that the receiving entity should be able to verify the certificate chain up to the root CA in order to verify the message authenticity. This is the underlying assumption of using certificates in real-time communication.

Contrary to this assumption, the real-time verification of the certificate may not be possible under all circumstances. It is especially the case in a dynamically changing communication environment involving moving vehicles in open space. For example, CAM messages do not always contain a certificate. CAM messages contain a certificate at least once a second. However, when they are sent more frequently, a *digest* (the least significant 8 octets of a hash output of a certificate) is added to replace a certificate. This use of *digest* enables a compact representation of a certificate without sending it in every CAM message. TS 103 097 [57] states that, if a vehicle receives a CAM message with unknown digest or a received certificate is signed by an unknown AA, then the receiving vehicle needs to resolve this situation by requesting the missing certificate to the surrounding vehicles and wait for a response (*inlineP2pcdRequest*). Only after this step, the vehicle can verify the validity of the received message. This additional message exchange causes delay in message verification in the order of several 100 milliseconds at least. This situation contradicts with the

underlying expectation to process vehicular communication in real-time under all circumstances. Due to these issues, message identification based on certificate verification as a mean to ensure authentication in V2X communications remains an open issue.

7.2 Certificate Usage and Change Policy

As discussed in Sec. 4.2, the certificate management in the EU issues a set of ATs per week [65]. ATs used in the V2X communication are expected to be changed periodically in the order of minutes. This implies that a set of ATs are reused multiple times during a specific one-week period. However, the exact duration of one AT and the mechanism to select the next one is not specified according to ETSI TR 103 415 [51]. If ETSI standard stops at the level of recommendations and leave details to implementations, there will likely be variations in terms of its effectiveness in preventing adversaries from predicting the next AT. In this sense, careful considerations are required as sub-optimal usage and change policy can lead to successful linking of the certificate to the vehicle. We also discussed the open issue of pseudonym usage and its implications on privacy protection in Sec. 6.4. Thus, it is an area that needs further consideration.

7.3 Certificate Reloading

Another area not specifically defined in the standard is the reloading of certificates. Under any circumstances, situations need to be avoided where a vehicle runs out of valid certificates, preventing that vehicle from sending messages altogether. Several research papers discuss certificate reloading schemes such as in [114]. These schemes use an RSU as an entry point to communicate with the AA. In these schemes, the underlying assumption is that an RSU is available whenever and wherever it is needed. However, RSUs may not necessarily be ubiquitous. Therefore, a universally workable solution is necessary so that legitimate vehicles can obtain new set of certificates without relying on the presence of RSU.

One possible approach is to store sets of certificates beyond the immediate period. Storing 3-years worth of certificates up front, as described in SCMS [18] and the 5GCAR D4.1 document [65], is one such approach. Such scheme, at least in theory, alleviates the reloading needs for the duration of three years. However, it comes at the expense of additional storage to hold this amount of certificates in the vehicle. Also, longer term storage of certificates complicates the system if they need to be revoked due to, for example, the vehicle being identified as malicious, or adversaries steal valid certificates from a legitimate

vehicle and use them for malicious purposes. Another consideration is handling of unused certificates when the vehicle is deregistered, or when the ownership is transferred to someone else.

Another possible approach is to reload certificates for multiple periods in the future, or request the next set of certificates well before the currently stored sets are exhausted – analogous to refilling the gas tank well before it is empty. For example, a vehicle stores sets of n consecutive weeks worth of certificates, and requests the next sets well before the end of the n-th week. This approach gives extra time in case network connection is not available at the first attempt to contact the AA. In this case, the vehicle can retry within the remaining time. This approach avoids potential exhaustion of certificates at the end of every one-week cycle, and does not require large storage capacity compared to storing 3-years worth of certificates. As of today, the challenge to propose a system ensuring a continuous flow of valid certificates while contextually relevant and memory efficient for V2X message verification remains open.

7.4 Certificate Revocation

Active Revocation

Active revocation of certificates is an area that is distinctively different between the US and the EU systems as previously discussed in Sec. 4.2. The US system based on IEEE 1609.2 [127] (SCMS [18]) supports active revocation of certificates while ETSI ITS does not. Active revocation involves two aspects: 1) detection, reporting, and validation of vehicle misbehaviour, and 2) generation and distribution of the CRL. As the first aspect relative to handling misbehaviours is discussed later in this paper, in this subsection we focus on the latter – CRL generation and distribution.

Management of the CRL, including its generation and distribution, is already challenging in a conventional PKI-based system [126]. Notable difficulties are guaranteeing the distribution of the CRL in a timely manner and keeping up with the scale of the distribution itself. It is even more challenging with moving vehicles. Because vehicles are assigned with a set of certificates valid for a limited period as discussed in Sec. 7.2, the number of certificates per vehicle significantly impacts the CRL size. This situation requires a technique to aggregate current and future certificates that belong to a vehicle and represent them in a compact manner for efficient distribution. The situation becomes even more prominent if a large sets of certificates are preloaded to the vehicle ahead of time, as discussed in Sec. 7.3. We previously explained in Sec. 4.2 that in order to address this issue, the SCMS describes the revocation scheme using

linkage value. It addresses one aspect of the distribution issues by reducing the amount of revocation-related information per vehicle. However, the CRL size is still a concern as the number of revoked vehicles increases over time. SCMS [18] does not address this aspect; it is most likely left as a deployment-level matter as it depends on the size of the vehicle population under a certificate management system.

Other issues of the revocation process remain open, especially the ones related to efficiently distributing the CRL. The main question on this issue is how to ensure the latest CRL is made available to vehicles in a timely manner. Even if the latest most up-to-date CRL is generated correctly, if it is not delivered to vehicles that need it when they need it, it is of little value. Online Certificate Status Protocol (OCSP) specified in RFC 6960 [120] is an alternative approach to the use of CRL. However, it does not solve the issue as OCSP suffers from the same issue of absence of guaranteed connection with the network under all circumstances [119].

The other related issue of CRLs distribution is their size versus the vehicle's storage capacity. Clearly, it is not realistic for a vehicle to store all revoked certificates of all vehicles. It is straightforward to consider that vehicles need to store CRL of vehicles that are *relevant* to them. By *relevant*, we mean related to vehicles that they may encounter on the road. There is no point of receiving and storing CRLs concerning vehicles that the receiving vehicle never comes across. However, how to determine the relevance is a matter of context for each individual vehicle. It depends on where a given vehicle drives, e.g. which country, region or province, highway or street, etc. Ideally, all vehicles that encounter a given revoked vehicle should be provided with the CRL containing the revoked certificates of that vehicle in question. If a vehicle misses a specific vehicle's certificates in its CRL and receives a message from this revoked vehicle, it does not know that it should reject all messages sent by this revoked vehicle. How to determine the relevance, or even the concept of CRL *relevance*, is not defined in IEEE 1609.2 [127] (SCMS [18]). Thus, it most likely falls in the implementation-dependent area. It is certainly not a trivial problem to solve, making it a possible further research area.

Previous research has been conducted on the subject of CRL distribution in V2X context proposing various schemes to make it efficient. Some of these schemes include: 1) splitting CRL in small pieces [79, 100], 2) distribution through RSU [105], 3) CRL dissemination in epidemic fashion [84], 4) use of Bloom Filter to reduce the CRL size [115]. Although these works include novel approaches to increase efficiency of CRL distribution, they do not address the *relevance* aspect we discussed.

Another issue related to CRL distribution is how to determine expired entries

and when to remove them to prevent the CRL size from growing indefinitely over time. Even if a vehicle is already de-commissioned and thus is no longer on the road, it does not necessarily mean that these entries can be removed from the CRL as it is necessary to prevent the situation where adversaries can steal valid certificates and corresponding private keys from such vehicle to pose as a legitimate vehicle. Although many research papers focus on the CRL distribution, there is little attention to this area. This is not a trivial question as it closely relates to the preloading and reloading of certificates (cf. Sec. 7.3), i.e. the longer the perloading and reloading period, the longer the entry needs to remain in the CRL. This is also an open question that the IEEE 1609.2 standard [127] needs to address.

Passive Revocation

As discussed in Sec. 4.2, the EU system does not require active revocation of certificates, thus relies solely on passive revocation. Passive revocation is a scheme based on a *blocklist*. A malicious or misbehaving vehicle is blocklisted. Thus, when a vehicle sends a request to reload certificates next time, the certificate management system denies the request if the requesting vehicle is on the *blocklist*.

One advantage of passive revocation is its simplicity as the certificate management system alleviates itself from the trouble of generating and distributing the CRL to vehicles. However, the disadvantage of relying only on passive revocation is the very nature of being passive. In other words, it leaves a time-gap between the time the system revokes a given vehicle and the time when the vehicle stops its communication. The latter occurs when either all certificates in the vehicle expires or it voluntarily stops communication as the result of rejection to request new certificates.

For example, if a vehicle stores only one week worth of certificates, it likely requests the next set for the following one-week period sometime toward the end of the current period – the timing in which the request is rejected if the vehicle is blocklisted. In worst-case scenario, this time gap can be up to 7 days. During this period, the vehicle continues to use its certificates; other vehicles certainly accept messages from this vehicle as valid. If the certificate reloading cycle becomes longer as the vehicle reload multiple weeks worth of certificates at a time, this time gap extends proportionally. Worse still, if the vehicle is preloaded with certificates for an extended period, such as 3 years, it does not request reloading for 3 years. This implies that certificate preloading for an extensive period is mutually exclusive with passive revocation approach. This

way, the simplicity of the scheme comes at a price. ETSI ITS specification does not address this issue, thus requires further consideration.

7.5 Certificate Management of RSUs

As discussed in Sec. 6.3, RSUs do not require privacy protection and thus does not require the use of pseudonyms, strictly speaking. However, the certificate management system described in ETSI TS 102 940 [52] does not address these types of ITS-S or if any specific certificate management different from privately owned vehicles is required at all. This is another open area that needs to be addressed in the standards.

It may be necessary for vehicles to uniquely identify a specific RSU from another while still maintaining its anonymity. One possible approach is to assign pseudonyms with longer validity periods than those for vehicles, such as days, weeks, or months depending on how static the RSU pseudonyms can be. The similar principle may apply to non-privately-owned vehicles such as emergency vehicles. On the other hand, longer validity period negatively impacts revocation of such ITS-S types. For example, if an adversary hacks an RSU, steals its pseudonym certificates and corresponding private keys, and uses them on a fake RSU, this fake device can send legitimate messages for longer period than privately-owned vehicles. This situation is further pronounced in EU systems where it relies solely on *passive revocation*. Therefore, a good balance needs to be achieved in order to minimize negative impacts from such situations.

7.6 Certificate Management of VRUs

The EU projects related to V2X communication define various use case scenarios [97, 61, 132, 108, 92]. These projects are under 5G-PPP, thus their technology focus is naturally on C-V2X as opposed to ITS-G5. Many of the use cases captured in these documents involve new and unique aspects in C-V2X compared to ITS-G5. One example is Vulnerable Road Users (VRU). VRU refers to pedestrians, cyclists, other human or non-human road users [55]. Inclusion of scenarios involving VRUs extends vehicular communication and contributes to further improvement of the road safety. In 2010, ETSI EN 302 665 [41] defined handheld devices, or *personal ITS-S*, as one of the ITS-S types. However, subsequent ETSI specifications focused exclusively on vehicle-centric view only. In this respect, increasing interest of VRUs due to the emergence of C-V2X was the trigger to start standardization work specific to VRUs. In fact, between 2019 and 2021, ETSI published TR 103 300-1 [55], TS 103 300-2 [58], and

TS 103 300-3 [59] which exclusively address VRU-related use cases, define functional architecture, and specify VRU basic service, respectively. The second specification [58] covers security-related issues. However, its content stays at the analysis level and leaves many issues open. The last one [59] specifies VRU Awareness Messages (VAM). It covers security aspects. However, the extent of its scope is limited; it does not define mechanisms and procedures such as enrolment of VRU devices and VRU-specific certificate policy including provisioning and usage of pseudonym certificates. In fact, it states that these areas are outside the scope of this specification (cf. clause 6.5.4 in [59]).

The above situation also means that the VRUs (handheld devices) as a type of ITS-S were not originally envisioned as a part of the certificate management system defined in ETSI TS 102 940 [52], and it is still the case today. In fact, we have already pointed out in Sec. 6.3 that the existing management system [52] is strictly vehicle-centric view only. This situation raises several points: 1) inclusion of VRU as a type of ITS-S, including certificate management of VRUs, 2) definition of a certificate management back-end system for VRUs, equivalent for vehicles as in clause 7 in [52].

Including the VRU as a type of ITS-S has several implications. VRUs use smartphones to communicate with other ITS-S, such as indicating pedestrians' presence to nearby vehicles. This obviously means that smartphones, as a type of ITS-S, need to become legitimate members in the V2X communication system, including provisioning and usage of pseudonym certificates as in vehicle ITS-S. Because the coupling between a human user and his or her smartphone is even tighter than that of vehicles, even higher level of privacy protection is required for VRUs. In addition, if a specific VRU device needs to be revoked for any reason, appropriate mechanism needs to be in place to ensure that it is excluded from the V2X communication. Introduction of smartphones can serve as an easily-accessible potential new attack surface to the whole V2X communication system. As these consumer products are readily accessible than vehicle OBUs, the threshold is lower for adversaries to develop a malicious software on an open-source-based OS (e.g. Android) using available open-source software development tools – picking up a smartphone and plugging in a USB cable to it is far easier and trivial than opening a part of a vehicle's dashboard, exposing a connection to the CAN bus and connecting to it. Hacking a vehicle OBU requires extensive knowledge, both mechanical and electronical, of vehicle's construction. In this sense, the above-mentioned VRU-specific specifications [55, 58, 59] fall short from addressing these aspects, leaving them as open issues.

One possible approach is to define a distinct ITS management system for smartphones separate from vehicles and RSUs. Separately manage smartphones likely simplifies the certificate management by isolating specific characteristics

and aspects unique to them. One such example is the potential needs to interact with Mobile Network Operators (MNOs) if verification of the subscriber information is required before admitting the device as a legitimate member of the ITS system. At the same time, this separation of management also implies that an interconnection is needed between these two types of ITS-S management systems. In addition, multiple MNOs may be involved to accommodate subscribers of different MNOs, including MNOs of other countries to address roaming scenarios.

7.7 Certificate Usage in Multiple Communications

It is likely that vehicles are engaged in multiple different types of communication with different entities for different purposes simultaneously. For example, a group of trucks in a platoon communicates with one another to coordinate their movement while maintaining safe driving distance with adjacent trucks within the platoon. In this case, these trucks likely use either unicast or multicast (groupcast) mode of communication rather than broadcast mode. At the same time, these trucks also broadcast basic service messages such as CAM to other surrounding non-platoon vehicles. The intended target and purposes of these messages are different.

In this case, it makes sense to use different pseudonyms for different purposes. This approach also aligns with the privacy protection perspective as one pseudonym used for broadcast mode does not reveal the pseudonym used for unicast mode. This way of pseudonym separation is likely to be beneficial, especially because broadcast mode does not provide confidentiality protection from observers (cf. Sec. 8.1). Such separation of pseudonym usage enhances the security of V2X communication.

ETSI specifications EN 302 636-1 [46], EN 302 636-3 [47], EN 302 636-4-1 [49], EN 302 636-6-1 [48] discuss the use of multicast in GeoNetworking. They discuss security-related functionalities, such as authentication, authorization, integrity, privacy, and non-repudiation. However, they do not mention confidentiality especially in the context of user-plane traffic. Thus, encryption is not applied in multicast mode user traffic in GeoNetworking. Therefore, the vulnerabilities of multicast and broadcast traffic are at the same level. On the other hand, separate use of pseudonyms in unicast has a value as it can apply encryption, thus worth exploring this usage (cf. Sec. 8.2). However, it is not specified in these GeoNetworking related specifications and other key security-related specifications, such as TS 102 637-1 [42], TS 102 940 [52], or TS 102 941 [56]. As such, it embodies an interesting open challenge.

8 Security Issue: Communication Modes

8.1 Broadcast-Oriented Communication

The basic services provided by V2X communication includes CAM and DENM as defined in ETSI TS 302.637-2 [53] and TS 302.637-3 [54], respectively. These messages are broadcast to the surrounding vehicles. Broadcast messages, by definition, are sent to any and all entities within the communication range. This is in contrast to unicast or multicast messages, which are sent to a specific endpoint or a known group of endpoints. The very nature of the broadcast is that the transmitting node is not concerned with the number of receiving entities within the communication range and their identities. It is further aggravated with the dynamic topology changes due to moving vehicles. Therefore, a set of vehicles within a communication range of a vehicle are in the constant flux depending on the density and the relative speed differences. Another characteristic of broadcast messages is the absence of confidentiality protection as specified in TS 102.943 [45]. Therefore, any entity with a suitable equipment can receive these messages.

These two points are significant from a V2X communication perspective because any passive observer with a suitable device can receive, collect, and analyse CAM and DENM messages. The receiving entity can verify the message authenticity and integrity by using the certificate contained in the message itself. Due to the use of periodically-changing pseudonyms and the unlinkability property from the privacy protection requirement, it is not trivial to identify the transmitting vehicle. However, a passive observer can still detect and recognize the existence of a specific pseudonym in the vicinity just by observing messages. This way, the broadcast nature of the basic messages has no or little protection from persistent observers to collect messages and detect long-term patterns of any given vehicle. This is an area of concern from a privacy protection perspective.

8.2 Unicast – Confidentiality Protection

Applicability of Confidential Protection

Confidentiality protection applies to unicast mode only. On the other hand, basic services are based on broadcast mode as discussed in Sec. 8.1. This is captured in Table 2 in ETSI TR 102 893 [50]. Unicast-based communication is rather a minority in V2X communication and is limited to specific use cases. In other words, confidentiality protection is applicable to a rather small portion of V2X communication where unicast is used. The 5GCAR D4.2 document in [64]

expresses a concern of the sole reliance on the PKI system [7] for security and privacy of V2X communication. A proposed scheme in [64] introduces a new entity called *key manager* that generates symmetric keys for encryption. The proposed scheme is a step towards introducing an additional security mechanism. However, it overlooks the fact that the confidentiality protection is applicable to unicast mode only. Thus, it has limited applicability in V2X communication.

Usability of Unicast Communication

The use of unicast in V2X communication is likely an IP-based communication to support value-added services. ETSI TS 102 941 [56] states that the use of IPsec or TLS is assumed for the confidentiality protection in unicast. The use of IPsec or TLS implies a notion of a *session* between two endpoints. Security Association (SA) establishment involves a handshake procedure which is an important factor to consider in a V2X communication environment where the vehicle topology changes constantly and dynamically.

The same characteristic of dynamic topology change as discussed in Sec. 8.1 equally applies to unicast communication. The communication range of DSRC is expected to be 300 meters [17]. Then, depending on the relative speed and direction of vehicles, the communication between two ITS-Ss can be short-lived in the order of seconds. For example, if we assume communication between an RSU at a fixed location and a vehicle moving at 120 km per hour, the communication lasts only 9 seconds. In the case of vehicles moving in the same direction, the communication between them may last longer. For example, if the relative speed difference of two vehicles is 10 km/hour, then the period they are within the communication range is 108 seconds, assuming a 300-meter range. Obviously, as the relative speed difference increases, the time duration shortens proportionally. Whether this time period is meaningful to establish an SA between two vehicles or not depends on the use cases and scenarios in which unicast communication is used.

A prime example where the use of unicast makes sense is when one of the endpoints is a remote entity over the long-range communication (V2N), such as remote driving discussed in Sec. 6.6. In this case, the vehicle's location or speed is not a factor. However, this is a rather value-added use case beyond the basic service. Strictly in V2V scenarios, a group of trucks in a platoon is one example where unicast communication makes sense as they move in the same direction with short inter-vehicle distance for extended duration. However, in other situations of V2V or V2I communication, in the worst case, vehicles may go out of the communication range as soon as an SA is established, rendering

SA establishment a moot point. It is worthwhile for the ETSI ITS specification to include a guidance on the usability of unicast in V2X communication.

9 Security Issue: Message Handling

9.1 Plausibility Validation and Misbehavior Detection

The concept of plausibility is present in different security aspects of V2X communications as specified in ETSI TR 102 893 [50] and EN 302 636-4-1 [49]. The idea of validation via plausibility, and why it is necessary in vehicular communication, is intuitively clear. A receiving vehicle needs to detect and reject bogus messages transmitted by an entity with a malicious intent to cause an accident or a road hazard, or to reject faulty messages transmitted by a vehicle with malfunctioning sensors. In this sense, plausibility validation is one of the key countermeasures to prevent potential threats in vehicular communication. There are two distinctive elements in the plausibility validation: 1) plausibility determination, and 2) misbehavior detection.

Determination of Plausibility

ETSI TR 102 893 [50] clause 11.3.20 states: *"Plausibility checks are non-cryptographic measures which use rules and other mechanisms to determine the likelihood that received data is correct. These rules and mechanisms range from simple heuristics to quite sophisticated and more complex, methods."* Also, clause B.4.5.3.2 in ETSI TR 102 893 [50] describes suspicious behaviors as *"any behavior that does not comply to expected behavior, based on direct evidence and probabilistic models."* It lists examples such as spurious and bogus packets. A spurious packet contains a proper signature but flawed payload; a bogus message contains a flawed signature. These definitions in the standard describe the intent of what plausibility check aims to accomplish, but it lacks clarity in terms of what qualifies as a good or valid plausibility check. Plausibility in V2X communication revolves around the idea of determining whether a given received message from another entity is reasonably genuine and thus should be accepted as valid. This level of message validation is above and beyond the verification of message integrity using digital signature.

Judging the plausibility of received messages may involve a number of contextual factors, such as: 1) location, 2) vehicle's mobility (e.g. position, speed, and direction), 3) environment (e.g. local street or highway), 4) time of the day (e.g. rush hour or last night), and 5) other conditions (e.g. weather). However, these

definitions in the standard are too abstract to be usable in reality to identify messages that do or do not conform to a given criterion. In other words, a more concrete and unambiguous definition is needed with respect to what constitute a set of criteria usable for plausibility validation. In addition, plausibility check needs to occur in real-time with high confidence to process time-critical messages such as DENM, which requires urgent and timely reaction such as an indication of an approaching emergency vehicle. In this sense, the result of plausibility validation determined too late or with less than 100 per cent confidence is either useless or may even result in an undesirable consequence.

Not defining a set of criteria for plausibility validation implies that it is left up to individual implementations on how it is accomplished. Such situation will most likely results in variations of coverage and effectiveness among them, where some of them better secure operational abilities than others in practice. Clearly, such situation is undesirable. However, establishing such criteria has a number of benefits such as:

1. Unambiguously defining how vehicles should behave under specific situations,
2. Minimizing variation of implementations so that all vehicles on the road will have uniform and predictable behavior under the same situation,
3. Enabling OEMs to evaluate their implementations during development cycle for validation and improvement,
4. Raising consumer confidence for successful adoption of the V2X technology in the market.

While this is arguably a difficult area to standardize, possible definition of common criteria is worth pursuing in standards given the potential benefits. One possible approach is to define a common *minimum set* of criteria that all OEMs must comply in their implementations. It can be done by defining a set of scenarios, associated with expected plausibility judgement and behaviour by vehicles. If a given OEM chooses to enhance its implementation with additional scenarios, it can be a differentiator from other OEMs without affecting the standardized set of scenarios.

Misbehavior Detection

Misbehavior detection is closely related to plausibility validation. They are two sides of the same coin. Detecting misbehavior implies detecting and analyzing patterns of plausibility validation failures on messages from another entity over

time. Most likely, a single plausibility failure does not constitute a positive misbehavior detection. It requires continuous evaluation over time to determine if a misbehavior condition exists or not to reach reasonable level of confidence. Studies by van der Heijden et al. [130] and Ambrosin et al. [10] provide good basis for various approaches toward misbehavior detection. Especially, the analysis in [130] captures a comprehensive overview and in-depth analysis of many misbehavior detection mechanisms. It analyzes and categorizes various mechanisms and classifies them into two dimensions, resulting in four categories.

The two dimensions described in [130] are: 1) *node-centric vs. data-centric*, and 2) *autonomous vs. collaborative*. The first dimension concerns with whether focusing on transmission patterns of a specific entity or analyzing data irrespective of the transmitting entity. The second dimension concerns with whether misbehavior detection is done locally within a node or as a result of exchanging information with other nodes. The resulting four categories are:

- *Behavioral* (*node-centric* and *autonomous*)
- *Trust-based* (*node-centric* and *collaborative*)
- *Plausibility* (*data-centric* and *autonomous*)
- *Consistency* (*data-centric* and *collaborative*)

Each of these four categories is based on certain conditions and assumptions. Thus, none of them is universally applicable under all circumstances. For example, *collaborative*-based models (i.e. *trust-based* and *consistency*) imply that there are multiple vehicles in the area with which a vehicle can exchange information with to make an assessment on a specific vehicle. If there is not sufficient number of vehicles in the immediate area or not enough data is available to reach a conclusion, mechanisms in these categories are not effective. Another aspect of *collaborative* category is the concept of *honest majority* – an assumption that the majority of the vehicles are honest and provide genuine information. However, if there is a small proportion of malicious entities or vehicles with faulty sensors providing incorrect data, it can skew the final decision on a vehicle in question.

The *autonomous*-based models (i.e. *behavioral* and *plausibility*) solely rely on data within a vehicle. Therefore, the assessment and the decision of whether a given vehicle is misbehaving or not is necessarily limited to the information within the vehicle. The vehicle may reach a different decision if it has information other vehicles may have but does not locally. In this respect, combinations of all 4 categories is likely necessary to cover all possible scenarios and to gain confidence in the misbehavior detection. This is another area that needs further

study. Ideally, a single solution that covers all possible situations is desirable. So far, the analysis in [130] indicates this is not the case.

Similar to plausibility validation, misbehaviour detection will likely result in different levels of effectiveness if it is left up to implementations. Defining a common approach or common test set to evaluate different implementations is worthwhile to guarantee uniform detection of misbehaviour. As discussed in Sec. 9.1, the same approach to standardize a common criteria will be helpful to achieve the same benefits for misbehaviour detection.

9.2 Communication involving Vulnerable Road Users

As discussed in Sec. 7.6, emergence of C-V2X introduces new use cases involving VRUs. They relate to the safety of road users other than vehicles such as pedestrians and cyclists who uses smartphones as a type of ITS-S. VRU-related messages include communicating presence and movement of pedestrians or cyclists to vehicles, or vice-versa. TS 102 300-3 [59] specifies VAM; these messages enable VRU devices to communicate its position and movement with vehicles or other VRUs to improve road safety. Specifying these messages is a step forward to achieve this goal. However, this specification hints that more work is needed. Informative annex G in this specification gives a glimpse into unique issues and difficulties associated with VRU scenarios. It has to do with the unpredictable nature of pedestrian's movement compared to that of vehicles. One example is the transition from a pedestrian to a cyclist, and vice-versa, and how VAM messages accurately reflect this transition (e.g. VRU profile to change from a *pedestrian* to a *cyclist*). This annex indicates that these transitions are not a trivial problem to solve, thus requires further research and standardization.

10 Security Issue: System Level Issues

10.1 ITS-S Device-Dependent Trust Level

ITS-S consists of different types of devices. Vehicles are manufactured by OEMs and a large proportion of them is owned and used by private individuals. On the other hand, RSUs are special type of devices owned and managed by government authorities, and they are installed at fixed locations on a permanent basis. In this sense, it may make sense to differentiate the level of trust for vehicles and RSUs. In other words, the trust level for RSUs can be higher than vehicles and treat messages differently based on the message source. It implies that

receiving vehicles need to distinguish message sources, at a coarse level such as *RSU-type* or the *vehicle-type*. Such differentiation does not compromise the privacy requirement (anonymity property).

In addition, such device type-level identification has benefits. For example, trusting messages from RSUs may be useful in addressing new approaches in plausibility validation or misbehaviour detection discussed in Sec. 9.1. One possible approach to address misbehaviour detection is to have intelligence in RSUs to collect and analyse data sent by vehicles, and integrate data from other RSUs at the back-end system to detect positive misbehaviour of vehicles. Then, this information can be distributed to vehicles in the area as an *authoritative information*, which can only be sent by RSUs. A survey by Wang et al. [134] discusses this concept as one of the approaches of certificate revocation by considering RSUs as an Intermediate Authority (IA). The concept of *authoritative information* is somewhat akin to distributing CRL from the PKI system. The certificate definition in IEEE 1609.2 [127] includes `SubjectAssurance` which can fit for this purpose. However, it also states that the exact content definition is outside its scope. This is another area for further research.

A potential issue of this approach is an abuse of trust level if adversaries can compromise an RSU and modify its behaviour. However, protection against unauthorized tampering with malicious intent is a general issue that applies to all ITS-S types. Thus, it falls into the issue of hardening devices against such attacks. Specifically, TS 102 940 [52] recommends the use of HSM as a solution.

10.2 Interconnection between Multiple Security Management Systems

A vehicular communication system involves government authorities that manage RSUs embedded in traffic lights and other road infrastructure that communicates with vehicles. This system also manages certificates to vehicles as specified in ETSI TS 102 940 [52]. However, it is not just one management system, but multiple systems. A security management system most likely exists per appropriate geographical domain that has authority over specific jurisdiction. Depending on the deployment of the system, there may be one such management system at the national level, state or provincial level. It is up to individual country and its relevant authority to determine how this management system is owned and managed.

If we consider the certificate management system as described in ETSI TS 102 940 [52], each vehicle is expected to belong to one such management system.

However, vehicles on the road likely belong to different such management systems. For example, highways in any given EU country are used by vehicles from multiple countries in addition to local vehicles. The above point implies that there needs to be an interaction between multiple management systems.

The following examples illustrate the relevant scenarios. As the first example using Fig. 5, we consider a scenario where a vehicle (V_{A1}) from Country A travels to Country B (event 1). During its stay in Country B, V_{A1} is involved in a minor accident that causes some of the sensors to malfunction. As a result, V_{A1} starts to report inaccurate or incorrect events and generates faulty messages to surrounding vehicles. In this case, a local vehicle (V_{B1}) in Country B determines a misbehavior condition of V_{A1} and reports this event to its certificate management system (MS_B) in Country B (event 2). However, certificates of V_{A1} were issued by the management system (MS_A) in Country A. Therefore, there is nothing MS_B can do unless there is an appropriate mechanism in place. It includes steps such as: 1) MS_B to identify the V_{A1}'s country of origin and to notify such event to MS_A (event 3), 2) MS_A to revoke V_{A1}'s certificates and report it back to MS_B (event 4).

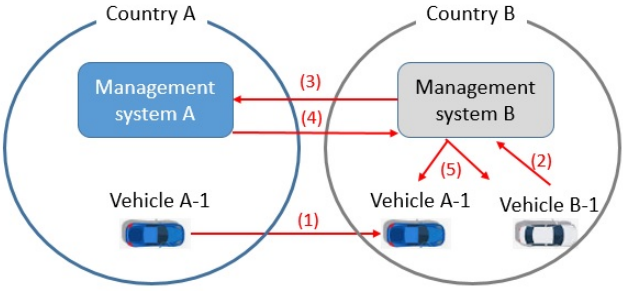


Figure 5: Scenario of Interconnection between Management Systems

Another example is the active revocation of vehicles. This is applicable in the US system as discussed in Sec. 4.2. If the management system revokes a vehicle, it generates and distributes the CRL containing this vehicle's information. However, in this case, vehicles (V_{Bs}) that encounter this vehicle on the road in Country B also need to receive this CRL so that V_{Bs} can correctly disregard any messages sent by V_{A1}. For this scenario to work correctly, MS_B needs to be notified of the revocation condition of V_{A1} from MS_A so that MS_B can distribute the CRL to vehicles in its territory. These aspects involving interaction across multiple security management systems are not covered in the ETSI ITS specifications. Given that cross-border mobility is a daily normal events in Europe, ETSI needs to address these aspects.

10.3 Multiple Security Management Systems for Different ITS-S Types

As discussed in Sec. 6.3, ITS-S consists of multiple different types (i.e. vehicles, RSUs). However, ETSI TS 102 940 [52] does not clearly specify how these different ITS-S types should be managed in the most effective and meaningful manner. Because these two types of ITS-S are owned and are used differently, it may make sense to manage them under separate management systems. For example, RSUs are owned, administered, and managed by government authorities, while majority of vehicles are owned and used by individual vehicle owners. One way to manage them is to manage RSUs under the national or provincial road authority, while vehicles are managed under regional vehicle registration offices. In addition, as discussed in Sec. 7.6, the inclusion of smartphones as a type of ITS-S in V2P scenarios raises a question of how they are managed to incorporate them as legitimate members of the ITS system. This is another aspect not currently covered by the ETSI ITS standard, thus it requires appropriate specification.

10.4 Absence of Consideration on Post-Quantum Cryptography Technologies

Both ETSI ITS [57] and IEEE 1609.2 [127] use Elliptic Curve Cryptography (ECC) to generate digital signatures and encrypt messages. However, existing public key cryptographic algorithms, including ones based on ECC, are known to be vulnerable in the face of a quantum computer [124]. Because vehicles, as an example of durable goods, have a lifespan as long as 23 years [102], they require technologies that can withstand against cyber threats during their lifetime. This includes migration to quantum-resistant security solutions [62]. When vehicles adopt post-quantum (PQ) digital certificate in the future, a smooth transition from the conventional to new PQ certificates need to be ensured.

Consideration in this area involves two aspects in the V2X context: (1) support of post-quantum cryptography (PQC) technologies, and (2) new issues that stem from the support of such technologies. First, quantum computers are already a reality [98]. Although it is expected to take many years for its capability to become an imminent threat [39], technologies being launched today need to have a solid migration strategy toward PQC paradigm. Evolving capabilities of quantum computers in the future necessitate cycles of updates in affected systems. This may imply that vehicles may require cycles of software update, upgrade, or even hardware replacement during the vehicle's lifetime to stay ahead of threats posed by future evolution of quantum computers. It further

introduces a new challenge to securely execute these updates and replacements. This is an uncharted territory involving both vehicles and the underlying system infrastructure. One such example is qSCMS [13] which is a quantum-resistant version of butterfly key [125]. Designing of new solutions to enhance or replace existing mechanisms to support PQ paradigm are required.

Second, support of PQC means that the public key size will increase significantly from the conventional public key schemes. Since 2015, the US National Institute of Standard and Technology (NIST) started the process of selecting PQC [101]. If we assume a code-based quantum-resistant signature algorithm, the size of public key and signature from the ECC-based algorithm increase from 0.1KB to 190KB [78]. This will significantly impact the amount of storage space required in vehicles, especially if a large number of certificates are expected to be preloaded. This will make the preloading of 5 year worth of certificate as proposed in IFAL [131] impractical, if not impossible. This situation will further shift more toward the on-demand based AT reloading strategy we discussed in Sec. 7.3 as a realistic solution.

11 Root Cause Analysis And Recommendations

Based on our analysis of ETSI ITS specifications, IEEE WAVE specifications, V2X related EU project documents, and relevant research papers, we have identified and discussed multiple gaps and issues in security aspects of V2X communication. We analyzed each of them and classified their origins into distinct root causes in Table 3. In this table, cells marked with a "✓" indicate a gap in the applicable categories. All of these represent identified issues that need further study, research, and solutions. In this section, we clarify each of their root cause category, along with our recommendations for the ETSI ITS specifications to address. Table 4 consolidates the identified issues.

Root cause 1: Conflicting or Insufficient Specification. We have identified a number of areas where existing ETSI ITS specifications contain conflicting requirements and areas that are not sufficiently specified. Conflicting requirements likely lead to an ineffective system as the end result. Insufficient specification means certain security aspects are specified for a certain subset only, or implicitly left to implementation decisions.

Recommendations & research objectives:

- Solve the conflicting requirements between privacy, anonymity, and safety – this refers to the situation where the mechanisms to ensure privacy of a vehicle owner result in potential compromise in road safety. One

Table 3: Summary of Security Issues

Root Cause Categories	Concerned Section	Conflicting or insufficient specification	Characteristics in vehicle comm. environment	Broadcast based communication	Implementation-dependent ambiguity	Certificate usage and management for vehicles	Certificate management of non-vehicle ITS-S type	RSU infrastructure dependency	MNO involvement and dependency
Sec.6 Privacy protection									
Privacy, Threat Actors, and Vehicle Operation	6.1	✓	✓	✓	✓				
Applicability of Privacy 1: Vehicle Types and Usages	6.2	✓				✓			
Applicability of Privacy 2: Non-Vehicle ITS-S	6.3	✓					✓		
Privacy and Cooperative Awareness	6.4	✓	✓	✓					
Privacy and Road Safety	6.5	✓	✓	✓					
Privacy and Use of Unicast	6.6		✓			✓			
Sec.7: Use of certificate									
Certificate-based Message Verification	7.1	✓	✓		✓				
Certificate Usage and Change Policy	7.2	✓	✓		✓	✓	✓		
Certificate Reloading	7.3	✓			✓	✓		✓	
Certificate Revocation	7.4	✓			✓	✓		✓	✓
Certificate Management of RSUs	7.5	✓			✓		✓	✓	
Certificate Management of VRUs	7.6	✓			✓		✓		✓
Certificate Usage in Multiple Comm.	7.7	✓		✓	✓	✓			
Sec.8: Communication modes									
Broadcast-Oriented Communication	8.1		✓	✓					
Unicast – Confidentiality Protection	8.2		✓						
Sec.9: Message handling									
Plausibility Validation and Misbehavior Detection	9.1	✓	✓		✓				
Communication involving VRU	9.2	✓					✓		✓
Sec.10: System level									
ITS-S Device-dependent Trust Level	10.1	✓		✓				✓	
Interconnection between Multiple Security Management Systems	10.2	✓			✓	✓			
Multiple Security Management Systems for Different ITS-S Types	10.3	✓			✓	✓	✓		✓
Absence of Post-Quantum Cryptography Technologies	10.4	✓							

example is the unobservability property making vehicles not being able to determine whether to apply brake or not upon receiving EEBL message from a surrounding vehicle (Sec. 6.5). Another example is the certificate management of non-vehicle ITS-S types (Sec. 6.3, 7.5, 7.6, and 9.2).

- Clarify the relationship and define the interworking mechanism between security management systems of different organizational entities, jurisdictions, and countries – vehicles from multiple regions and countries need to be able to communicate seamlessly across boundaries. This includes validation of pseudonym certificates in the receives messages, plausibility validation, and misbehavior detection (Sec. 9.1 and 10.2).
- The integration and joint risk assessment of complex system requirements that encompass safety, security, and privacy is a poorly understood field of research. Analysis techniques that combine approaches from safety engineering with those from security engineering, e.g. STPA-Sec or integrating attack vectors with fault trees may help but have not been applied to systems at the scale of V2X.

Root cause 2: Characteristics of Vehicular Communication Environment. The fundamental characteristic of a vehicle in operation is its dynamically changing position, both in relation to a static geo-referential or other vehicles in operation. The paradigm of constant topological changes combined with short-range direct communication poses challenges. This also applies to GeoNetworking as it is a chain of short-range communication between vehicles. This fundamental characteristic likely limits the type of services that can be realized in such environment. In particular, direct communications that are expected to last longer or between specific endpoints in unicast mode may suffer from a communication loss and impact its services as a result.

Recommendations & research objectives:

- Establish realistic expectations of the communication in both broadcast and unicast modes. Articulate the criteria and condition to use unicast communication as vehicles at the borderline of communication range will likely suffer communication failure (Sec. 6.6, 8.2).
- Establish guidelines on how to use and change pseudonyms for different purposes effectively in dynamically changing topology (Sec. 7.2, 7.7).
- A potential avenue towards increasing fault tolerance of V2X networks is to improve peer-to-peer networking between road users. To improve road safety, V2X technology must be used together with direct sensor perceptions in autonomous vehicles.

Root cause 3: Broadcast Based Communication. Basic services in the V2X are CAM and DENM which are broadcast based communication. Its fundamental characteristics are that: 1) any entity can receive messages, and 2) confidentiality protection is not applied. These two points render CAM and DENM *open* communication. There are solutions to apply encryption to broadcast traffic [37, 66, 118, 68]. However, the ETSI ITS standard does not require such mechanism. This situation makes it trivial for a malicious entity to eavesdrop and collect data (cf. Sec. 8.1). The only solution to render vehicular communication trustworthy is to apply the PKI-based message authentication and validation mechanism [7]. This makes V2X infrastructure dependent on security and reliability of PKI systems.

Recommendations & research objectives:

- Consider alternative approaches to apply confidentiality protection or pseudonymity to the broadcast-based communication, investigate efficient means for cryptographic credential and trust management at scale.

Root cause 4: Implementation-Dependent Ambiguity. We discussed the challenges, such as CRL distribution, plausibility validation, and misbehaviour detection. These areas are often implementation specific and are left up to the individual OEM's decision. This situation results in variations of effectiveness among implementations, where one implementation performs better than others in real life. It is likely not realistic to specify every aspects of the communication system in the standard. In fact, it may make sense or is inevitable to leave some aspects to implementation choice. However, those aspects should at least be documented in the standard to be cognizant of the choice of the extent the standard does not cover. This way, possible consequences are made clear.

Recommendations & research objectives:

- Define baseline criteria, which consists of a set of test cases, test data, and resulting decision criteria as a common foundation upon which various implementations can be tested and evaluated against. Doing so has a number of benefits (Sec. 9.1). One example is to define a clear and unambiguous method to validate plausibility and detect misbehaviour (Sec. 9.1).

Root cause 5: Certificate Usage and Management for Vehicles. Vehicles' usage of pseudonym certificates is not well defined in ETSI ITS specifications. This includes their usage period, change rules, and reloading mechanisms. In addition, another unspecified area is the pseudonym usage for different purposes (e.g. broadcast and unicast).

Recommendations & research objectives:

- Define how pseudonym and certificate are used by vehicles. This includes usage and change rules (Sec. 7.2), revocation and reloading rules and policy (Sec. 7.3, 7.7).
- Investigate efficient means for cryptographic credential and trust management at scale, consider the use of light-weight Hardware Security Modules (HSM) and Trusted Execution Environments (TEE) in vehicles.

Root cause 6: Certificate Management of Non-Vehicle ITS-S Types. Pseudonym usage by RSUs is not explicitly specified in the ETSI ITS standard. Thus it remains unclear if and how their usage is different from vehicles. Introducing smartphones (VRU) as a type of ITS-S requires appropriate management of these devices. Smartphones are consumer-owned generic platform as opposed to dedicated purpose devices such as OBUs and RSUs, thus a different approach to manage them will be required. Another open issue of smartphones is whether and how they can be revoked and removed from ITS system, if and when it is necessary.

Recommendations & research objectives:

- Define how the pseudonym usage in RSU is different from vehicles (Sec. 7.5). Define how smartphones as a type of ITS-S is managed in the ITS system, including enrolment, verification, and authorization, issuance of certificates, usage of pseudonyms, and how they are revoked from the system (Sec. 7.6).

Root cause 7: RSU Infrastructure Dependency. Many functionalities discussed in EU project use cases depend on RSUs and the infrastructure behind them, such as distribution and reloading of certificates. However, ubiquitous installation and availability of RSUs is an assumption, not a given condition. How soon an RSU infrastructure will be deployed depends on a number of non-technical factors, such as government policy on ITS and budget allocation. It is likely a gradual process and varies from one region to another and one country to another. ITS-capable vehicles likely find themselves in the situation where RSU installation is either scarce or non-existent. Thus, being overly dependent on RSUs is counterproductive to the deployment of V2X technology.

Recommendations & research objectives:

- Define alternative solutions to reduce dependency on the ubiquitous RSU deployment in such a way that necessary functionalities can be fulfilled

independent from RSUs when it is necessary, while making effective use of RSUs when they are available (Sec. 7.3).

Root cause 8: MNO Involvement and Dependency. Within the context of VRUs, whether interaction is required between the ITS system and MNOs to manage their access to the ITS system is unspecified in the ETSI ITS specification. If required, the solution needs standardization so that it will be adopted by all MNOs at international level.

Recommendations & research objectives:

- Define if the ITS management system and MNOs need to interact with each other to manage VRUs (smartphones) or not. This interaction between them includes definition of message contents (Sec. 7.6). This involves coordination with appropriate standard bodies such as 3GPP.

Table 4: List of Recommended Actions to ETSI ITS Specifications

Num	Description	Section
1	Specify possible differences in the privacy protection requirements for different ITS-S types.	6.2, 6.3
2	Resolve conflicting requirements of privacy protection and including vehcile-identifiable information in CAM and DENM.	6.4
3	Resolve conflicting requirements of privacy protection and road safety.	6.1, 6.5
4	Resolve privacy protection in unicast communication from both internal and external threats.	6.6
5	Address the potential issue of real-time certificate validation.	7.1
6	Standardise certificate change and reloading rule or policy.	7.2, 7.3
7	Resolve the time gap associated with passive revocation.	7.4
8	Specify certificate management of RSUs and VRUs.	7.5, 7.6
9	Specify different use of certificates for different purposes.	7.7
10	Address vulnerabilities of broadcast messages against passive observers.	8.1
11	Establish guidances on the use of unicast mode.	8.2
12	Establish guidance on the implementation of plausibility validation and misbehaviour detection.	9.1
13	Investigate solutions for accurate detection of VRU movement to VAM.	9.2
14	Consider possible notion of device type-dependent trust level.	10.1
15	Analyse and establish scenarios of interconnecting multiple management systems.	10.2, 10.3

12 Conclusion and Future Work

In this paper, we examined the EU standards for ITS, related US standards, various V2X-related EU projects, and relevant research papers. We integrated information from these sources, analyzed, and identified gaps in the security aspects of vehicular communication, focusing on the ETSI ITS specifications.

The issues and gaps we have identified are significant. They include conflicting and undefined specification in the standards. System level aspects need further definition, e.g. interworking of multiple management systems across multiple jurisdictions and countries. The security management of VRUs (smartphones) as a new ITS-S type is missing. Without addressing these aspects, the vehicular communication in reality can very well be unreliable, insecure, and unusable, ultimately leading to accidents, injuries, or loss of properties. Leaving details to implementation-specific solutions can lead to varying degree of effectiveness among implementations. To ensure uniform operation and effectiveness, further research and standardization is needed. In this respect, the future work is to address these gaps and issues to define possible solutions.

As a conclusion, the security solution in the ITS standards solely based on PKI leaves a number of areas to reconsider. Additional approaches and solutions are required to ensure vehicular communication is indeed secure so that the overall objective to make roads safer and reduce road accidents can be achieved rather than providing a new target for cyberattacks. The fundamental nature of cyber-physical system, such as vehicular communication, is that a sub-optimal system can cause physical damage in reality. In order to avoid such losses, all relevant security and privacy aspects of vehicular communication need to be addressed.

Acknowledgments

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203. This work was also supported in part by the Research Council KU Leuven C1 on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058. In addition, this work was supported in part by the Flemish Government through the imec Netsec project, through the EIT Health RAMSES project, through the Smart Highways SErVo project, and by the European Commission through the Horizon 2020 research and innovation programme under grant agreement H2020-SC1-FA-DTS-2018-1-826284 ProTego and MSCA-ITN-814035 5GhOSTS.

Appendix: Online Supplemental – Related Work: Extended Overview[6]

1. Survey Papers

We first review related work of V2X communication.[7] In the past years, a number of survey papers on security and privacy aspects of V2X have been published. Table 5 captures the overview of these surveys. The purpose of this section is to highlight the differences of our work compared to them. These survey papers can be categorized into three groups: ① discussion and solutions for generic vehicular network, ② surveys that cover both DSRC and C-V2X based solutions, and ③ surveys that focus specifically on C-V2X solutions.

In the first group, Hasan et al. [69], van der Heijden et al. [130], and Bißmeyer [15] exclusively focus on misbehaviour detection. In [69], a large part of this survey is dedicated to the discussion on attack and misbehaviour detection mechanisms by classifying and comparing numerous proposals on this subject. Survey in [130] provides in-depth analysis of detection mechanisms, and classify them into two-dimensions. The first dimension is *node-centric vs. data-centric*; the second dimension is *autonomous vs. collaborative*. Based on this classification, misbehaviour detection mechanisms can be categorized into one of the four types. The work in [15] focuses in two main areas: 1) misbehaviour detection, and 2) attacker identification in both local short-term and central long-term scope.

The survey by Badea and Stanciu [12] has a limited focus on security and privacy aspects. The only security related topic is on specific use cases and scenarios such as car sharing. Similarly, Ometov and Bezzateev [103] is not a survey; it is a proposal to apply multi-factor authentication (MFA) in V2X communication. This solution uses reversed Lagrange polynomial from Shamir's secret sharing schema as the building block. Wang et al. [134] focus specifically on the certificate revocation schemes in V2X communication. They analyse and classify them based on location where the revocation information has been placed. The entire revocation process is then divided into three stages: 1) resolution, 2) distribution, and 3) the use of revocation information.

In the second group, Huang et al. [72] treat both security and privacy topics although it is a small part of their paper as the content provides overview of 3GPP specifications on both LTE and 5G-based C-V2X rather than a survey.

[6] The content in this appendix appears only as the online supplemental material which expands Sec.2

[7] This is an extended version of Sec.2 in the main paper.

Table 5: V2X Related Survey Papers

Author	Year	Ref.	Group	Focused area	High level description
Hasan et al.	2020	[69]	①	misbehaviour detection	Analysis of attack types and misbehaviour detection mechanisms.
van der Heijden et al.	2018	[130]	①	misbehaviour detection	In-depth analysis of misbehaviour detection mechanisms and classifications.
Bißmeyer	2014	[15]	①	misbehaviour detection	Misbehaviour detection and attacker identification in both local short-term and central long-term scope.
Badea and Stanciu	2018	[12]	①	car sharing	Limited coverage on security aspects, focused on specific use cases and scenarios, e.g. car sharing.
Ometov and Bezzateev	2017	[103]	①	MFA	Despite its title, it is not a survey; it is a proposal to apply multi-factor authentication (MFA) in V2X.
Wang et al.	2020	[134]	①	certificate revocation	Analysis of various revocation schemes and classify them based on the location where the revocation information has been placed.
Huang et al.	2020	[72]	②	security and privacy solutions	Categorization of security and privacy solutions from two perspectives: 1) cryptography-based schemes, and 2) trust-based schemes. Discussion on both LTE and 5G-based C-V2X security.
Alnasser et al.	2019	[9]	②	security threats and solutions	Analysis of security threats and solutions for both DSRC and LTE-based C-V2X. Threat analysis includes availability, integrity, confidentiality authenticity, and non-repudiation.
Ghosal and Conti	2020	[67]	②	attack types and solutions	Analysis on security challenges and requirements by examining various attack types, their impacts, followed by solution analysis.
Cao et al.	2019	[19]	③	5G system	Covers overall 5G system security and privacy aspects of vertical applications (e.g. IoT, D2D, and 5G-specific topics such as network slice) rather than specifically on 5G-based C-V2X.
Muhammad and Safdar	2018	[95]	③	LTE C-V2X	Focus is specifically on the authentication mechanism of LTE systems in C-V2X context. They describe attack types, their relevance and countermeasures within the C-V2X context.
Lu et al.	2019	[87]	③	LTE, 5G C-V2X	Challenges in trust, security, and privacy-related issues in C-V2X, and strategies to resolve each of them for LTE and 5G-based C-V2X.
Lai et al.	2020	[85]	③	platoon operation	Proposal of security solutions specifically for platoon operation, including privacy-preserving group set up, distributed group key management, and cooperative message authentication.
Marojevic	2018	[91]	③	LTE C-V2X	Focus is on threat scenarios of LTE-based C-V2X, lists out associated security requirements, and sets out research directions to satisfy these requirements along with the needs of further standardization.

For security aspect, they discuss basic security services and attack types in vehicular networks, then categorize security solutions from two perspectives: 1) cryptography-based schemes, and 2) trust-based schemes. For privacy solutions, they categorize them into two types: 1) identity privacy preservation, and 2) location privacy preservation. Alnasser et al. [9] analyse security threats and solutions for both DSRC and LTE-based C-V2X. Their threat analysis includes availability, integrity, confidentiality, authenticity, and non-repudiation aspects. Then, they categorize security solutions including cryptography-based, behaviour/trust-based, and identity-based solutions. Ghosal and Conti [67] provide overview and background of both DSRC/WAVE and 3GPP-based LTE and 5G C-V2X systems, then discuss security challenges by analysing various attack types and how they impact V2X communication. Later, they examine techniques and solutions in specific areas, including symmetric key cryptography, privacy preservation, message authentication.

In the third group, Cao et al. [19] cover overall 5G system security and related topics rather than focusing on 5G-based C-V2X. They describe security and privacy aspects of other vertical applications such as IoT, device-to-device (D2D), and 5G-specific topics such as network slice. Only one section (Sec.VI) is dedicated to security in both LTE and 5G-based C-V2X solutions. In it, security requirements, solutions, and open issues are discussed. Muhammad and Safdar [95] focus specifically on the authentication mechanism in the context of LTE C-V2X. They enumerate attack types and describe their relevance and corresponding countermeasures. They discuss multiple proposed authentication solutions and analyse how they can meet the needs of C-V2X communication. Lu et al. [87] focus on security and privacy aspects of LTE and 5G-based C-V2X. Their survey is on challenges in trust, security, and privacy-related issues in C-V2X, followed by discussions on strategies to resolve them. The discussion in Lai et al. [85] rather narrowly focuses on a specific C-V2X scenario (platooning) rather than more general V2X communication. They propose security solutions, including privacy-preserving platoon group set up, distributed group key management, and cooperative message authentication. Marojevic [91] focuses on LTE-based C-V2X, discusses its threat scenarios, lists out associated security requirements, and proposes research directions to satisfy these requirements, along with the needs of further standardization to ensure security mechanisms are in place. In summary, the examined surveys can be characterized as follows:

- Analysis of relevant threat scenarios and attack types and their impacts to V2X communication,
- Discussion of issues, challenges, and requirements on specific security areas,

- Discussion on approaches and strategies to address stated issues and requirements,
- Description and comparison of existing proposed solutions on specific security areas,
- A new proposal on specific security or privacy area.

In contrast to these surveys, as articulated in Sec.1.2, our unique contribution in this paper is to point out fundamental issues and gaps in the ETSI ITS standards and unreported security and privacy issues that have not been discussed in the existing survey papers.

2. European Union Research Actions

In Europe since 2008, there have been numerous EU projects that either focus on or include V2X communications within their scope [112, 123, 110, 74, 60, 104, 38, 111, 32, 73, 1, 71, 8, 81, 20, 30, 22, 113, 21, 34, 5, 25, 122], which are listed in Table 6 in chronological order. Most of these projects are already completed at the time of writing and some of them no longer have active websites. In such cases, we refer to the respective EU project websites [26], project deliverables, and research papers specific to these projects. Given that some of the most representative security related ETSI ITS specifications, such as ETSI TS 102 940 [52] and 102 941 [56], first appeared in 2012, it is likely that some of the EU projects before that period had paved the way toward the creation of these security and privacy related specifications. Notable such examples are SeVeCom [123], PRECIOSA [110], EVITA [60], OVERSEE [104], and PRESERVE projects [111].

SeVeCom project [123] addressed the privacy issue in V2V and V2I communication by defining a pseudonym change management mechanism to avoid the use of fixed MAC address which leads to positive identification of vehicles [83]. PRECIOSA project [110] focused on the privacy protection of personal data in ITS applications. It adopted and clarified the privacy-by-design approach to address this issue [83]. Objectives of EVITA project [60] was to design, verify, and prototype security building blocks for automotive on-board networks to ensure sensitive data are protected against tampering. This project successfully designed a secure on-board architecture using Hardware Security Module (HSM) as the root-of-trust and secure on-board communication protocols [70]. OVERSEE project [104] developed an open and secure vehicular platform that provides protected run-time environment that enables secure execution of multiple applications. This design protects networks both internal and

Table 6: V2X Related EU Projects

Project Name	Full Project Name	Project Period	Ref.
PREVENT	Preventive and Active Safety Application	2004-02∼2008-01	[112]
SeVeCom	SEcure VEhicle COMmunication	2006-01∼2008-12	[123]
PRECIOSA	Privacy Enabled Capability In CO-operative systems and Safety Applications	2008-03∼2010-08	[110]
INTERSAFE-2	Cooperative Intersection Safety	2008-06∼2011-05	[74]
EVITA	E-safety Vehicle Intrusion proTected Applications	2008-07∼2011-12	[60]
OVERSEE	Open VEhiculaR SEcurE platform	2010-01∼2012-12	[104]
EcoGem	Cooperative Advanced Driver Assistance System for Green Cars	2010-09∼2013-02	[38]
PRESERVE	Preparing Secure Vehicle-to-X Communication Systems	2011-01∼2015-06	[111]
CONVERGE	Communication Network Vehicle Road Global Extension	2011-08∼2015-10	[32]
ICSI	Intelligent Cooperative Sensing for Improved Traffic Efficiency	2012-11∼2015-04	[73]
Autonet 2030	Co-operative Systems in Support of Networked Automated Driving by 2030	2013-11∼2016-10	[1]
HIGHTS	High precision positioning for cooperative ITS applications	2015-05∼2018-04	[71]
SCOOP@F Part2	SCOOP	2016-01∼2018-12	[122]
ADASANDME	Adaptive ADAS to support incapacitated drivers Mitigate Effectively risks through tailor made HMI under automation	2016-09∼2020-02	[8]
KoMoD	Kooperative Mobilität im digitalen Testfeld Düsseldorf	2017-06∼2019-06	[81]
5GCAR	5G Communication Automotive Research and innovation	2017-06∼2019-07	[20]
CONCORDA	Connected Corridor for Driving Automation	2017-10∼2020-06	[30]
Synergy CAV	Synergy CAV- Connectivity and intelligent mobility	2017-11∼2020-04	[22]
PRoPART	Precise and Robust Positioning for Automated Road Transports	2017-12∼2019-11	[113]
5G CARMEN	5G for Connected and Automated Road Mobility in the European UnioN	2018-11∼2021-10	[21]
5G CroCo	5G Cross Border Control	2018-11∼2021-10	[34]
5G-Mobix	5G for Cooperative & Connected Automated MOBility on X-border corridors	2019-06∼2022-06	[5]
C-Roads ITALY 3	C-Roads ITALY 3	2020-07∼2023-12	[25]

external to the vehicle, using standardized interfaces, against active and passive attacks [31]. Finally, PRESERVE project [111] specifically focused on security and privacy aspects of V2V and V2I communications as the primary scope of their work. It is likely that a large part of the security and privacy-related ETSI ITS specifications are the culmination of the results from these projects. Other projects not specifically mentioned up to this period (∼2015) [112, 74, 38, 32, 73, 1, 71, 8, 81, 20, 30, 22, 113, 21, 34, 5, 25, 122] focus on other aspects of vehicular technologies and include V2X communication as a part of the overall project scope.

More recent EU projects primarily focus on demonstrations of technology readiness in V2X services in controlled or real-world environments rather than exclusively focusing on specific technical domains such as security or privacy aspects. It is especially notable in 5G Infrastructure Public Private Partnership (5G-PPP) related V2X projects such as in [20, 21, 34, 5]. These projects are based on specific use cases and scenarios as described in the respective documents [97, 61, 132, 108, 92]. Although these EU projects are beneficial to demonstrate the technology itself, none of them include security considerations within their scope. Studying their use case description documents reveals that almost all of them lack even a clear definition of underlying assumptions in the communication mode used (e.g. broadcast, unicast) or message direction (e.g. uplink, downlink). The underlying implicit assumption is that security solutions and mechanisms are in place, and all messages exchanged are verified, correct, and trustworthy. This assumption does not, however, reflects the reality. We have conducted a security and privacy gap analysis based on the aforementioned 5G-PPP EU projects, relevant ETSI ITS standard specifications, and research papers. As a result, we have identified significant security gaps and conflicts between the standard and what V2X communication aims to achieve. Our findings capture the main security and privacy gaps and concerns in V2X communication systems; they are confirmed by a number of other research papers [67, 72, 9, 23] that focus on the security aspects of V2X communication. Most notably is the work of Chator and Green [23]. In our analysis, we include the aspects specifically raised in [23] where relevant.

References

[1] Autonet 2030. Co-operative Systems in Support of Networked Automated Driving by 2030. `https://www.autonet2030.eu/`.

[2] 3GPP. TS 23.285, Architecture Enhancements for V2X Services, v16.2.0. Technical report, 3rd Generation Partnership Project, 12 2019.

[3] 3GPP. Study on Security Aspects of 3GPP Support for Advanced V2X Services. Technical Report (TR) 33.836, 3rd Generation Partnership Project (3GPP), 07 2020. Ver. 16.0.0.

[4] 3GPP. TS 23.287, Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services, v.17.2.0. Technical Specification (TS), 3rd Generation Partnership Project, 12 2021.

[5] 5G-Mobix. 5G for Cooperative & Connected Automated MOBIility on X-border Corridors. `https://www.5g-mobix.com`.

[6] NIS Act. Cybersecurity act. *OJ L*, 194(19.7), 2019.

[7] Carlisle Adams and Steve Lloyd. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Addison-Wesley Professional, 2003.

[8] ADASANDME. Adaptive ADAS to Support Incapacitated Drivers Mitigate Effectively Risks Through Tailor Made HMI under Automation. `https://www.adasandme.com/`.

[9] Aljawharah Alnasser, Hongjian Sun, and Jing Jiang. Cyber Security Challenges and Solutions for V2X Communications: A Survey. *Computer Networks*, 151:52–67, 2019.

[10] Moreno Ambrosin, Lily L Yang, Xiruo Liu, Manoj R Sastry, and Ignacio J Alvarez. Design of a Misbehavior Detection System for Objects Based Shared Perception V2X Applications. In *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*, pages 1165–1172. IEEE, 2019.

[11] Nick Asselin-Miller, Marius Biedka, Gena Gibson, Felix Kirsch, Nikolas Hill, Ben White, and Kotub Uddin. Study on the deployment of C-ITS in Europe: Final Report. *Report for DG MOVE MOVE/C*, 3:2014–794, 2016.

[12] Radu Alexandru Badea and Lucian Stanciu. A Survey and Research Model for Vehicular Communication and Security Challenges. In *2018 International Conference on Communications (COMM)*, pages 291–296. IEEE, 2018.

[13] Paulo SLM Barreto, Jefferson E Ricardini, Marcos A Simplicio Jr, and Harsh Kupwade Patil. qSCMS: Post-Quantum Certificate Provisioning Process for V2X. *IACR Cryptol. ePrint Arch.*, 2018:1247, 2018.

[14] Giampaolo Bella, Pietro Biondi, Gianpiero Costantino, and Ilaria Matteucci. Toucan: A Protocol to Secure Controller Area Network. In *Proceedings of the ACM Workshop on Automotive Cybersecurity*, pages 3–8, 2019.

[15] Norbert Bißmeyer. *Misbehavior Detection and Attacker Identification in Vehicular Ad-Hoc Networks.* PhD thesis, Technische Universität Darmstadt, 2014.

[16] Norbert Bißmeyer, Hagen Stübing, Elmar Schoch, Stefan Götz, Jan Peter Stotz, and Brigitte Lonc. A Generic Public Key Infrastructure for Securing Car-to-X Communication. In *18th ITS World Congress on Intelligent Transport Systems*, volume 14, 2011.

[17] Benedikt Brecht. Security and Privacy for a Connected Vehicle Environment. `https://www.researchgate.net/publication/310234154_Security_and_privacy_for_a_connected_vehicle_environment`, 08 2016.

[18] Benedikt Brecht, Dean Therriault, André Weimerskirch, William Whyte, Virendra Kumar, Thorsten Hehn, and Roy Goudy. A Security Credential Management System for V2X Communications. In *IEEE Transactions on Intelligent Transportation Systems*, volume 19, pages 3850–3871. IEEE, 2018.

[19] Jin Cao, Maode Ma, Hui Li, Ruhui Ma, Yunqing Sun, Pu Yu, and Lihui Xiong. A Survey on Security Aspects for 3GPP 5G Networks. *IEEE Communications Surveys & Tutorials*, 22(1):170–195, 2019.

[20] 5G Car. Fifth Generation Communication Automotive Research and Innovation. `http://5gcar.eu`.

[21] 5G Carmen. 5G for Connected and Automated Road Mobility in the European UnioN. `https://5gcarmen.eu/`.

[22] Synergy CAV. Synergy CAV - Connectivity and Intelligent Mobility. `http://synergy-cav.com/`.

[23] Alishah Chator and Matthew Green. Don't Talk to Strangers-On the Challenges of Intelligent Vehicle Authentication. In *VEHITS*, pages 522–528, 2018.

[24] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *USENIX Sec*, 2011.

[25] European Commission. C-Roads Italy. `https://www.c-roads.eu/pilots/core-members/italy/Partner/project/show/c-roads-italy.html`.

[26] European Commission. Transport Research and Innovation Monitoring and Information System. `https://trimis.ec.europa.eu/search/site`.

[27] European Commission. Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). *C-ITS Platform Phase II*, 2017.

[28] European Commission. Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), rel.1.1. *C-ITS Platform Phase II*, 2018.

[29] IEEE 802 LAN/MAN Standards Committee. IEEE Standard for Information Technology-Telecommunication and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment1: Radio Resource Measurement of Wireless LANs. Standard, Institute of Electrical and Electronics Engineers, 2016.

[30] Concorda. Connected Corridor for Driving Automation. `https://connectedautomateddriving.eu/project/concorda`.

[31] OVERSEE Concortium. Deliverable D8.3: OVERSEE Final Report, 2013.

[32] CONVERGE. Communication Network Vehicle Road Global Extension. `https://trimis.ec.europa.eu/project/communication-network-vehicle-road-global-extension`.

[33] Quentin Covert, Dustin Steinhagen, Mary Francis, and Kevin Streff. Towards a Triad for Data Privacy. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.

[34] 5G CroCo. Fifth Generation Cross-Border Control. `https://5gcroco.eu/`.

[35] Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, and Pascal Thubert. IETF RFC 3963-Network Mobility (NEMO) Basic Support Protocol. Online Document. Updated in January 2005. Cited on 2.2. 2011.

[36] NIS Directive. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union. *OJ L*, 194(19.7):2016, 2016.

[37] Xinjun Du, Ying Wang, Jianhua Ge, and Yumin Wang. An ID-Based Broadcast Encryption Scheme for Key Distribution. *IEEE Transactions on broadcasting*, 51(2):264–266, 2005.

[38] EcoGem. Cooperative Advanced Driver Assistance System for Green Cars. `https://algowatt.com/portfolio-items/ecogem/`.

[39] Ericsson. Ensuring Security in Mobile Networks Post-Quantum. *Ericsson Technology Review*, 12, 2021.

[40] Stephan Escher, Markus Sontowski, Knut Berling, Stefan Köpsell, and Thorsten Strufe. How Well Can Your Car Be Tracked: Analysis of the European C-ITS Pseudonym Scheme. In *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, pages 1–6. IEEE, 2021.

[41] ETSI. EN 302 665: Intelligent Transport Systems (ITS); Communications Architecture; V1.1.1. Standard, European Telecommunications Standards Institute (ETSI), 09 2010.

[42] ETSI. TS 102 637-1: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements; V1.1.1. Standard, European Telecommunications Standards Institute (ETSI), 09 2010.

[43] ETSI. TS 102 731: Intelligent Transport Systems (ITS); Security; Security Services and Architecture; V1.1.1. Standard, European Telecommunications Standards Institute, 09 2010.

[44] ETSI. TS 102 942: Intelligent Transport Systems (ITS); Security; Access Control Technical Specification; V1.1.1. Standard, European Telecommunications Standards Institute, 06 2012.

[45] ETSI. TS 102 943: Intelligent Transport Systems (ITS); Security; Confidentiality Services; V1.1.1. Standard, European Telecommunications Standards Institute (ETSI), 06 2012.

[46] ETSI. EN 302 636-1: Intelligent Transport Systems (ITS); Vehicular Communications; Geonetworking; Part 1: Requirements; V1.2.1. Standard, European Telecommunications Standards Institute (ETSI), 04 2014.

[47] ETSI. EN 302 636-3: Intelligent Transport Systems (ITS); Vehicular Communications; Geonetworking; Part 3: Network Architecture; V1.2.1. Standard, European Telecommunications Standards Institute (ETSI), 12 2014.

[48] ETSI. EN 302 636-6-1: Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols; V1.2.1. Standard, European Telecommunications Standards Institute (ETSI), 05 2014.

[49] ETSI. EN 302 636-4-1: Intelligent Transport Systems (ITS); Vehicular Communications; Geonetworking; Part 4: Geographical Addressing and Forwarding for Point-to-Point and Point-to-Multipoint Communications; Sub-part 1: Media-Independent Functionality; V1.3.1. Standard, European Telecommunications Standards Institute (ETSI), 08 2017.

[50] ETSI. TR 102 893: Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA); V1.2.1. Standard, European Telecommunications Standards Institute (ETSI), 03 2017.

[51] ETSI. TR 103 415: Intelligent Transport Systems (ITS); Security; Pre-Standardization Study on Pseudonym Change Management; V1.1.1. Standard, European Telecommunications Standards Institute (ETSI), 04 2018.

[52] ETSI. TS 102 940: Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management; V2.1.1. Standard, European Telecommunications Standards Institute, 07 2018.

[53] ETSI. EN 302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, V1.4.1. Standard, European Telecommunications Standards Institute, 04 2019.

[54] ETSI. EN 302 637-3: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service; V1.3.1. Standard, European Telecommunications Standards Institute, 04 2019.

[55] ETSI. TR 103 300-1: Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) Awareness; Part 1: Use Cases Definition; Release 2; V2.2.1. Standard, European Telecommunications Standards Institute (ETSI), 04 2021.

[56] ETSI. TS 102 941: Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; V2.1.1. Standard, European Telecommunications Standards Institute, 10 2021.

[57] ETSI. TS 103 097: Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats; Release 2; V2.1.1. Standard, European Telecommunications Standards Institute, 10 2021.

[58] ETSI. TS 103 300-2: Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) Awareness; Part 2: Functional Architecture and Requirements Definition; Release 2; V2.2.1. Standard, European Telecommunications Standards Institute (ETSI), 04 2021.

[59] ETSI. TS 103 300-3: Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) Awareness; Part 3: Specification of VRU Awareness Basic Service; Release 2; V2.1.2. Standard, European Telecommunications Standards Institute (ETSI), 04 2021.

[60] EVITA. E-safety Vehicle Intrusion proTected Applications. https://www.evita-project.org/.

[61] Antonio E. Fernandez, Mikael Fallgren, and Nadia Brahmi. 5GCAR Scenarios, Use Cases, Requirements and KPIs. *Fifth Generation Communication Automotive Research and innovation, Tech. Rep. D*, 2, 2019.

[62] Tiago M Fernández-Caramés. From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. *IEEE Internet of Things Journal*, 7(7):6457–6480, 2019.

[63] Flightradar24.com. https://www.flightradar24.com.

[64] Laurent Gallo and Massimo Condoluci. 5GCAR D4.2 Final Design and Evaluation of the 5G V2X System Level Architecture and Security Framework. *Fifth Generation Communication Automotive Research and innovation, Tech. Rep. D*, 2019.

[65] Laurent Gallo, Thierry Lejkin, Bruno Tossou, and Bernadette Villeforceix. Initial Design of 5G V2X System Level Architecture and Security Framework. *Fifth Generation Communication Automotive Research and Innovation, Tech. Rep. D*, 2, 2018.

[66] Juan A Garay, Jessica Staddon, and Avishai Wool. Long-Lived Broadcast Encryption. In *Annual International Cryptology Conference*, pages 333–352. Springer, 2000.

[67] Amrita Ghosal and Mauro Conti. Security Issues and Challenges in V2X: A Survey. *Computer Networks*, 169:107093, 2020.

[68] Dani Halevy and Adi Shamir. The LSD Broadcast Encryption Scheme. In *Annual International Cryptology Conference*, pages 47–60. Springer, 2002.

[69] Monowar Hasan, Sibin Mohan, Takayuki Shimizu, and Hongsheng Lu. Securing Vehicle-to-Everything (V2X) Communication Platforms. *IEEE Transactions on Intelligent Vehicles*, 2020.

[70] Olaf Henniger. EVITA Project Summary, 2012.

[71] HIGHTS. High Precision Positioning for Cooperative ITS Applications. https://trimis.ec.europa.eu/project/high-precision-positioning-cooperative-its-applications.

[72] Jiaqi Huang, Dongfeng Fang, Yi Qian, and Rose Qingyang Hu. Recent Advances and Challenges in Security and Privacy for V2X communications. *IEEE Open Journal of Vehicular Technology*, 1:244–266, 2020.

[73] ICSI. Intelligent Cooperative Sensing for Improved Traffic Efficiency – ICSI. `https://www.fpz.unizg.hr/oms/?page_id=1246&variable=ICSI`.

[74] INTERSAFE-2. Cooperative Intersection Safety. `https://trimis.ec.europa.eu/project/cooperative-intersection-safety`.

[75] ISO. Road Vehicles — Functional Safety. Standard ISO 26262, International Organization for Standardization (ISO), 2018.

[76] ISO. Road Vehicles — Cybersecurity Engineering. Standard ISO/SAE 21434, International Organization for Standardization (ISO), 2021.

[77] iso39001. Road Traffic Safety (RTS) Management Systems — Requirements with Guidance for Use. Standard ISO 39001, International Organization for Standardization (ISO), 2012.

[78] Panos Kampanakis, Peter Panburana, Ellie Daw, and Daniel Van Geest. The Viability of Post-Quantum X. 509 Certificates. *IACR Cryptol. ePrint Arch.*, 2018:63, 2018.

[79] Mohammad Khodaei and Panagiotis Papadimitratos. Scalable & Resilient Vehicle-Centric Certificate Revocation List Distribution in Vehicular Communication Systems. *IEEE Transactions on Mobile Computing*, 2020.

[80] Florian Klingler, Falko Dressler, and Christoph Sommer. IEEE 802.11p Unicast Considered Harmful. In *2015 IEEE Vehicular Networking Conference (VNC)*, pages 76–83. IEEE, 2015.

[81] KoMoD. Kooperative Mobilität im Digitalen Testfeld Düsseldorf. `https://www.ika.rwth-aachen.de/en/research/projects/automated-driving/2534-komod.html`.

[82] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. Experimental Security Analysis of a Modern Automobile. In *2010 IEEE Symposium on Security and Privacy*, pages 447–462. IEEE, 2010.

[83] Antonio Kung. ICT and Privacy: Barriers. In *Annual Privacy Forum*, pages 177–186. Springer, 2012.

[84] Kenneth P Laberteaux, Jason J Haas, and Yih-Chun Hu. Security Certificate Revocation List Distribution for VANET. In *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, pages 88–89, 2008.

[85] Chengzhe Lai, Rongxing Lu, Dong Zheng, and Xuemin Sherman Shen. Security and Privacy Challenges in 5G-enabled Vehicular Networks. *IEEE Network*, 34(2):37–45, 2020.

[86] Stéphanie Lefevre, Jonathan Petit, Ruzena Bajcsy, Christian Laugier, and Frank Kargl. Impact of V2X Privacy Strategies on Intersection Collision Avoidance Systems. In *2013 IEEE Vehicular Networking Conference*, pages 71–78. IEEE, 2013.

[87] Rongxing Lu, Lan Zhang, Jianbing Ni, and Yuguang Fang. 5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy. *Proceedings of the IEEE*, 108(2):373–389, 2019.

[88] Xiaomin Ma, Xianbo Chen, and Hazem H Refai. Performance and Reliability of DSRC Vehicular Safety Communication: A Formal Analysis. *EURASIP Journal on Wireless Communications and Networking*, 2009:1–13, 2009.

[89] Georg Macher, Christoph Schmittner, Omar Veledar, and Eugen Brenner. ISO/SAE DIS 21434 Automotive Cybersecurity Standard-In a Nutshell. In *International Conference on Computer Safety, Reliability, and Security*, pages 123–135. Springer, 2020.

[90] MarineTraffic.com. `https://www.marinetraffic.com`.

[91] Vuk Marojevic. C-V2X Security Requirements and Procedures: Survey and Research Directions. *arXiv preprint arXiv:1807.09338*, 2018.

[92] Ángel Martin and Gorka Vélez. 5G-Enabled CCAM Use Cases Specifications. *5G Mobix*, 2, 2019.

[93] McKinsey. Cybersecurity in Automotive, Mastering the Challenge. `https://www.mckinsey.com/industries/automotive-and-assembly/our-insights`.

[94] Charlie Miller and Chris Valasek. Remote Exploitation of an Unaltered Passenger Vehicle. *Black Hat USA*, 2015.

[95] Mujahid Muhammad and Ghazanfar Ali Safdar. Survey on Existing Authentication Issues for Cellular-Assisted V2X Communication. *Vehicular Communications*, 12:50–65, 2018.

[96] Hyeran Mun, Kyusuk Han, and Dong Hoon Lee. Ensuring Safety and Security in CAN-Based Automotive Embedded Systems: A Combination of Design Optimization and Secure Communication. *IEEE Transactions on Vehicular Technology*, 69(7):7078–7091, 2020.

[97] Dries Naudts, Vasilis Maglogiannis, and Simon Vanneste. Test Site BE Operational- Belgian Pilot Site. *Concorda*, 2, 2018.

[98] NewScientist.com. IBM Unveils Its First Commercial Quantum Computer. `https://www.newscientist.com/article/2189909-ibm-unveils-its-first-commercial-quantum-computer/`.

[99] NHTSA. Preliminary Regulatory Impact Analysis, FMVSS No. 150 Vehicle-To-Vehicle Communication Technology for Light Vehicles. *NHTSA*, 2, 2016.

[100] Michael E Nowatkowski and Henry L Owen. Certificate Revocation List Distribution in VANETs Using Most Pieces Broadcast. In *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)*, pages 238–241. IEEE, 2010.

[101] National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standardization. `https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization`. Accessed: 2021-12-03.

[102] Masahiro Oguchi and Masaaki Fuse. Regional and Longitudinal Estimation of Product Lifespan Distribution: A Case Study for Automobiles and A Simplified Estimation Method. *Environmental Science & Technology*, 49(3):1738–1743, 2015.

[103] Aleksandr Ometov and Sergey Bezzateev. Multi-Factor Authentication: A Survey and Challenges in V2X Applications. In *2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 129–136. IEEE, 2017.

[104] OVERSEE. Open VEhicular SEcurE platform. `https://www.oversee-project.com/`.

[105] Panagiotis Papadimitratos, Ghita Mezzour, and Jean-Pierre Hubaux. Certificate Revocation List Distribution in Vehicular Communication Systems. In *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, pages 86–87, 2008.

[106] European Parliament. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal

Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications). *JL 201, 31.7. 2002, at 37.(Directive on Privacy and Electronic Communications)*, 2002.

[107] The European Parliament and The Council of The European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council. *Official Journal of the European Union*, 679, 2016.

[108] Eric Perraud and Kurt Eckert. Test Case Definition and Test Site Description Part 1. *5G CroCo*, 2, 2019.

[109] Andreas Pfitzmann and Marit Hansen. A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. `http://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf`, 2010.

[110] PRECIOSA. Privacy Enabled Capability in Co-Operative Systems and Safety Applications. `https://trimis.ec.europa.eu/project/privacy-enabled-capability-co-operative-systems-and-safety-applications`.

[111] PRESERVE. Preparing Secure Vehicle-to-X Communication Systems. `https://trimis.ec.europa.eu/project/preparing-secure-vehicle-x-communication-systems`.

[112] PREVENT. Preventive and Active Safety Application. `https://www.prevent-ip.org/`.

[113] PRoPART. Precise and Robust Positioning for Automated Road Transports. `http://propart-project.eu/`.

[114] Han Qiu, Meikang Qiu, and Ruqian Lu. Secure V2X Communication Network Based on Intelligent PKI and Edge Computing. *IEEE Network*, 2019.

[115] Giovanni Rigazzi, Andrea Tassi, Robert J Piechocki, Theo Tryfonas, and Andrew Nix. Optimized Certificate Revocation List Distribution for Secure V2X Communications. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pages 1–7. IEEE, 2017.

[116] Ishtiaq Rouf, Robert D Miller, Hossen A Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study. In *USENIX Security Symposium*, volume 10, 2010.

[117] SAE. J2735, Surface Vehicle Standard, V2X Communications Message Set Dictionary. Standard SAE J2735:2006, SAE International, 2006.

[118] Ryuichi Sakai and Jun Furukawa. Identity-Based Broadcast Encryption. *IACR Cryptol. ePrint Arch.*, 2007:217, 2007.

[119] Alexey Samoshkin. SSL Certificate Revocation and How It Is Broken in Practice. `https://medium.com/@alexeysamoshkin/how-ssl-certificate-revocation-is-broken-in-practice-af3b63b9cb3`.

[120] Stefan Santesson, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams. X. 509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP. *RFC*, 6960:1–41, 2013.

[121] Christoph Schmittner, Gerhard Griessnig, and Zhendong Ma. Status of the Development of ISO/SAE 21434. In *European Conference on Software Process Improvement*, pages 504–513. Springer, 2018.

[122] SCOOP. SCOOP. `http://www.scoop.developpement-durable.gouv.fr/en/`.

[123] SeVeCom. Secure Vehicle Communication. `https://trimis.ec.europa.eu/project/secure-vehicle-communication`.

[124] Peter W Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM review*, 41(2):303–332, 1999.

[125] Marcos A Simplicio, Eduardo Lopes Cominetti, Harsh Kupwade Patil, Jefferson E Ricardini, and Marcos Vinicius M Silva. The Unified Butterfly Effect: Efficient Security Credential Management System for Vehicular Communications. In *2018 IEEE Vehicular Networking Conference (VNC)*, pages 1–8. IEEE, 2018.

[126] Adam Slagell, Rafael Bonilla, and William Yurcik. A Survey of PKI Components and Scalability Issues. In *2006 IEEE International Performance Computing and Communications Conference*, pages 10–pp. IEEE, 2006.

[127] IEEE Vehicular Technology Society. Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Services. Technical specification, Institute of Electrical and Electronics Engineers, Piscataway, NJ, United States, 03 2016.

[128] Syrma SGS Technology. Automotive ECU: Core Component for Connected Cars. `https://www.syrma.com/ecu/`.

[129] IoT World Today. Connectivity Changes How Customers, Manufacturers Look at Vehicles. `https://iotworldtoday.tradepub.com/free/w_defa2552/prgm.cgi`, 2022. Accessed: May 27, 2022.

[130] Rens Wouter van der Heijden, Stefan Dietzel, Tim Leinmüller, and Frank Kargl. Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. *IEEE Communications Surveys & Tutorials*, 21(1):779–811, 2018.

[131] Eric Verheul, Christopher Hicks, and Flavio D Garcia. IFAL: Issue First Activate Later Certificates for V2X. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 279–293. IEEE, 2019.

[132] Filippo Visintainer. 5G CARMEN Use Cases and Requirements. *5G CARMEN*, 2, 2019.

[133] Skanda Vivek, David Yanni, Peter J Yunker, and Jesse L Silverberg. Cyberphysical Risks of Hacked Internet-Connected Vehicles. *Physical Review E*, 100(1):012316, 2019.

[134] Qianpeng Wang, Deyun Gao, and Du Chen. Certificate Revocation Schemes in Vehicular Networks: A Survey. *IEEE Access*, 8:26223–26234, 2020.

[135] Takahito Yoshizawa and Bart Preneel. Survey of Security Aspect of V2X Standards and Related Issues. In *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 1–5. IEEE, 2019.

Publication

Survey of Security Aspect of V2X Standards and Related Issues

Publication Data

Yoshizawa, T., and Preneel, B. Survey of Security Aspect of V2X Standards and Related Issues. In 2019 IEEE Conference on Standards for Communications and Networking (CSCN), IEEE, pp. 1–5, 2019.

Contributions

- Principal author.

Survey of Security Aspect of V2X Standards and Related Issues

Takahito Yoshizawa and Bart Preneel

KU Leuven, ESAT/COSIC, Leuven, Belgium

Abstract. In the past years, two communication technologies have emerged for Vehicle-to-everything (V2X) communication, namely IEEE 802.11p-based and cellularbased solutions. However, V2X-related standards continue to evolve. For example, IETF has been working on V2X topics from an IP network and transport perspective. After completing the LTE-based V2X standard specifications, 3GPP continues with a 5G-based V2X solution. While IEEE 802.11p-based and cellular-based solutions appear to be two competing solutions, there have been proposals for a hybrid approach in which both technologies co-exist and are used at the same time in a different manner. However, this implies that there are two different security solutions with different architectures: this requires careful consideration to ensure co-existence and operation. This paper presents a survey of the recent developments in the area of V2X standardization with a focus on security aspects.

1 Introduction

Connected-car and autonomous driving concepts have been gaining momentum in the automotive industry in the past years. The market size of these technologies is expected to grow significantly, and their economic impact will be significant. The deployment of these innovative technologies requires the definition of appropriate standards; several Standard Defining Organizations (SDOs) have taken on this task. IEEE started the standardization work on 802.11p in 2004; the resulting standard was published in 2010. Further standardization work was initiated in 2006 by IEEE and ETSI, resulting in the IEEE 1609 series and the ETSI ITS series of standards being adopted in the US and Europe, respectively. In the US, the IEEE 1609 series of specifications led SAE to define application layer standards for V2V communication. IEEE 1609 is generally referred to as the Wireless Access in Vehicle Environment (WAVE), and SAE coined the term Dedicated Short Range Communication (DSRC). In

Europe, the ETSI specification is referred to as Intelligent Transport System (ITS-G5) or Cooperative ITS (C-ITS).

Starting from 2015, as a part of Release 14, the 3rd Generation Partnership Project (3GPP) has started to define the Vehicle-to-Everything (V2X) related standard based on cellular technology, namely Long Term Evolution (LTE), or Fourth Generation (4G) mobile system. Their work has resulted in a set of Technical Specifications (TS) for V2X. 3GPP is currently working on Release 16 and continues to further define specifications for V2X based on 5G.

Consequently, this situation results in two different standards to address the same needs, defined by different SDOs using different technologies. Naturally, different system architectures and solutions imply two different security architecture and solutions.

Recently, several proposals (e.g., Abboud et al. [5]) have been made to adopt a hybrid approach where the 802.11p-based and cellular-based V2X technologies co-exist and are used simultaneously. However, the security implications of this hybrid approach have not been analyzed in detail. For this reason, this paper summarizes the recent developments of V2X standards and analyzes them from a security perspective.

The remainder of this paper is organized as follows. Part 2 summarizes the evolution of the V2X related standards. In Part 3, we discuss the security implications of the hybrid approach, identify issues and address potential solutions. Part 4 concludes the paper with areas of future work.

2 Evolution OF V2X Standards

This section presents an overview of the standardization landscape of two different V2X communication technologies. In order to clarify the relationships between the two main standards, Fig. 1 shows the protocol stacks for ETSI ITS / 802.11 OCB and 3GPP PC5 as well as the Uu interfaces.

2.1 802.11-OCB mode (formerly 802.11p)

IEEE first published 802.11p the specification as an amendment to the 2010 version of the 802.11 specification. It was later incorporated into the 2016 version of 802.11 [9]. Thus “802.11p” is now a historical term only. The original feature published as 802.11p is now called “outside of context of a basic service” mode (OCB) in [9]. The overall objective of the OCB mode is to address the needs of

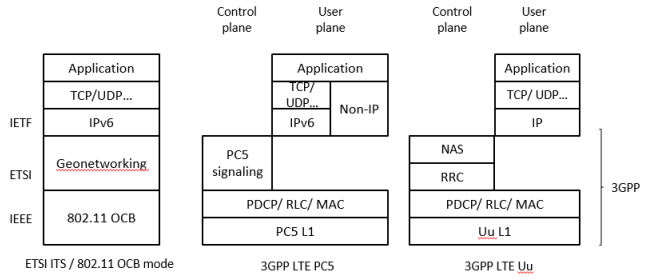


Figure 1: Protocol Stack for ETSI ITS / 802.11 OCB, 3GPP PC5, and 3GPP Uu Interfaces

vehicular communication environment where the duration of communication is short-lived and thus it is necessary to establish communication quickly. The main characteristics of OCB mode can be summarized as follows:

- No IEEE 802.11 Beacon frames are transmitted
- No authentication is required to communicate
- No association is needed to communicate
- No encryption is provided

The absence of security mechanisms in 802.11 OCB mode implies that there is no procedure to establish communication, such as device authentication or association establishment, unlike in the conventional 802.11 operation. The underlying assumption is that these functions are provided at the higher layer. In other words, any adversary can transmit frames or monitor the traffic in the vicinity at any time without establishing proper authentication to the network or without agreeing on the cryptographic keys. This complete "openness" in lower layers goes against the general principle to make the network more secure. In fact, the complete absence of security mechanism in the 802.11 OCB mode makes it easier for an adversary to launch types of attacks which may not be possible in a conventional 802.11 network. This is a significant point given that V2X communication deals with vehicles that move in outdoor public space such as open roads and highways.

For this reason, it is essential that an adequate privacy protection mechanism is in place to prevent an adversary from identifying and tracking vehicles. This is achieved through a pseudonym that is periodically changed.

The 802.11 OCB mode is used as the underlying layer 1 and layer 2 for region-specific V2X standards, namely 1) the IEEE 1609 series of standard used in the US (WAVE), and 2) ETSI ITS used in Europe (ITS-G5).

2.2 IETF IPWAVE

In 2016, IETF established the IP Wireless Access in Vehicular Environment (IPWAVE) WG to specify the details of transmitting IPv6 packets over the 802.11 OCB mode. The WG charter includes as objective the investigation of the security and privacy aspects, and in particular privacy-friendly methods to preclude unwanted tracking.

IPWAVE WG has recently published its two latest drafts. The first one contains the problem statement and describes the use cases [10]; the second one deals with the transmission of IPv6 packets over the 802.11 OCB mode [13].

The discussion in [10] covers the Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) use cases and analyzes the existing protocols for vehicular networks. The network architecture shows that both the vehicle and the infrastructure device, such as a Road Side Unit (RSU), consist of multiple entities to form an internal network, including one or more hosts, a router, and a DNS server. These internal entities are connected in subnets which are separate from the external interface with which other vehicle or RSUs are connected. Therefore, individual vehicle and RSU contains a network by itself and the communication between vehicles (V2V) and between vehicle and RSU (V2I) is an inter-connection of two networks.

Fig. 2 shows the IPWAVE network architecture. The top half is the inter-connection in the V2V case, and the bottom half is the inter-connection in the V2I case. The external subnet represents the connection over the wireless link using the 802.11 OCB mode.

The first IPWAVE Internet Draft [10] also highlights the underlying functionalities such as neighbor discovery, mobility management, and security and privacy.

From a security perspective, [10] recommends the use of the Vehicle Identification Number (VIN), a user certificate, and an identifier generator in the vehicle to allow the authentication server in the infrastructure to authenticate the vehicle through an RSU. In addition, the establishment of secure end-to-end (E2E) vehicle communication is supported by TLS certificates.

The second Internet Draft [13] describes the IPv6 operation over the 802.11 OCB mode. Specifically, it defines the MTU, frame format, link-local address,

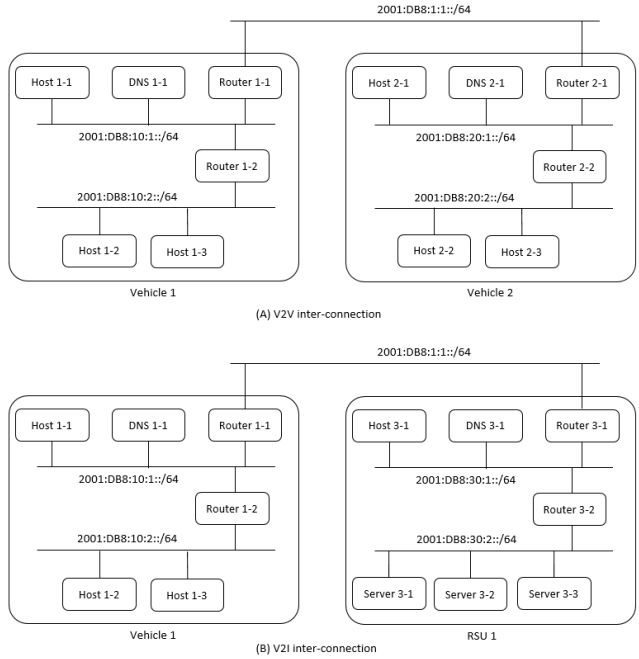


Figure 2: IPWAVE Architecture – V2V and V2I Inter-Connection

autoconfiguration, unicast and multicast address mapping, and the subnet structure.

From a privacy perspective, pseudonyms are used for MAC addresses and the corresponding IPv6 addresses. The pseudonyms need to be sufficiently randomized: for this purpose they should be generated with a hash function or a random number generator. Changing the pseudonym periodically intends to make it difficult for adversaries to track and/or identify a vehicle [16]. At the same time, the continuity of the ongoing communication must be ensured while the pseudonym changes. This is an essential requirement because even a short interruption of the communication can negatively affect the vehicle's operation and safety, especially when the vehicle is moving at high speed. It should be noted that the change of pseudonym for the MAC address on the 802.11 OCB mode interface necessarily results in the change of all the interface identifiers of the IPv6 addresses assigned to that interface.

From a security perspective, [13] reconfirms that the absence of security mechanism in 802.11 OCB mode is expected to be covered at the higher layer as specified in IEEE 1609 and ETSI ITS. At the same time, it also suggests to

provide security at the network layer by combining e.g. IPsec with a Public Key Infrastructure (PKI) to establish and manage credentials.

2.3 IEEE 1609 and ETSI ITS

The IEEE 1609 and ETSI ITS specifications define the upper layers for V2X communications running on top of the 802.11 OCB mode. Both IEEE 1609 and ETSI ITS have been published for several years; these standards are well studied and numerous articles have been published by governments, industry and academia. Abboul et al. [5] present a summary table that lists the standards and spectrum allocations for the US, Europe, and Japan. Therefore, we focus mainly on the more recent discussions on security.

For IEEE 1609, the security aspects are defined in the 1609.2 specification [15]. It defines the security framework for V2X communication, including secure data service, message format and security processing of V2X messages such as encryption and signing of messages, and certificate distribution and management (e.g. CRL). A large part of the security solution in [15] is built on top of a PKI: it defines certificates and associated mechanisms, such as generation, distribution, verification, usage, revocation, and other related management functions. The latest version of the overall certificate management solution adopted in IEEE 1609.2 is described in [7]. It covers general V2X scenarios with details on certificate provisioning and revocation management.

For ETSI ITS, the direct communication, called GeoNetworking, is defined in EN 302 636. The security aspects are specified separately in multiple documents: overall security architecture (TS 102 940), trust and privacy management (TS 102 941), access control (TS 102 942), confidentiality (TS 102 943), security header and certificate format (TS 103 097). ETSI ITS also adopts a PKI-based security architecture that is very similar to IEEE 1609.

Certificate management

The PKI-based V2X security architecture, and in particular the credential management aspects have been studied extensively. One of the key issues of PKI-based solution is the handling of revocation, which is typically achieved through a Certificate Revocation List (CRL). This is significant in vehicle communication environment given that possible damage caused by compromised but otherwise legitimate devices and other malicious entities can cause disruption in vehicle communication, which may result in physical damages or even loss of lives. The analysis in [12] refers to IEEE 1609.2 and states that there is

no standardized solution for certificate revocation and no defined mechanism exists to revoke pseudonyms. Statements such as these imply that the handling of certificate revocation is left up to implementation, which may result in a varying degree of effectiveness in real deployment. Festag et al. [8] analyze the Geocast communication in ETSI ITS and conclude that the largest processing overhead is created by certificate verification. There are also other proposals for improved credential management mechanisms; one example is Khodaei et al. [11].

Several papers discuss the security aspects of these standards and point out security issues. For example, Serban et al. [14] identify shortcomings in the ETSI ITS security specifications and show scenarios of a possible replay attack on the enrollment process. They propose that ETSI ITS should add details on how to preclude such an attack. Alnasser et al. [6] present a comprehensive analysis of the security issues in the 802.11 OCB mode-based system (namely WAVE and ETSI ITS) as well as the LTE-based cellular V2X (C-V2X) system; they also suggest solutions to address these issues.

2.4 Cellular-based: LTE V2X

3GPP started specification work on V2X communication as a part of Release 14 in 2015. The overall LTE-based V2X architecture is defined in TS 23.285 [3]. The architecture introduces two new dedicated entities to manage the V2X User Equipment (UE), namely the V2X Control Function and the V2X Application Server (AS). The overall architecture for the non-roaming and roaming scenarios are shown in [3]. A simplified version of the overall architecture is shown in the left hand side of Fig. 3 to illustrate the key relationship among the V2X UEs and these newly defined entities. It should be noted that Fig. 3 contains a simplified version of the version [3] ; it ignores details such as the type of UEs (i.e. On-Board Unit (OBU), RSU, pedestrian, etc.) to make the figure simpler. LTE V2X supports both LTE-Uu- and PC5-based communication. In the former case, both unicast and multicast are possible.

It should be highlighted that the Uu interface has been the only mode of communication in the traditional cellular network until the emergence of the Proximity Service (ProSe) in Release 13. This "macro" connection between the UE and the base station is what differentiates it from the 802.11 OCB mode / IEEE 1609 / ETSI ITS architecture where short-range direct communication between vehicles and other entities such as RSU was the only communication mode. In this respect, the existence of both PC5 (short-range) and Uu (macro) connections make it possible to envision expanded use case scenarios that may have not been possible with direct short-range communication only.

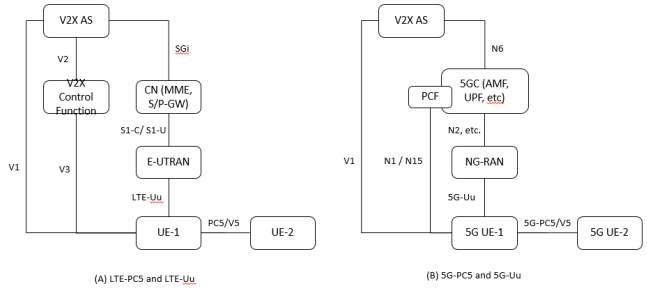


Figure 3: V2X Reference Architecture

The V2X Control Function is mainly responsible for configuring the V2X UE for both LTE-Uu and PC5 interfaces. The V2X UE can be configured in several ways: 1) pre-configured in the Mobile Equipment (ME), i.e. mobile handset as hardware, 2) configured in the USIM, 3) provided by the V2X control function to the ME, or d) a combination of the previous options. The last option, i.e. the combination of configuration methods, allows the V2X control function to update the UE configuration later on, if necessary.

Authorization of LTE V2X communication

The V2X UE is authorized prior to the use of V2X communication. This authorization applies to both the PC5 interface for direct communication with other V2X UEs and the LTE-Uu interface for traditional communication to the gNB. According to TS 23.285 [3] and TS 24.386 [1], the authorization procedure is initiated by the requesting V2X UE by sending a provisioning request to the V2X control function. In response to this request, the V2X control function provisions the Managed Object (MO) for the PC5 interface to the UE. The successful completion of the provisioning is considered as an authorization by the network to use the PC5 interface. If the UE is not allowed to use V2X communication for any reason, the V2X control function does not provide the MO to the V2X UE.

The validity timer of the configuration parameters ensures that the V2X UE periodically contacts the V2X control function in the network to obtain a valid up-to-date configuration.

Security and privacy in PC5 communication

The PC5 interface was originally defined to address the needs of public safety communication starting from Release 12. ProSe was specified in 3GPP for this purpose. With the emergence of V2X in Release 15, the original ProSe function was adopted also cover the needs of the automotive industry. It resulted in a part of the TS 33.185 [2] specification. One notable difference in ProSe usage in V2X from the public safety option is comparable to the 802.11 OCB mode specification. The original ProSe feature includes functionalities such as discovery of proximity UEs, the establishment of an association between them, and the establishment of a secure cryptographic channel for one-tomany communication. However, in order to meet the needs of the V2X use case where the device association is expected to change dynamically and can be short-lived as vehicles moves at higher speed, much of the communicationestablishment phases, including the security aspect, are removed to allow UEs to send messages quicker. Similar to the 802.11 OCB mode, the underlying assumption is that the necessary security functionalities are covered at the higher layers.

From a privacy perspective, similar to IEEE 1609 and ETSI ITS security architecture, the 3GPP V2X system also supports pseudonyms in the PC5 interface to protect the privacy of the V2X UE in direct communication and to protect the user from being tracked or identified by other UEs. It is achieved by periodically changing the layer-2 ID and source IP address. The timer T5000 is defined for this purpose. Upon expiration of this timer, the V2X UE changes its layer-2 ID and corresponding IPv6 address, followed by restarting the timer. Its default value is 300 seconds (5 minutes) according to TS 24.386 [1]. It should be noted that, unlike in IEEE 1609 or ETSI ITS, no pseudonym certificate is required in the 3GPP V2X architecture, as the layer-2 ID and the IP address are generated and assigned in the V2X UE itself as specified in [1].

Security and privacy in the LTE-Uu interface

In the LTE-Uu interface used in V2X communication, the existing EPS security solution is applied as defined in TS 33.185 [2]. In other words, there is no specific privacy and security enhancement in the LTE-Uu interface, at least for Release-15 time period.

2.5 Cellular-based: 5G V2X

3GPP started the standardization work for 5G-based V2X in early 2018 as part of 5G phase 2. At the time of the writing of this paper, the system

architecture work for 5Gbased V2X is in progress. 5G-based V2X will naturally utilize equivalent functionalities as in the LTE system such as the Multimedia Broadcast Multicast Service (MBMS) and the PC5 interface. However, it should be noted that MBMS and ProSe for 5G have not yet been standardized as they were not a part of the phase 1 scope. This implies that both these functionalities need to be first defined for the 5G system in order to fully define the V2X functionalities in 5G. This involves both radio and system aspects.

The 5G V2X architecture is defined in TS 23.287 [4] (work in progress). According to [4], the V2X specific functional entity that was originally defined in LTE V2X architecture [3] is absorbed into the existing entities in the 5G system, namely the Policy Control Function (PCF). The right hand side of Fig. 3 illustrates the 5G V2X architecture as a simplified version of what is captured in [4]. It should be compared against the LTE version in the left hand side of the figure. The 5G V2X architecture also defines the interworking with the LTE V2X system to ensure 5G V2X is backward compatible. In this figure, we are using the naming convention "5G-Uu" and "5G-PC5" to clearly differentiate them from the counterpart in the LTE system. Note that the description in TS 23.287 [4] is unclear on this point.

Authorization and provisioning of 5G V2X communication

The general principle to authorize and provision the UE for 5G-Uu and 5G-PC5 interfaces is equivalent to that in the LTE system as described in the previous section. One difference is that the entity that authorizes the UE is the PCF in 5G instead of the V2X Control Function in LTE. Also, authorization of the UE depends whether the UE is under the coverage of E-UTRAN (i.e. LTE Radio Access Network (RAN)) or 5G New Radio (NR), i.e. 5G RAN.

Privacy in PC5 communication

Privacy in 5G PC5 communication is not explicitly defined in TS 23.287 [4]. However, we consider the same type of privacy protection (i.e. periodic change of the layer 2 identity and the corresponding IPv6 address) is also applied in 5G PC5.

Security aspect of 5G V2X

Work is in progress on the security aspect of 5G V2X as 5G Phase 2 in Release 16. The actual specification is not yet available. It is the subject of future work.

3 Security Consideration on The Hybrid Approach

IEEE 1609 and ETSI ITS systems based on 802.11 OCB mode focus on the direct communication between vehicles (V2V) and infrastructure (V2I) as the sole communication mode. On the other hand, cellular-based solution provides both wide area communication (Uu interface) and a direct communication capability (PC5 interface) for which the latter facilitates the functionality equivalent with the 802.11 OCB mode.

Recent work, such as Abboud et al. [5], suggests a hybrid system in which 802.11 OCB mode based and cellular based systems to co-exist. However, from a security perspective, the fundamental security architectural approaches are different. The 802.11 OCB mode does not provide any security mechanism in layer 1 and layer 2 under the assumption that they are provided at the higher layers. The higher layer – IEEE 1609 and ETSI ITS systems – are built around PKI, and much of the security mechanism in these higher-layer standards is focused on the credential management. The PC5 interface in cellular-based solutions is similar in this respect. On the other hand, the security solution in the Uu interface is based on the secret key and other unique information associated with individual subscription stored in USIM; it uses Authentication and Key Agreement (AKA) procedures to establish cryptographic keys per UE based on symmetric cryptography. In other words, the cellular system does not use PKI and asymmetric cryptography (at least until 5G in limited scope – it is outside the scope of this paper). These differences in these two systems need further analysis. For example, if a cellularbased solution is used as an alternative lower layer to carry upper layer protocols as defined in IEEE 1609 and ETSI ITS, the overall security solution may need further study to validate its effectiveness.

Moreover, the recent IETF Internet Drafts on the use of IPv6 focus solely on the 802.11 OCB mode. However, the cellular-based V2X solution also uses IPv6. In this respect, these Internet Drafts also need to take the cellular-based solution into consideration.

As for the V2X solution, the 3GPP work on the study of security of 5G V2X is currently in progress. Its discussion and outcome need to be taken into account for the overall 5G V2X solution.

4 Conclusion and Future Work

This paper discusses the recent development of V2X related standardization and summarizes the two main technology solutions. It also presents the similarities and differences between 802.11 OCB mode / IEEE 1609 / ETSI ITS and the cellular LTE / 5G architectures from a security perspective. It highlights the areas that need further work, primarily based on the differences in the two technology solutions.

In addition, the 3GPP work on 5G-based V2X architecture is currently in progress. The outcome of this study and any differences from the LTE V2X architecture will need to be examined as the future work.

References

[1] 3GPP. TS 24.386, User Equipment (UE) to V2X Control Function; Protocol Aspects; Stage 3, v15.2.0. Technical report, 3rd Generation Partnership Project, 12 2018.

[2] 3GPP. TS 33.185, Security Aspect for LTE Support of Vehicle-to-Everything (V2X) Services, v15.0.0. Technical report, 3rd Generation Partnership Project, 06 2018.

[3] 3GPP. TS 23.285, Architecture Enhancements for V2X Services, v15.3.0. Technical report, 3rd Generation Partnership Project, 03 2019.

[4] 3GPP. TS 23.287, Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services, v0.2.0. Technical report, 3rd Generation Partnership Project, 03 2019.

[5] Khadige Abboud, Hassan Aboubakr Omar, and Weihua Zhuang. Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey. *IEEE Transactions on Vehicular Technology*, 65(12):9457–9470, 2016.

[6] Aljawharah Alnasser, Hongjian Sun, and Jing Jiang. Cyber Security Challenges and Solutions for V2X Communications: A Survey. *Computer Networks*, 151:52–67, 2019.

[7] Benedikt Brecht and Thorsten Hehn. A Security Credential Management System for V2X Communications. In *Connected Vehicles*, pages 83–115. Springer, 2019.

[8] Andreas Festag, Panagiotis Papadimitratos, and Tessa Tielert. Design and Performance of Secure Geocast for Vehicular Communication. *IEEE Transactions on Vehicular Technology*, 59(5):2456–2471, 2010.

[9] IEEE. IEEE Standard 802.11-2016 - IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Technical report, Institute of Electrical and Electronics Engineers, Piscataway, NJ, United States, 2016.

[10] Jaehoon Paul Jeong, Nabil Benamar, Sandra Cespedes, Jerome Haerri, Dapeng Liu, Tae (Tom) Oh, Charles E. Perkins, Yiwen Chris Petrescu, Alexandre Shen, and Michelle Wetterwald. IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases, draft-ietfipwave-vehicular-networking-08.pdf. IETF draft, Internet Engineering Task Force, 03 2019.

[11] Mohammad Khodaei, Hongyu Jin, and Panagiotis Papadimitratos. SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems. *IEEE Transactions on Intelligent Transportation Systems*, 19(5):1430–1444, 2018.

[12] Mohammad Khodaei and Panos Papadimitratos. The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems. *IEEE Vehicular Technology Magazine*, 10(4):63–69, 2015.

[13] Alexandre Petrescu, Nabil Benamar, Jerome Haerri, Jong-Hyouk Lee, and Thierry Ernst. Transmission of IPv6 Packets over IEEE 802.11 Networks Operating in Mode Outside the Context of a Basic Service Set (IPv6-over-80211-OCB)", draft-ietf-ipwave-ipv6-over-80211ocb-36.pdf. IETF draft, Internet Engineering Task Force, 04 2019.

[14] Alexandru Constantin Serban, Erik Poll, and Joost Visser. A Security Analysis of the ETSI ITS Vehicular Communications. In *International Conference on Computer Safety, Reliability, and Security*, pages 365–373. Springer, 2018.

[15] IEEE Vehicular Technology Society. Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Services. Technical specification, Institute of Electrical and Electronics Engineers, Piscataway, NJ, United States, 03 2016.

[16] Carmela Troncoso, Enrique Costa-Montenegro, Claudia Diaz, and Stefan Schiffner. On the Difficulty of Achieving Anonymity for Vehicle-2-X Communication. *Computer Networks*, 55(14):3199–3210, 2011.

Publication

A New Privacy Enhancing Beacon Scheme in V2X Communication

Publication Data

Yoshizawa, T., Singelée, D., and Preneel, B. A New Privacy Enhancing Beacon Scheme in V2X Communication. In Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, pp. 139–151, 2021.

Contributions

- Principal author.

A New Privacy Enhancing Beacon Scheme in V2X Communication

Takahito Yoshizawa, Dave Singelée, and Bart Preneel

KU Leuven, ESAT/COSIC, Leuven, Belgium

Abstract. We propose a new privacy-enhancing beacon scheme in Vehicle-to-Everything (V2X) communication systems and evaluate its effectiveness based on a simulation. With this scheme, vehicles dynamically adjusts their periodic transmission of Cooperative Awareness Message (CAM) and Basic Safety Message (BSM) messages based on the observation of surroundings and transmit these messages only when it is necessary. This new scheme addresses the gap in standards where continuous transmission of broadcast-based unencrypted vehicle information is assumed but may not be needed under certain circumstances. Our beacon message does not convey any privacy-linking information. This way, this new scheme enhances privacy protection of vehicle owners by limiting the transmission of information that can be linked to a particular vehicle. The complexity of its processing in both transmitting and receiving ends is kept at minimum and is simpler than CAM and BSM processing. Our simulation result indicates that this new scheme is highly effective if the density of vehicles with V2X technology is limited.

1 Introduction

V2X communication offers a service in which vehicles periodically broadcast its presence to surrounding vehicles. These messages are defined as Cooperative Awareness Messages (CAMs) in ETSI EN 302 637.2 [10] in Europe and as Basic Safety Message (BSM) in SAE J2735 [18] in the US, respectively [5]. Vehicles within communication range exchange these messages to construct and maintain a dynamic map of the presence of vehicles. Vehicles' situational awareness as the result of these message exchanges leads to an overall improvement in road safety. To establish this awareness, CAM and BSM contain vehicle information such as position, speed, direction, and acceleration. In addition, they also contain vehicle's physical characteristics such as vehicle type, its length and

width [9]. These messages are digitally signed using certificates issued by a management system for authenticity. From a privacy perspective, information in CAM and BSM allows receiving vehicles to discern the sending vehicle by examining the message content and correlate it with sensory observations. Due to its broadcast nature, these messages are sent in clear. It implies that any suitable device, legitimate or not, can receive them. This condition enables adversaries to receive, collect, and analyse these messages from all transmitting vehicles within communication range.

Vehicles exchange these messages to establish and maintain awareness of one another. In other words, CAM or BSM transmission is meaningful only when there are other vehicles within the communication range from a given vehicle. However, this is not always the case. For example, there are situations where no vehicle is present within the communication range for extended period of time. This no- or low-traffic condition includes scenarios such as: 1) late night, 2) small town and rural areas, 3) quiet residential areas, and 4) early days of V2X technology introduction. Under these conditions, transmitting CAMs or BSMs achieves no useful purpose. On the contrary, doing so may result in exposing vehicle information to passive adversaries. In this paper, we propose an alternative approach to this problem in such a way that the exposure of privacy information is prevented whenever possible. Our proposed beacon scheme does not contain any vehicle-specific information, not even a temporary identifier or pseudonym. Using extensive simulations, we show that the new approach is effective under various conditions.

The rest of the paper is organized as follows. Section 2 discusses the existing literature as a background information for Sect. 3 in which we describe the new beacon scheme. In Sect. 4, we discuss the simulation results to evaluate the effectiveness of the beacon scheme, followed by conclusion in Sect. 5.

2 Related Work

Various solutions for privacy protection and trustworthiness in V2X communication have been proposed in existing literature. Privacy protection hinges on the effective use of pseudonyms to prevent or minimize the leak of privacy-related information. It includes various pseudonym change schemes. A *mix zone* [4] is a defined area, such as an intersection. Vehicles within the mix zone collaborate and change pseudonyms at the same time. Presence of multiple vehicles moving in different directions around an intersection while changing pseudonyms makes tracking more difficult. In a *silent period* [11], a vehicle stops transmission for a pre-defined time period when a pseudonym is changed.

Doing so prevents a change of pseudonym from being immediately observable. *Decoy traffic* [12] refers to transmitting CAMs for one or more non-existing vehicles to make it appear as if there are more vehicles. *Location obfuscation* [3] is a technique to intentionally report incorrect location information during the pseudonym change. Reporting fake location information thwarts adversaries from correlating pseudonyms before and after the change. In *Transmission range adjustment* [2], a vehicle reduces its transmission power to reduce the number of vehicles that can observe it.

From the trustworthiness perspective, multiple elaborate schemes have been proposed to ensure that received messages are trustable in V2X communication while protecting privacy of vehicles involved. Threshold anonymous announcement (TAA) [6] is a mechanism to verify uniqueness of message origin based on a message signature using direct anonymous attestation (DAA). It allows receiving vehicles to determine the message validity using threshold, i.e. the number of endorsement of a message by other receiving vehicles while remaining anonymous. Message linkable group signature (MLGS) [21] is a group signature scheme that also uses threshold as the measure of message trustworthiness. This scheme ensures that a vehicle can endorse a given received message only once, thus prevents from adversaries from artificially altering the endorsement outcome. Another group signature scheme in [16] enables efficiently sign and verify V2V messages while maintaining group members' privacy. A reputation-based scheme [14] is another approach. It allows vehicles to send feedback of whether they consider a given message by a sender as trustable or not. This feedback can be either positive or negative. Based on multiple such feedbacks, a sender's reputation is derived. Receiving vehicles consult this reputation upon determining whether accept messages from the sender or not. Balancing trust management and privacy preservation (BTMPP) [15] is another reputation-based scheme. It specifically focuses on the trustworthiness of emergency messages. Its reputation is also based on feedbacks from receiving vehicles while preserving privacy of them.

2.1 Our contribution

The existing schemes we discussed above can be characterized as follows. For privacy protection, the overall approach revolves around pseudonym usage and how to obscure the change from one to another to maintain the unlinkability property. For trustworthiness, the focus is on addressing how receiving ends of the communication can determine whether to accept or reject received messages. Contrary to these solutions, we approach the privacy protection problem from a completely different angle. To the best of our knowledge, this is the first of

its kind to propose this type of approach to this problem. In our new scheme, vehicles

- observe its surrounding to judge whether V2X transmission is warranted or not,
- refrain from transmission when observation indicates as such, thus minimizing potential exposure of privacy information,
- continue to observe its surrounding and adjust its transmission behavior as needed.

3 New Beacon Scheme

3.1 Overview

In our proposed beacon scheme, we apply the discovery concept in Proximity Service (ProSe) specified by the 3rd Generation Partnership Project (3GPP). ProSe allows direct communication between mobile devices [1]. Its original application was for public safety, but it was later extended to support V2X communication. Upon applying ProSe to V2X, some functionalities were removed to allow instantaneous communication with low overhead. This reduced functionality in ProSe in V2X is analogous to the relationship between the conventional IEEE 802.11 operation and 802.11 OCB mode (former 802.11p) [7]. Specifically, discovery, association, and security related procedures are omitted for V2X purpose in which communication duration among moving vehicles is expected to be short and the overhead to establish communication needs to be minimal.

In our proposed scheme, we apply the ProSe discovery model A (*"I am here."*) [1]. Its sole purpose is to announce the presence of a vehicle. Beacon messages sent by vehicles are identical; they contain no vehicle-specific or unique information. As with CAM, they are broadcast messages sent in clear. Therefore, this new beacon mechanism needs to ensure secure operation and should not negatively impact the exchange of CAMs.

At a high level, the proposed beacon scheme is a two-tier process – the first is beacon transmission and reception; the second is verification of vehicle presence and subsequent decision to select beacon or CAM transmission. In the first tier step, vehicles announce their presence by transmitting beacons, and detect the potential presence of other vehicles by receiving them. Because beacons are not unique per vehicle and can also be sent by adversaries, simply receiving

them does not guarantee that vehicles are present. In the second tier step, vehicles verify actual presence of vehicles using opportunistic and provisional CAM transmission and reception. If the result of this verification indicates that at least a minimum number of vehicles are actually present, vehicles commit to CAM transmission (*CAM mode*). Otherwise, they fall back to beacon transmission (*beacon mode*). Vehicles continue to monitor incoming messages and adjust its transmission mode as needed. To avoid rapid and frequent changes in the vehicle's transmission mode due the dynamically changing RF environment in moving traffic, pre-determined threshold and hysteresis are used to make this decision.

3.2 Security Properties of the Beacon Scheme

From security perspective, we identify the following desired properties of the beacon operation in our analysis.

1. beacon messages need to accurately reflect the actual vehicle presence.
2. beacon messages transmitted by active adversaries do not negatively influence honest vehicles' behavior.
3. beacon messages enhance security and privacy protection compared to the current CAM transmission alone.
4. beacon message transmission does not introduce any new security issues or negative side effects to the V2X communication.
5. beacon message processing is no more complex than CAM processing.

Property 1 and 2 are closely related. The only purpose of beacon messages is to announce its presence to vehicles within the communication range. Therefore, they need to accurately reflect the actual vehicle presence. On the other hand, due to its nature of broadcasting identical unencrypted messages by all vehicles, active adversaries can also generate and transmit, or replay, beacons to make ghost vehicles appear. In this sense, it is important that adversaries do not negatively influence honest vehicles.

In addition, property 3 and 4 requires that there are clear benefits of introducing the new beacon scheme from security and privacy perspectives. Moreover, we need to ensure that the introduction of this scheme does not result in any negative side effect or new security issues.

Finally, property 5 requires the processing of beacon messages should be simple, lightweight, and no more complex than CAM processing for both transmitting

and receiving vehicles. Strictly speaking, it does not fall under security or privacy. However, it is nonetheless important to prevent additional overhead.

3.3 Adversary Model

For real-world application, the solution needs to be resistant against adversaries. For this purpose, we assume the presence of Local Active Adversaries (LAA) with limited capabilities and Global Passive Adversaries (GPA).

An LAA has one or more devices installed at road side at fixed locations. They can actively transmit beacon messages to entice honest vehicles to transmit CAMs. A device can transmit beacons locally without coordinating with other devices, thus it is a local adversary. Further, we assume that they do not have access to the legitimate certificates and corresponding private keys, thus they cannot transmit valid CAMs. Hence the adversary is an LAA with limited capabilities

A GPA has a set of devices installed along roads at fixed locations. They can passively collect and analyse CAMs from vehicles within the communication range. When vehicles pass by one of these devices while transmitting CAM at regular intervals, the device detects the presence of these vehicles with specific information from received messages. Using timestamp, adversary devices may share and aggregate information over a wider area. This way, they may be able to construct the recurring appearance of a vehicle (i.e. pseudonym) at various locations and time, such as a commuting pattern. They are passive devices that only monitor incoming messages but collaborate with other devices at multiple locations, hence GPA.

3.4 Beacon Scheme Algorithm

Algorithm 1 illustrates the beacon operation. A vehicle starts with *beacon mode* by default, and hysteresis counter for CAM (d_{CAM}) and for beacon (d_{Beacon}) are reset (line 1,2). The vehicle checks the presence of other vehicles by monitoring the channel for n seconds and count the number of received CAM (N_{CAM}) and beacon messages (N_{Beacon}) (line 4∼6). Lines 8 through 20 describe the vehicle behavior when it is in *beacon mode*. If N_{CAM} is above threshold (th_C) for longer than hysteresis period (hy_C), then the vehicle switches to *CAM mode* (line 8∼11). On the other hand, if N_{Beacon} is above threshold (th_B) for longer than hysteresis period (hy_B), then the vehicle transmits CAMs with probability p (line 12∼17). This is a provisional transition to *CAM mode*. If the detected number of vehicles (N_{Beacon} or N_{CAM}) falls below the threshold

Algorithm 1: Switching between CAM and Beacon Mode

Result: determine CAM or Beacon to send

```
txMode ← "Beacon";
d_CAM, d_Beacon ← 0;
repeat
    monitor V2X channel for n seconds;
    N_CAM ← number of CAMs received;
    N_Beacon ← number of Beacon messages received;
    if (txMode="Beacon") then
        // handling when current txMode="Beacon"
        if (N_CAM > th_C) & (d_CAM > hy_C) then
            txMode ← "CAM"; d_CAM ← 0; // switch to CAM
        else if (N_CAM > th_C) & (d_CAM <= hy_C) then
            d_CAM ← d_CAM + n;
        else if (N_Beacon > th_B) & (d_Beacon > hy_B) then
            nextMsg ← coinToss(p); d_Beacon ← 0;
            if (nextMsg == "CAM") then
                txMode ← "CAM"; // provisional switch to CAM
        else if (N_Beacon > th_B) & (d_Beacon <= hy_B) then
            d_Beacon ← d_Beacon + n;
        else
            d_Beacon, d_CAM ← 0;
        end
    else
        // handling when current txMode="CAM"
        if (N_CAM <= th_C) & (d_CAM > hy_C) then
            txMode ← "Beacon"; d_CAM ← 0; // switch to beacon
        else if (N_CAM <= th_C) & (d_CAM <= hy_C) then
            d_CAM ← d_CAM + n;
        else
            d_CAM ← 0;
        end
    end
    switch txMode do
        case "CAM" mode do send CAMs;
        case "Beacon" mode do send Beacon messages;
    end
until arrives at destination;
```

(th_B or th_C) before the hysteresis condition (hy_B or hy_C) is reached, then the hysteresis values (hy_C, hy_B) are reset (line 19).

The provisional transitions to *CAM mode* verifies the vehicle's existence to other vehicles. During the next monitoring period, vehicles verify that received CAMs from other vehicles which also transition to *CAM mode* provisionally or already in that mode. Using the certificate and vehicle-specific information contained in each CAM, receiving vehicles can deduce the actual number of vehicles present within the communication range. Under the assumption of LAAs with limited capabilities as stated in Sect. 3.3, all valid CAMs are considered as legitimate and honest vehicles.

Lines 21∼29 describe the vehicle behavior when it is in *CAM mode* and is actively transmitting CAMs. If N_{CAM} falls below the threshold (th_C) longer than the hysteresis period (hy_C), then the vehicle falls back to *beacon mode*; otherwise, it stays in the *CAM mode*. If N_{CAM} exceeds the threshold before the hysteresis condition (th_C) is reached, then the hysteresis value (hy_C) is reset (line 27), avoiding rapid and frequent change of mode. Finally, the vehicle transmits the selected mode based on the previous steps (line 30∼33). This cycle repeats until the vehicle reaches its destination.

3.5 Consideration on Security Properties

In this section, we discuss how the proposed beacon scheme addresses the stated security properties in Sect. 3.2. Property 1 and 2 are addressed by the two-tier process discussed in Sect. 3.1. LAAs may transmit fake beacons to entice honest vehicles to transmit CAMs. However, if the second tier process indicates that the actual number of vehicles does not meet the minimum threshold (th_C), vehicles remains in *beacon mode*. This way, the impact of LAAs can be mitigated. During this period, each vehicle in *beacon mode* provisionally transmits CAMs with a probability of p. If this value is set high, more vehicles will provisionally transmit CAMs, i.e higher chance of honest vehicles falling victim to LAAs. Therefore, p needs to be sufficiently low. However, lower p value implies a situation where the number of detected vehicles will fall short of the actual vehicle presence. As p decreases, this condition is pronounced further. In this case, more honest vehicles need to be present to cross the threshold. Under a marginal situation where the detected number of vehicles is around the threshold, it may delay the CAM transmission with lower p value when ($N_{CAM} > th_C$) condition is already met in reality. This is a fine balance to attain as delayed transition implies potential impact to safety applications that rely on CAMs. This is a trade-off between privacy protection and safety

Table 1: Simulation Parameters

Parameter	Value
City size	large, small
Opportunistic CAM transmission prob. (p)	30, 50, 70, 90%
Mode switch threshold (th_C)	1∼7 vehicles
Average passenger vehicle length	4.18 m
Average truck length	10.71 m
Passenger vehicle vs. truck ratio	80%, 20%
Vehicle buffer space	5 m
Road capacity	95 vehicle/km/lane
Drive distance (1 way)	30.0 km
Number of lanes	1, 2, or 3
Ratio of 1/2/3-lane roads	25%, 50%, 25%
Beacon transmission rate	1 msg/sec
Vehicle monitor interval	1 sec
Mode switch hysterisis (hy_C)	3
Inter-GPA distance	800 m
V2X communication distance	300 m
Repeat per run	10 times

applications to maximize the benefit of the former while minimizing impact on the latter.

Regarding property 3 and 4, beacon messages enhance privacy protection of vehicle as the beacon scheme ensures that CAMs are sent only when they are indeed necessary and useful to achieve its purpose, i.e. exchange information with other vehicles. If the number of vehicles does not meet the condition, no privacy-relevant information is transmitted. Regarding property 5, it is clear that beacon message processing is simpler from both transmitting and receiving vehicles' perspectives. Beacon messages is static and do not contain any vehicle-specific dynamic information, such as vehicle's speed and direction. Therefore, processing is much simpler than CAM processing.

4 Simulation

4.1 Approach

Table 1 lists the set of parameters used in our simulation. We conducted driving in two different settings: a large city and a small city. In both cases, we used

Table 2: Traffic Congestion in Brussels by Time of the Day (2019)

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
0:00	4%	3%	4%	4%	5%	6%	7%
1:00	1%	2%	1%	2%	2%	3%	5%
2:00	1%	2%	1%	1%	1%	2%	3%
3:00	0%	1%	1%	1%	1%	1%	2%
4:00	0%	1%	1%	1%	1%	1%	1%
5:00	3%	3%	3%	3%	3%	1%	1%
6:00	22%	24%	22%	24%	18%	2%	1%
7:00	56%	58%	52%	57%	45%	4%	1%
8:00	77%	83%	70%	81%	63%	6%	2%
9:00	50%	55%	46%	56%	41%	12%	5%
10:00	30%	34%	31%	37%	32%	19%	10%
11:00	28%	28%	32%	34%	35%	25%	14%

(continue to the next column)

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
12:00	29%	30%	43%	37%	41%	28%	16%
13:00	28%	29%	40%	36%	41%	28%	17%
14:00	30%	32%	38%	38%	46%	30%	19%
15:00	44%	47%	45%	53%	62%	30%	19%
16:00	59%	66%	59%	72%	75%	29%	20%
17:00	71%	80%	73%	86%	75%	30%	25%
18:00	54%	64%	64%	72%	59%	31%	26%
19:00	23%	30%	34%	38%	36%	26%	19%
20:00	9%	12%	13%	14%	18%	16%	12%
21:00	6%	8%	8%	9%	12%	11%	8%
22:00	7%	9%	9%	11%	11%	11%	7%
23:00	5%	7%	7%	9%	10%	10%	5%

values 1 through 7 for th_C. The average length for passenger vehicles was obtained by taking an average of full-size, mid-size, small, and mini vehicle lengths [8]. The average truck length was obtained from taking an average of class 1 and class 2 trucks [13]. We made an assumption that the ratio of passenger vehicles and trucks on the road is 80% to 20%, and each vehicle has a buffer space of 5 meters in front of it. Using these values, the vehicle density is obtained as 95 vehicles/km/lane. We also assumed the number of lanes vary with the ratio of 1, 2, and 3-lane roads of 25%, 50%, and 25% of the travel.

We simulated a vehicle's behavior as described in Algorithm 1 in Sect. 3.4 in

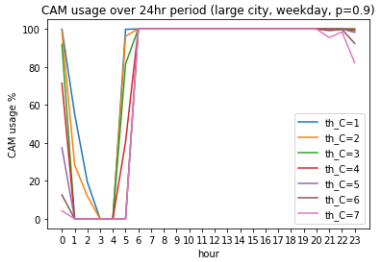
a round-trip drive with distance of 30.0 km one way. It transmits beacons at a rate of 1 message/sec, and monitors the V2X channel for a period of 1 sec. A hysteresis threshold (hy_C) of 3 is used. We assume a maximum V2X communication distance of 300 m [19]. For the large-city scenario, we used the actual data of weekly traffic congestion in Brussels in 24 hours over a 7-day period. Table 2 shows this statistics [20] (green/yellow/red for low/medium/high density). For the small-city scenario, we scaled it down to model a city having one-tenth of the traffic in Brussels. Using these data, we simulated a round-trip drive for each hour over a 7-day period.

4.2 Discussion and Evaluation

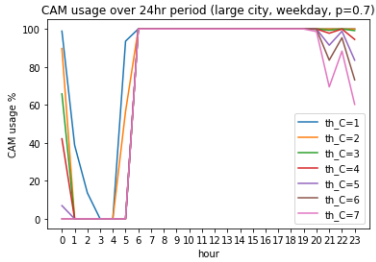
Figures. 1, 2 illustrate the use of CAM in a large and a small city for weekdays over 24 hour period with decreasing value of p, respectively[1]. Lines in each figure represent th_C values. Table 2 shows low traffic period is between 9 PM and 5 AM next morning each day. Driving in this period makes vehicles switch to and stay in *beacon mode* as shown in these two figures, i.e. the main contributor to the reduced CAM usage. As th_C value increases from 1 to 7, vehicles switch to *beacon mode* progressively earlier in the evening. On the contrary, in Fig. 1, the use of CAMs continues throughout the day time in a large city irrespective of th_C value, while Fig. 2 shows that the traffic in a small city reduces between 10 AM to 2 PM to an extent that vehicles switch to *beacon mode* during this period. This further reduction of CAM usage in a small city indicates that our beacon scheme is more effective in lower traffic environment in reducing exposure of vehicle information to GPAs.

Figure 3 summarizes the reduction of CAM transmission in both large and small cities during weekdays with the same set of p values as in previous two figures. Figure 3(b) clearly highlights a larger reduction of CAM in a small city. It reflects the lower traffic condition during late night and early afternoon period as shown in Fig. 2. On the contrary, CAM reduction in a large city is limited up to approximately 40% with increasing value of th_C as shown in Fig. 3(a). This limited effectiveness in a large city reflects the situation where use of beacons occurs in early morning hours only as seen in Fig. 1 where a lower p value has no influence to the consistent use of CAM throughout the day time. On the other hand, the CAM reduction in a small city in Fig. 3(b) is more significant. Even for $th_C = 1$ and $p = 0.9$, the CAM reduction already starts from approximately 40%. This is another data point showing that the beacon scheme is more effective in a reduced traffic environment. In other

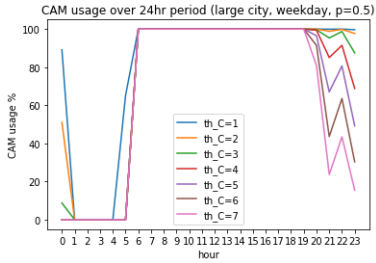
[1]Our simulation results also include weekend traffic pattern. However, as the result is similar to weekdays and does not add significant insights, we omit including the figures and discussion.



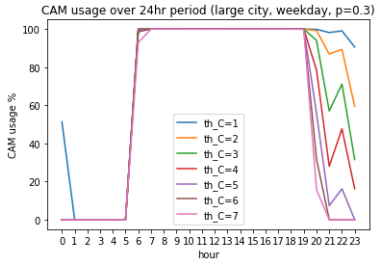
(a) $p = 0.9$



(b) $p = 0.7$



(c) $p = 0.5$

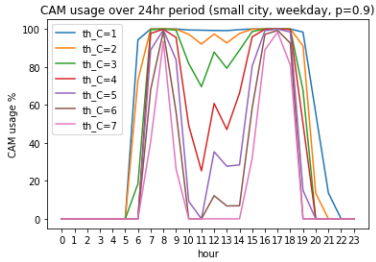


(d) $p = 0.3$

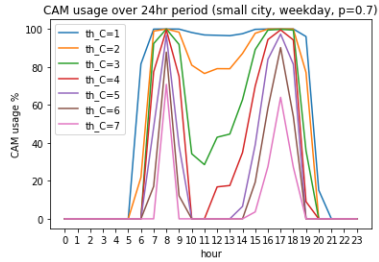
Figure 1: CAM Usage over 24hr Period (Large City, Weekdays)

words, a lower traffic condition, such as in small cities, rural areas, and quiet residential areas, benefits more from the use of our beacon scheme. This is crucial as majority of the land in a country are small cities or rural environment. In addition, privacy concerns are higher in these environments as it is harder to disappear in the masses. Large cities have limited benefit. However, Fig. 3(a) clearly shows that there are benefits nonetheless.

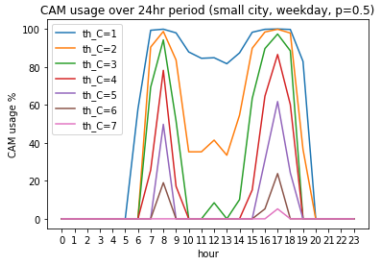
Our solution is also effectiveness in the early days of V2X technology deployment where the proportion of V2X-capable vehicle is low in the total vehicle population. Because proliferation of new technology takes long time, especially durable goods such as passenger cars last as long as 9 to 23 years [17], this is a significant point. In our simulation, we assumed that all vehicles are V2X capable. However, during this period, the effective number of vehicles reduces as the proportion of the V2X-capable vehicles in the total vehicle population is low. In this case, the effectiveness of our beacon scheme increases further by refraining from possibly volunteering privacy-related information to GPAs.



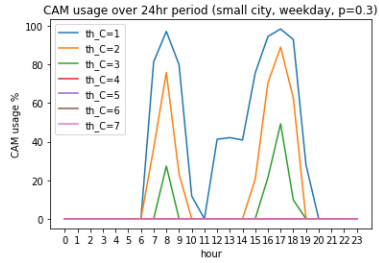
(a) $p = 0.9$



(b) $p = 0.7$

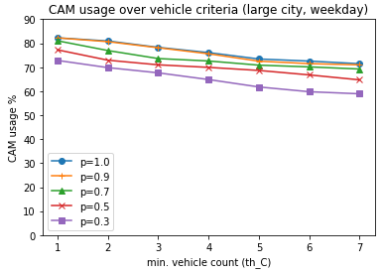


(c) $p = 0.5$

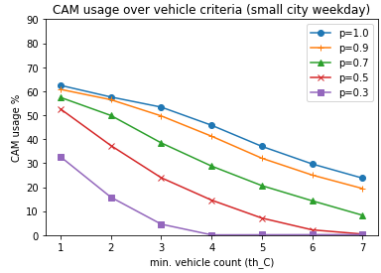


(d) $p = 0.3$

Figure 2: CAM Usage over 24hr Period (Small City, Weekdays)



(a) large city, weekdays



(b) small city, weekdays

Figure 3: CAM Usage over Varying Provisional CAM Probability (p)

5 Conclusions and Future Work

In this paper, we proposed a new beacon scheme for V2X communication. Through extensive simulations, we showed that our scheme reduces the exposure of vehicle information to potential adversaries when transmission of CAM is unnecessary. Our proposed scheme seamlessly adjusts to the traffic environment and use CAMs only when it is necessary and appropriate. Further it dynamically adjusts its behavior by taking into account geography (large city and small cities or rural areas), time (day and night, weekdays and weekend), as well as the V2X adoption rate over a longer time period. Beacon message processing is simpler than that of CAM as the former contains static information only. The potential latency of switching between the two can possibly influence the effectiveness of CAMs. However, our scheme presents a trade-off between privacy protection and benefits of CAM operation. The potential impact can be mitigated by carefully selecting optimal parameter values such as p (the probability to transmit CAMs) and th_C (CAM threshold). Studying the optimal values depending on the operational condition, such as traffic density and type of location, would be an interesting topic for future work.

Acknowledgments

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203 and by the Research Council KU Leuven C1 project on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058.

References

[1] 3GPP. TS 23.303 Technical Specification Group Services and System Aspects; Proximity-Based Services (ProSe); Stage 2, ver.16.0.0. Standard 3GPP TS 23.303:2020, 3rd Generation Partnership Project, 2020.

[2] Messaoud Babaghayou and Nabila Labraoui. Transmission Range Adjustment Influence on Location Privacy-Preserving Schemes in VANETs. In *2019 International Conference on Networking and Advanced Systems (ICNAS)*, pages 1–6. IEEE, 2019.

[3] Leila Benarous, Benamar Kadri, and Saadi Boudjit. Alloyed Pseudonym Change Strategy for Location Privacy in VANETs. In *2020 IEEE 17th*

Annual Consumer Communications & Networking Conference (CCNC), pages 1–6. IEEE, 2020.

[4] Alastair R Beresford and Frank Stajano. Mix Zones: User Privacy in Location-Aware Services. In *IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second*, pages 127–131. IEEE, 2004.

[5] Claudia Campolo, Antonella Molinaro, and Riccardo Scopigno. *Vehicular ad hoc Networks*. Springer International Publishing, Switzerland, 2015.

[6] Liqun Chen, Siaw-Lynn Ng, and Guilin Wang. Threshold Anonymous Announcement in VANETs. *IEEE Journal on Selected Areas in Communications*, 29(3):605–615, 2011.

[7] IEEE 802 LAN/MAN Standards Committee. IEEE Standard for Information Technology-Telecommunication and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment1: Radio Resource Measurement of Wireless LANs. Standard, Institute of Electrical and Electronics Engineers, 2016.

[8] Jeffery Ekweghi. Car Length and Width. `https://autovfix.com/average-length-of-a-car-how-long-is-the-average-car/`.

[9] ETSI. TS 102 894-2: Intelligent Transport Systems (ITS); Users and Applications Requirements; Part 2: Applications and Facilities Layer Common Data Dictionary; V1.3.1. Standard, European Telecommunications Standards Institute, 09 2018.

[10] ETSI. EN 302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, V1.4.1. Standard, European Telecommunications Standards Institute, 04 2019.

[11] Leping Huang, Kanta Matsuura, Hiroshi Yamane, and Kaoru Sezaki. Enhancing Wireless Location Privacy Using Silent Period. In *IEEE Wireless Communications and Networking Conference, 2005*, volume 2, pages 1187–1192. IEEE, 2005.

[12] Mohammad Khodaei and Panos Papadimitratos. Cooperative Location Privacy in Vehicular Networks: Why Simple Mix Zones Are Not Enough. *IEEE Internet of Things Journal*, 8(10):7985–8004, 2020.

[13] Stefan Larsson. Weight and Dimensions of Heavy Commercial Vehicles as Established by Directive 96/53/EC and the European Modular System (EMS). In *Workshop on LHVs, Bruxelles*, 2009.

[14] Qin Li, Amizah Malip, Keith M Martin, Siaw-Lynn Ng, and Jie Zhang. A Reputation-Based Announcement Scheme for VANETs. *IEEE Transactions on Vehicular Technology*, 61(9):4095–4108, 2012.

[15] Zhiquan Liu, Feiran Huang, Jian Weng, Kun Cao, Yinbin Miao, Jingjing Guo, and Yongdong Wu. BTMPP: Balancing Trust Management and Privacy Preservation for Emergency Message Dissemination in Vehicular Networks. *IEEE Internet of Things Journal*, 8(7):5386–5407, 2020.

[16] Lukas Malina, Arnau Vives-Guasch, Jordi Castellà-Roca, Alexandre Viejo, and Jan Hajny. Efficient Group Signatures for Privacy-Preserving Vehicular Networks. *Telecommunication Systems*, 58(4):293–311, 2015.

[17] Masahiro Oguchi and Masaaki Fuse. Regional and Longitudinal Estimation of Product Lifespan Distribution: A Case Study for Automobiles and A Simplified Estimation Method. *Environmental Science & Technology*, 49(3):1738–1743, 2015.

[18] SAE. J2735: Dedicated Short Range Communications (DSRC) Message Set Dictionary. Standard SAE J2735:2009, SAE International, 2009.

[19] Robert K Schmidt, Robert Lasowski, Tim Leinmüller, Claudia Linnhoff-Popien, and Günter Schäfer. An Approach for Selective Beacon Forwarding to Improve Cooperative Awareness. In *2010 IEEE Vehicular Networking Conference*, pages 182–188. IEEE, 2010.

[20] TomTom.com. Brussels Traffic. `https://www.tomtom.com/en_gb/traffic-index/brussels-traffic/`.

[21] Qianhong Wu, Josep Domingo-Ferrer, and Ursula González-Nicolás. Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications. *IEEE Transactions on Vehicular Technology*, 59(2):559–573, 2009.

Publication

On Handling of Certificate Digest in V2X Communication

Publication Data

Yoshizawa, T., and Preneel, B. On Handling of Certificate Digest in V2X Communication. In 2022 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, pp. 160–165, 2022.

Contributions

- Principal author.

On Handling of Certificate Digest in V2X Communication

Takahito Yoshizawa and Bart Preneel

KU Leuven, ESAT/COSIC, Leuven, Belgium

Abstract. We propose a change in the IEEE 1609.2 and ETSI ITS standards that define a certificate distribution mechanism, called *inline peer-to-peer certificate distribution (P2PCD)*. Messages exchanged in V2X messages are secured with digital signatures and digital certificates for the corresponding public keys. This *P2PCD* mechanism is used in Basic Safety Message (BSM) for the US and Cooperative Awareness Message (CAM) for Europe, and allows vehicles to proactively resolve unknown certificates. The unknown certificate situation occurs as not all messages contain the certificate in order to reduce overhead in these messages. This mechanism appears to be beneficial to minimize delay in verifying the authenticity and integrity of received messages. We evaluated its usefulness by conducting a simulation to recreate real-world highway traffic flow. The result indicates that, for high-way traffic, the benefit of this mechanism is negligble. At the same time, it increases unnecessary processing burden in vehicles. Based on our observation, we propose to update the IEEE 1609.2 and ETSI ITS standards in such a way that this mechanism should be restricted to traffic environments where it brings benefits.

1 Introduction

Vehicular communications and autonomous driving vehicles have been gaining increasing attention in recent years [18]. At the same time, both industry and academia raise concerns on cybersecurity aspects of so-called *connected vehicles*, or Vehicle-to-Everything (V2X) and challenges that lie ahead [6, 12]. To ensure coordinated implementations and deployments, standard bodies such as IEEE and ETSI have published specifications on vehicular communications. These standards include: (1) the IEEE 1609 series called Wireless Access in Vehicular Environments (WAVE), (2) IEEE 802.11p [14], (3) SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary [13], including the

Basic Safety Messages (BSM) definition, and (4) the ETSI ITS specifications. In recent years, a cellular-based V2X technology called Cellular-V2X (C-V2X) has emerged as an alternative solution to IEEE 802.11p-based DSRC [11].

To improve overall road safety, BSM [13] and Cooperative Awareness Message (CAM) [4] aim to achieve the same goal – to share vehicle information, such as a vehicle's speed, position, acceleration in order to establish and maintain awareness of others vehicles nearby to improve road safety. The expected range of V2X communication is 300 to 500 m [17].

From a security and privacy perspective, IEEE 1609.2 [15] specifies the solution to make vehicular communication secure and protect the vehicle owners' privacy. The security architecture and solution in the ETSI ITS standard [3] are based on the IEEE 1609.2 [15] specification with modifications to adapt to the European market. The key part of the security solution in IEEE 1609.2 [15] is the use of digital certificates to verify the authenticity of vehicles and the validity of messages they transmit. Messages from transmitting vehicles include a message payload, a digital signature, and a digital certificate. Receiving vehicles use the public key in this digital certificate to confirm the message authenticity and integrity by verifying the digital signature on the message. In this sense, the essential part of the security solution in V2X communication is a PKI system that generates, distributes, and uses digital certificates.

Because of the periodic nature of BSM [13] and CAM [4] messages, they allow the use of certificate *digest*, a short-hand notation of a full certificate, to occasionally replace a full certificate in these messages. ETSI TS 103 097 [5] states that vehicles include a *digest* in CAM messages by default, and a certificate at most once per second. While this mechanism reduces the message overhead, it also creates a situation where receiving vehicles may not locally have the certificate that corresponds to a *digest*, and are thus unable to verify the received message. To resolve this situation, the standard provides a mechanism to query vehicles within communication range to provide the certificate for a given *digest*. Despite the perceived benefit of this mechanism, our simulation result indicates that its benefit is negligible. This is due to a large majority of the resolution of unknown certificates is for vehicles that only interact very briefly.

The rest of this paper is organized as follows. In Sec. 2, we first describe the CAM transmission and reception as defined in the ETSI standard. Then in Sec. 3, we discuss our simulation to recreate traffic flow based on real-world data and analyze its result. In Sec. 4, we evaluate the simulation and reflect its result to the existing standard. We discuss related work in Sec. 5, and conclude the paper in Sec. 6.

2 CAM Transmission and Reception

ETSI EN 302 637-2 [4] specifies CAM transmission and reception. In particular, it describes the criteria for vehicles to transmit CAM messages. Since the last CAM transmission, either[1]:

1. the direction change exceeds 4 degrees;
2. the distance change exceeds 4 meters; or
3. the speed change exceeds 0.5 meter/sec.

In addition, the minimum ($T_GenCamMin$) and maximum transmission intervals ($T_GenCamMax$) are 100 msec and 1 sec, respectively. In other words, vehicles transmit CAM messages at specific movement changes with the frequency of between 1 to 10 times per second. If the CAM transmission rate is higher than 1 message/sec, the vehicle includes a certificate in only one message per second.

As stated in Sec. 1, the use of a certificate *digest* reduces the CAM message overhead. A study by C2C-CC indicates that the average CAM message size is 350 bytes while the size of certificates and signatures is between 100 bytes and 150 bytes [2]. This implies that the certificate and signature take up to 30% of the total message size. IEEE 1609.2 [15] defines this *digest* as `HashedId8` type which contains the least significant eight octets of the hash output of the certificate, ($d = LSB8(Hash(c))$, where d, $LSB8()$, $Hash()$, and c are a digest, a function to extract the least-significant eight octets of the argument, a cryptographic hash function, and a certificate, respectively). Thus, the use of *digest* reduces the certificate size from between 100 to 150 bytes to 8 bytes. This compact representation significantly reduces the total CAM message size. Because the CAM transmission is periodic and frequent, this reduction contributes to an efficient use of the radio channel.

On the other hand, the use of *digest* implies that receiving vehicles need to hold a mapping table that maps a *digest* to the corresponding certificate. This further implies that a situation can occur where a receiving vehicle does not have the certificate that maps to a *digest* received in a CAM message (*unknown certificate* situation). This situation occurs when a vehicle enters the communication range of another vehicle that just transmitted a CAM message with a *digest*. This is a problem as the receiving vehicle cannot verify the received CAM message

[1] In addition to these, the 802.11p-based system requires an additional timer (T_GenCam_Dcc) defining the minimum interval between two consecutive CAM messages to prevent channel congestion.

due to the absence of a certificate. There are two approaches to resolve this situation. The first is to simply wait for the next CAM message containing the missing certificate. The second is to proactively request the missing certificate to be sent.

The IEEE 1609.2 [15] and EN 302 637-2 [4] specifications provide a mechanism to realize the latter approach. It is called *inlineP2pcdRequest* which was added to the IEEE 1609.2 amendment 1 [16]. In this mechanism, a receiving vehicle requests the missing certificate to be sent so that either the transmitting vehicle itself or any other vehicle within the communication range can respond by sending this certificate. This request uses a field in the CAM message header; the requesting vehicle populates one or more *unresolved digest(s)* in this header field to indicate that it requests the corresponding certificate(s) to be sent. Receiving vehicles of a CAM message containing an *inlineP2pcdRequest* in its header checks its local memory, and if it has the corresponding certificate, it sends a response message. IEEE 1609.2 defines a throttle mechanism to avoid an excessive number of responses by vehicles.

Minimizing delay in verifying received messages is an important factor in real-time cyber-physical systems such as V2X communication to avoid accidents and improve road safety. However, the *inlineP2pcdRequest* mechanism also increases the CAM message length and processing at both sending and receiving vehicles. An excessive processing burden in vehicles and communication channel congestion can also cause a delay in message verification. Furthermore, if the next CAM message containing a certificate arrives while *inlineP2pcdRequest* is in progress, this request becomes a futile effort. Given the $T_GenCamMax$ value of 1 second, the next CAM message with a certificate is expected within 500 msec on average. Therefore, the time gap reduction for using this mechanism is an order of several 100 msec. A legitimate question is whether this is worth the effort. This paper investigates the benefit and effectiveness of this mechanism compared to the first *"do nothing"* approach in which the vehicle waits for the next CAM message containing the missing certificate.

3 Simulation to Reproduce Real-World Traffic Flow

To better understand the effectiveness of the *inlineP2pcdRequest* mechanism, we conducted a simulation to reproduce traffic flow based on real-world traffic data.

3.1 Traffic Data

We used the real-world traffic data from a government project conducted in 2019. This data contain vehicle flow in multi-lane highway segments and junctions that surround Antwerp, Belgium. The longest segment of collected data is approximately 9 km. The raw traffic data were recorded by inductive loops embedded in the road surface. The collected raw data include speed and size (length) of each passing vehicle over 24 hours a day for all lanes for one month. This log data provides insight into dynamic changes of traffic density over this entire collection period.

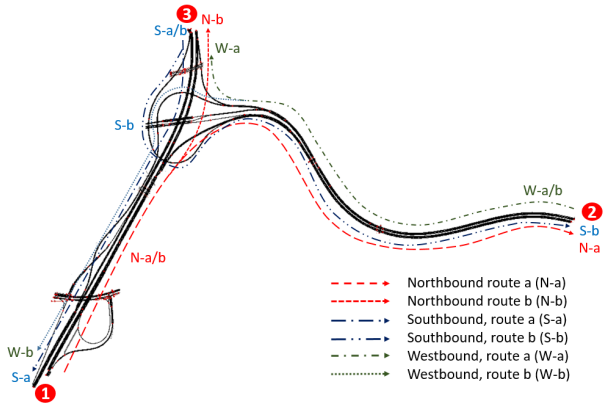


Figure 1: Route of the Simulated Traffic

Table 1: Vehicle Routes

Direction	Route	Label	From (position)	To (position)
Northbound	a	N-a	South entrance ①	East exit ②
Northbound	b	N-b	South entrance ①	North exit ③
Southbound	a	S-a	North entrance ③	South exit ①
Southbound	b	S-b	North entrance ③	East exit ②
Westbound	a	W-a	East entrance ②	North exit ③
Westbound	b	W-b	East entrance ②	South exit ①

The highway segment we consider is shown in Fig. 1 and in Table 1; it consists of three directions (northbound, southbound, westbound) with each direction divided into two routes (a and b), for a total of 6 trajectories. We selected the busiest traffic day from the one-month period, and chose three one-hour

time slots (high, medium, and low traffic density) from this day. Then we recreated the traffic flow of these three time slots using the SUMO traffic simulator [10].[2] We configured the SUMO simulator using the vehicle types and physical characteristics according to the definition from this national project: (1) passenger vehicle, (2) van, (3) lorrie, and (4) trailer and bus. We prepared 3 configuration files and ran the simulation 3 times to recreate high, medium, and low-density traffic according to the traffic density for each vehicle types as shown in Table 2.

3.2 Approach and Methodology

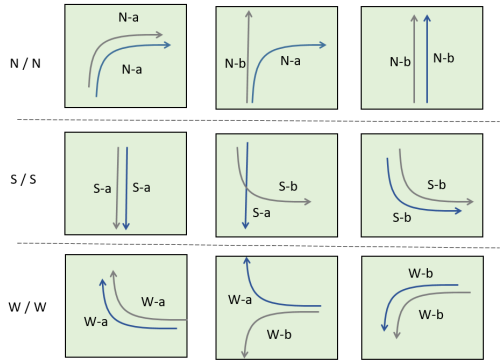
We used the *vTypeProbe* output mode in SUMO to analyze the traffic flow. Output from this mode includes the latitude/longitude of each vehicle in 1 second increments. We used this data to calculate the distance between a given pair of vehicles. For each vehicle as a reference point, we calculated the distance change in every second to all other vehicles on the highway. With this distance data, we analyzed the traffic flow from the perspective of the reference vehicle entering and leaving the communication range of other vehicles. Then we repeated this process for all vehicles as the reference point. This way, we obtained a complete distance change history from all vehicles to all other vehicles during the course of their travel.

Next, we grouped the combinations of two trajectories and categorized them based on the perceived importance to resolve the *unknown certificate* condition. Figure 2 shows all possible combinations; among all 21 combinations, 9 of them fall into what we call *low-impact* category. These are shown in pink with a dotted-line boundary. This category is characterized by vehicles moving in opposite directions; they approach and move away from each other with minimal time spent in each other's communication range. The higher each other's relative speed difference, such as in a highway scenario in our traffic data, the shorter this duration becomes. Once they leave the communication range, they are unlikely to meet again for the remainder of their trips. For example, two vehicles in opposite directions on a highway moving at 100 km/h spend only 5.4 to 9 seconds within each other's communication range of 300 to 500 meters. Using the *inlineP2pcdRequest* mechanism for such a short encounter does not appear to justify imposing additional processing in all vehicles within this communication range to resolve unknown certificates in broadcast CAM messages, given that the time saved is in the order of several 100 msec at best. The number of these requests increases proportionally to the traffic density, thus exacerbating the situation. Therefore we conclude the *inlineP2pcdRequest*

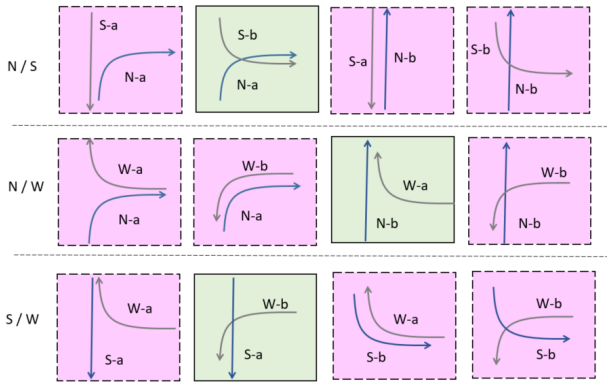
[2]Due to imported map data size limitation, the maximum highway segment in the SUMO simulation is limited to approx. 6km from the original data of approx. 9km segment.

Table 2: Traffic Density (vehicles/hour)

Vehicle Type	**Direction**	**Route**	**Traffic Density (High / Medium / Low)**
Passenger	North	a	2887 / 2153 / 111
Passenger	North	b	2890 / 2157 / 112
Van	North	a	588 / 572 / 47
Van	North	b	591 / 575 / 49
Lorrie	North	a	95 / 171 / 30
Lorrie	North	b	98 / 173 / 32
Trailer, Bus	North	a	313 / 590 / 132
Trailer, Bus	North	b	314 / 591 / 133
Passenger	South	a	3110 / 2574 / 217
Passenger	South	b	1374 / 750 / 55
Van	South	a	1720 / 1612 / 69
Van	South	b	152 / 100 / 9
Lorrie	South	a	145 / 324 / 31
Lorrie	South	b	48 / 78 / 4
Trailer, Bus	South	a	278 / 598 / 108
Trailer, Bus	South	b	167 / 335 / 25
Passenger	West	a	2056 / 889 / 60
Passenger	West	b	2059 / 891 / 62
Van	West	a	196 / 153 / 17
Van	West	b	200 / 154 / 17
Lorrie	West	a	66 / 98 / 19
Lorrie	West	b	68 / 101 / 21
Trailer, Bus	West	a	164 / 399 / 69
Trailer, Bus	West	b	166 / 401 / 71



(a) Combination Group 1



(b) Combination Group 2

Figure 2: Traffic Combinations

mechanism in the *low-impact* category has the least benefit in highway scenarios. On the other hand, the remaining 12 combinations in Fig. 2 fall into the *high-impact* category, shown in green with a solid line boundary. All combinations in this category share the common characteristic that the inter-vehicle distance remains relatively stable for an extended period as they move in the same direction in whole or at least in part of their trajectories. Therefore, in this category, this mechanism is more beneficial.

Table 3 shows the resulting handling of the received CAM messages between two vehicles. Here "CR" (certificate request) indicates the receiving vehicle uses the *inlineP2pcdRequest* mechanism to resolve unknown certificates, while "ignore" means that the vehicle waits for the next CAM message with a certificate.

Table 3: Unknown Certificate Handling Matrix

Direction-Route		Vehicle A					
		N-a	N-b	S-a	S-b	W-a	W-b
Vehicle B	N-a	CR	CR	ignore	CR	ignore	ignore
	N-b	–	CR	ignore	ignore	CR	ignore
	S-a	–	–	CR	CR	ignore	CR
	S-b	–	–	–	CR	ignore	ignore
	W-a	–	–	–	–	CR	CR
	W-b	–	–	–	–	–	CR

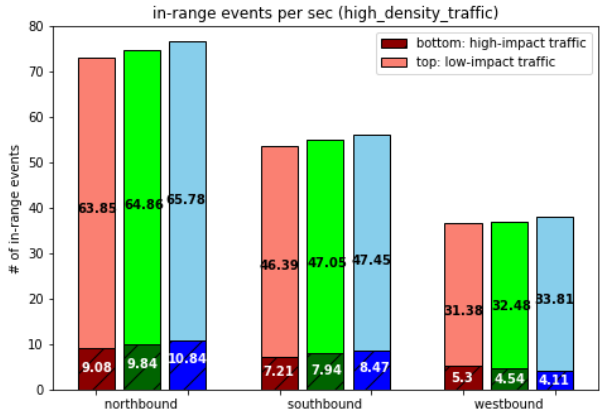
Note: CR: certificate request.

From the SUMO *vTypeProbe* output, we identified all events where a vehicle enters the communication range of another vehicle (we call it *in-range event* for the rest of this paper), applied the *high-* and *low-impact* categorization based on their trajectories, and counted the number of events in both categories. We analyzed the data using three communication range of 300 m, 400 m, and 500 m for all vehicle types and evaluated their effect. We selected these distances as they are the expected transmission range in both DSRC (ITS-G5) and C-V2X [17]. There are multiple criteria to trigger CAM messages as described in Sect. 2. However, given that our data represents highway traffic, we use the vehicle speed to derive the transmission interval of vehicles to simplify our analysis.

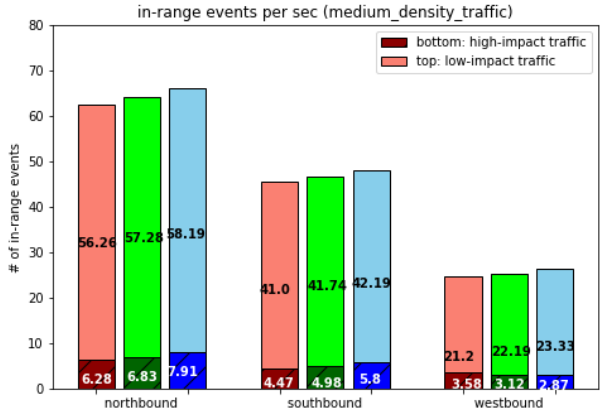
4 Discussion and Evaluation

Our analysis result is shown in Table 4 and Fig. 3. Table 4 shows the average duration a vehicle stays within the transmission range of another vehicle according to the traffic combination in Fig. 2. This duration is consistently longer for vehicles in the *high-impact* category and significantly shorter in the *low-impact* category. As discussed in Sec. 3.2, this is intuitive as vehicles in opposite trajectories spend less time in each other's communication range than that of similar trajectories. Vehicles in the former category stay in their communication range between 2.3 to 6.6 times longer than the latter depending on this range.

Figure 3(a) and 3(b) show the analysis of *in-range event* for high and medium



(a) high-density traffic



(b) medium-density traffic

Figure 3: In-Range Event per Second (The red, green, and blue bars represent the number of events per second in 300m, 400m, and 500m communication range, respectively. For each bar, the darker color at the bottom and the lighter color at the top show the *high-impact* and *low-impact* category.)

Table 4: In-Range Duration (sec.)

Traffic direction		Northbound		Southbound		Westbound	
Traffic Combination		High-Imp	Low-Imp	High-Imp	Low-Imp	High-Imp	Low-Imp
Comm. Range: 300m	High-D	72.19	15.15	57.39	17.53	88.09	13.69
	Med-D	72.77	14.87	57.51	16.12	89.15	13.51
	Low-D	61.50	12.94	46.00	13.66	73.17	12.37
Comm. Range: 400m	High-D	79.20	19.78	60.33	22.72	99.30	18.13
	Med-D	79.29	19.44	60.17	21.17	101.05	17.82
	Low-D	68.37	16.57	50.52	18.00	84.75	16.81
Comm. Range: 500m	High-D	83.89	24.46	62.58	26.97	107.23	23.44
	Med-D	83.61	24.07	61.77	25.68	107.56	23.09
	Low-D	73.26	20.14	53.12	21.80	90.91	21.21

Note: High-D: high-density, Med-D: medium-density,
Low-D: low-density, High-Imp: high-impact, Low-Imp: low-impact.

density traffic, respectively[3]. In Fig. 3(a) and 3(b), *in-range events* are grouped based on traffic direction (north, south, westbound). In all cases, the number of *in-range events* for the *low-impact* category are significantly higher than that of the *high-impact* category. On average, high-density traffic indicates that 85.6% to 89.2% of all *in-range events* occur between vehicles in the *low-impact* category. In medium-density traffic, this value is slightly higher between 85.5% to 90.0%. This trend is consistent across all communication distance of 300m, 400m, and 500m. In other words, a large majority of *in-range events* occur with vehicles in the *low-impact* category, and the events with vehicles in the *high-impact* category are a minority. Again, this result reflects our intuition – the *in-range event* occurs more frequently with relatively high speed difference between two vehicles, such as vehicles in opposing directions. On the other hand, vehicles moving in the same or similar trajectory have lower relative speed difference. Thus, threshold-cross events occur less often.

If we suppress the *inlineP2pcdRequest* mechanism in all *low-impact* category vehicles, it reduces a large proportion of such events. There are a number of benefits of doing so: it (1) reduces the processing and transmission of *inlineP2pcdRequest* in the CAM header from the requesting vehicle, (2) relieves the processing of these requests in all other vehicles within the communication range, and (3) reduces the use of communication channel.

Table 5 summarizes the resulting improvement due to suppressing the

[3]Low density traffic result is not shown as its numbers are significantly lower compared to these two scenarios, thus do not contribute additional value to the discussion.

inlineP2pcdRequest for *low-impact* category. Our simulation result indicates that the minimum and the maximum number of CAM messages/sec is 4.28 to 6.21 in high- and medium-density traffic.[4] As we described in Sec. 2, the CAM messages periodically include a full certificate at every 1 second interval. This implies that the probability of an *unknown certificate* situation is 76.6% to 83.9% of all *in-range events*. If we include the *inlineP2pcdRequest* in the CAM message header for all such events, as specified in IEEE 1609.2 [15], there are 58.69 and 55.46 requests per second for high- and medium-density traffic. If we suppress all these requests for *in-range events* in the *low-impact* category, then based on the number in Fig. 3(a) and 3(b), the average number of CAM messages containing the *inlineP2pcdRequest* reduces to 8.30 and 6.64 requests/sec, respectively. This is a 7.1 to 8.4 times improvement over the default behavior of generating *inlineP2pcdRequest* without considering the traffic trajectory.

Table 5: Reduced Overhead Due to InlineP2pcdRequest Message Supression

Data Points	Traffic density	
	High	Medium
# of CAM messages/sec	4.28	6.21
in-range events/sec	76.62	66.10
% of "unknown cert." condition	76.6%	83.9%
inlineP2pcdRequest events/sec (default)	58.69	55.46
high-impact %	14.14%	11.97%
inlineP2pcdRequest events (improved)	8.30	6.64

We acknowledge that our scheme relies on unverified CAM messages due to the absence of a certificate in received messages. In this sense, we assume an *honest majority*, i.e. a large proportion of the vehicles are honest and send genuine information in their CAM messages. Such an assumption may be a concern. However, it has only a negligible implication. If we ignore all *unknown certificate* situations irrespective of vehicle trajectories, we fall back to the *"do nothing"* approach and simply wait for the next CAM message with a certificate attached. If no such message is received from a given vehicle, it means that this vehicle has likely moved out of the communication range already. Thus we can safely disregard this vehicle. We also note that this simulation result and evaluation are limited to the highway traffic environment. Thus, we may obtain a different view in other environments such as busy local streets. However, our analysis indicates that using the *inlineP2pcdRequest* mechanism

[4]The CAM messages/sec is lower in high density traffic due to relatively lower speed than medium density traffic.

has almost no benefit in the highway environment while it only incurs additional processing in vehicles. Therefore, we conclude that vehicles should apply the *inlineP2pcdRequest* mechanism based on its attributes, such as speed, relative to that of encountered vehicles. This way, vehicles can use this mechanism where it is truly beneficial.

5 Related Work

Several works of literature discuss the impact of security-related processing in V2X communication and mention digest use in CAM messages. Javed et al. [7] and Brahim et al. [1] investigated the impact of processing ECC-based signature and encryption algorithm and evaluated their performance. Muhammad et al. [11] measured and analyzed the security overhead in broadcast communication in LTE C-V2X from the integrity and authenticity protection processing perspective. From a V2X-based service perspective, Lonc and Cincilla [9] summarize the implementation status of security services as defined in the ETSI ITS standard, and Labiod et al. [8] propose a service advertisement message called CAM-I.

All these studies mention certificate *digest* in CAM messages as background information within the context of their discussion. From a performance perspective, the common conclusion is that the overhead in security processing in C-ITS results in additional delay [7, 1, 11]. As such, they only mention the certificate *digest* as a feature in the ETSI ITS standard to reduce message size; no consideration is given to its usefulness in traffic patterns as we focus in this paper. To the best of our knowledge, the usefulness and the issue related to resolving unknown certificates in CAM messages using the *inlineP2pcdRequest* mechanism has not been studied.

6 Conclusion and Future Work

We presented the simulation result and analysis of using the *inlineP2pcdRequest* mechanism in highway scenario based on real-world traffic data. Based on our findings, we conclude that this mechanism has more disadvantages than advantages; it only increases processing loads in vehicles and the higher utilization of communication channel while its benefits remain unclear. Therefore, we propose ETSI and IEEE reevaluate this mechanism in their standards and modify its specification. Furthermore, conducting field test and measuring the message processing overhead of this mechanism on a hardware

platform will further reinforce our understanding of the performance implications. Also, additional simulation and analysis using other types of traffic scenarios would complement our findings further to understand this mechanism's benefits. We consider these areas our next step.

Acknowledgments

We express our gratitude to Be-Mobile NV, Prof. Chris Tampére and Dr. Mohammad Ali Arman of the Mechanical Engineering Dept. in KU Leuven for providing the traffic data. We also thank Dr. Dave Singelée in COSIC group in KU Leuven, Dr. Xavier Carpent and Ms. Dimah Mohammed Almani in Computer Science Dept. in Univ. of Nottingham for their insights. This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203 and by the Research Council KU Leuven C1 project on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058.

References

[1] Mohamed Ben Brahim, Elyes Ben Hamida, Fethi Filali, and Noureddine Hamdi. Performance Impact of Security on Cooperative Awareness in Dense Urban Vehicular Networks. In *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 268–274. IEEE, 2015.

[2] C2C-CC. TR2052, Survey on ITS-G5 CAM Statistics. Technical report, Car 2 Car Communication Consortium, 12 2018.

[3] ETSI. TS 102 940: Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management; V2.1.1. Standard, European Telecommunications Standards Institute, 07 2018.

[4] ETSI. EN 302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, V1.4.1. Standard, European Telecommunications Standards Institute, 04 2019.

[5] ETSI. TS 103 097: Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats; Release 2; V2.1.1. Standard, European Telecommunications Standards Institute, 10 2021.

[6] Numaan Huq, Craig Gibson, and Rainer Vosseler. Driving Security into Connected Cars: Threat Model and Recommendations. Whitepaper, Trend Micro Research, 2020.

[7] Muhammad Awais Javed, Elyes Ben Hamida, and Wassim Znaidi. Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice. *Sensors*, 16(6):879, 2016.

[8] Houda Labiod, Alain Servel, Gerard Seggara, Badis Hammi, and Jean Philippe Monteuuis. A New Service Advertisement Message for ETSI ITS Environments: CAM-Infrastructure. In *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–4. IEEE, 2016.

[9] Brigitte Lonc and Pierpaolo Cincilla. Cooperative ITS Security Framework: Standards and Implementations Progress in Europe. In *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 1–6. IEEE, 2016.

[10] Pablo Alvarez Lopez, Michael Behrisch, Laura Bieker-Walz, Jakob Erdmann, Yun-Pang Flötteröd, Robert Hilbrich, Leonhard Lücken, Johannes Rummel, Peter Wagner, and Evamarie Wießner. Microscopic Traffic Simulation Using SUMO. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pages 2575–2582. IEEE, 2018.

[11] Mujahid Muhammad, Paul Kearney, Adel Aneiba, and Andreas Kunz. Analysis of Security Overhead in Broadcast V2V Communications. In *International Conference on Computer Safety, Reliability, and Security*, pages 251–263. Springer, 2019.

[12] Maximilian Renner, Niels Münzenberger, Johanna von Hammerstein, Sebastian Lins, and Ali Sunyaev. Challenges of Vehicle-to-Everything Communication. Interviews among Industry Experts. In *Wirtschaftsinformatik (Zentrale Tracks)*, pages 1831–1843, 2020.

[13] SAE. J2735, Surface Vehicle Standard, V2X Communications Message Set Dictionary. Standard SAE J2735:2006, SAE International, 2006.

[14] IEEE Computer Society. IEEE Std. 802.11p-2010, Standard for Information Technology - Telecommunication and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. Technical specification, IEEE, 2010.

[15] IEEE Vehicular Technology Society. Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Services. Technical specification, Institute of Electrical and Electronics Engineers, Piscataway, NJ, United States, 03 2016.

[16] IEEE Vehicular Technology Society. IEEE 1609.2a-2017, Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages Amendment 1. Technical specification, IEEE, 2017.

[17] Branka Stojanović and Katharina Hofer-Schmitz. Formal Methods for Connected Vehicle Protocols. In *2019 27th Telecommunications Forum (TELFOR)*, pages 1–4. IEEE, 2019.

[18] DianGe Yang, Kun Jiang, Ding Zhao, ChunLei Yu, Zhong Cao, ShiChao Xie, ZhongYang Xiao, XinYu Jiao, SiJia Wang, and Kai Zhang. Intelligent and Connected Vehicles: Current Status and Future Perspectives. *Science China Technological Sciences*, 61(10):1446–1471, 2018.

Publication

Misbehaviour Reporting in ETSI ITS Standard Considered Broken

Publication Data

Yoshizawa, T., and Preneel, B. Misbehaviour Reporting in ETSI ITS Standard Considered Broken. In 2022 IEEE Conference on Standards for Communications and Networking (CSCN), IEEE, pp. 144–150, 2022.

Contributions

- Principal author.

Misbehaviour Reporting in ETSI ITS Standard Considered Broken

Takahito Yoshizawa and Bart Preneel

KU Leuven, ESAT/COSIC, Leuven, Belgium

Abstract. This paper identifies gaps in the Cooperative ITS Credential Management System (CCMS) in the European Telecommunication Standard Institute (ETSI) Intelligent Transport System (ITS) standard and proposes a solution to address them. Under the current specification, misbehaviour reporting is ineffective, especially in cross-border scenarios involving vehicles from different countries. This is the primary concern in Europe as these scenarios occur daily. Leaving these gaps open will result in practical issues when ITS systems are widely deployed across EU countries. Our solution effectively resolves these gaps while keeping the impact on the CCMS architecture at minimum. We propose that our solution is adopted in the ETSI ITS specifications.

1 Introduction

The development and deployment of vehicular communication, or vehicle-to-everything (V2X), has been gaining momentum in recent years. In Europe, it is evident in the continued effort in the past years by EU-funded projects that demonstrate the readiness of this technology [4]. The underpinning solution is specified by ETSI in Europe and IEEE in the US. In addition, regulatory work by the European Commission (EC) [5] shapes the deployment of this technology to the practical use in EU countries.

ETSI and the EC have defined the ITS specifications and regulations for vehicular communication for the European market. They ensure uniform implementations and deployments across the EU member states. From both security and privacy perspectives, V2X technology, as a type of cyber-physical system, has potential safety impact including physical damage, injuries, and death. For this reason, addressing security is vital. In addition, regulations on personal data protection, such as the General Data Protection Regulation (GDPR), also play an important role in preventing vehicular communications from disclosing vehicle owners'

personal information. Therefore, security and privacy protection are essential in V2X communication.

One crucial security aspect in V2X communication is to detect and evict misbehaving vehicles. Prompt action by the CCMS is required to prevent them from negatively influencing other vehicles with false information or causing undesirable consequences such as accidents. However, our analysis of the ETSI ITS specifications indicates that the misbehaviour reporting is ineffective. Moreover, the Misbehaviour Authority (MA), the entity responsible for analyzing Misbehaviour Reports (MRs), cannot even identify the allegedly misbehaving vehicle, let alone investigate and evict it. Furthermore, the ETSI ITS standard does not address cross-border scenarios in MR reporting. In Europe, a large number of vehicles crosses borders on a daily basis, as shared borders connect the countries, and several treaties allow for free movement of people and goods including vehicles. For this reason, MR reporting and subsequent actions by the MA to investigate and revoke vehicle's certificates, or Authorization Tickets (ATs), need to occur seamlessly irrespective of the vehicles' origins.

This paper proposes a solution that addresses and resolves these gaps in the ETSI ITS standard. In this context, the intended audience of this paper includes delegates who are involved with ETSI ITS standardization work and researchers who are interested in the standardization aspects of V2X communication.

This paper is organized as follows. In Sec. 2 and Sec. 3, we first discuss related work and the background and relevant standards. Then, we describe the cross-border scenarios in Sec. 4, followed by identifying the gap and its root cause in the ETSI ITS standard in Sec 5. In Sec. 6 and Sec. 7, we shift our focus to our solution and evaluate it against the existing solution in IEEE 1609 standard. conclude our discussion in Sec. 9.

2 Related Work

ETSI TR 103 460 [11] consolidates various approaches and techniques for misbehaviour detection from the research community. It discusses 34 research articles and groups them based on different detection approaches. As such, it does not raise or discuss the architectural gaps we have identified in Sec. 5. Van der Heijden et al. [30] present a comprehensive overview of many misbehaviour detection techniques and solutions by analyzing and categorizing them.

From cross-border perspective, Kousaridas et al. [19] and Trichias et al. [28] describe the related standard and maturity level of technology, regulatory, and business case aspects of 5G V2X services in cross-border scenarios. Raya et

al. [24] suggest different CAs in different countries and regions to be cross-certified so that vehicles from different countries or regions can authenticate each other.

Kousaridas et al. [20] describe cross-border scenarios in the 5GCroCo [6], 5G-CARMEN [3], and 5G-Mobix [1] projects. Their focus is on the technical challenges including handover, service continuity and QoS impacts when vehicles cross a border and change the mobile networks from one country to another. Muñoz et al. [22] specifically focus on the collision avoidance use case in the 5GCroCo project and describe their system setup. Hetzer et al. [15] also discuss 5GCroCo project use cases. Their focus is on mobile technologies in the 5G system context. Fallgran et al. [14] discuss 5G technology enablers. They consider both technology components and their challenges. These challenges include conflicting aspects in a vehicular environment, e.g. mobility and reliability, connectivity to different mobile networks, requirements on connection resilience, and security and data privacy. Peters et al. [23] describe their simulated platform to address cross-border scenarios in the 5G-MOBIX project.

Mendiboure et al. [21] propose a Blockchain (BC)-based authentication and access control solution for vehicular network. This also includes cross-border scenarios by cross-subnetworks to coordinate with each other for vehicle authentication and access control. Van der Heijden et al. [29] propose a BC-based vehicle revocation that offers an accountable mechanism while avoiding the issue of centralized trust in the CRL. This paper specifically discusses cross-border revocation and suggests a need of defining a protocol to achieve it. However, it does not cover the issues and gaps in the standard we have identified and addressed.

3 Background

The first standards for vehicular communication have been specified by the IEEE, namely, IEEE 802.11p [26] and the 1609 series [16]. They are called Wireless Access in Vehicular Environments (WAVE). The upper layer, defined by SAE J2735 [25], is called Dedicated Short Range Communications (DSRC) Basic Set Messages (BSM). IEEE 1609.2 [27] and 1609.2.1 [17] specify the certificate management at the system level and at the end entity level, e.g. vehicles, respectively. ETSI ITS also defined an equivalent standard for Europe based on these IEEE standards, as well as upper layer messages equivalent to the DSRC BSM. They include Cooperative Awareness Messages (CAM) [9] and De-centralized Environmental Notification Messages (DENM) [10].

The main pillar of the security mechanism in V2X communication is its capability to verify the message authenticity and authorization of vehicles. For this purpose, the CCMS issues digital certificates to authorized vehicles that use them to sign messages they transmit. This allows receiving vehicles to verify the authenticity and validity of the received messages. For this reason, the CCMS is concerned with a Public Key Infrastructure (PKI) system. In particular, mandatory use of pseudonyms and pseudonym certificates, or Authorization Tickets (AT), along with a periodic change of these, protects vehicle owners' privacy and prevents identifying and tracking vehicles and their owners. The CCMS architecture is specified in TS 102 940 [8] and its detailed procedures and messages for enrolment, authorization, and issuing ATs, are defined in TS 102 941 [12]. The certificate format, specifically designed for V2X communication, is specified in TS 103 097 [13]. A large part of the ETSI ITS's CCMS architecture and its details follow the IEEE 1609.2 [27] and 1609.2.1 [17] specifications, which, in turn, adopted the design from the Security Credential Management System (SCMS) by Brecht et al. [2].

4 Misbehaviour Scenario Descriptions

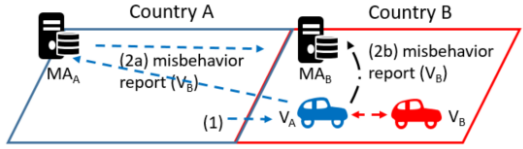
There are several relevant use case scenarios of MR reporting. Before we proceed further, we first define the term *border* in the CCMS context; *cross-border* refers to the situation where a vehicle crosses the boundary of one CCMS to another, either at the country-level or at any smaller division within a country if multiple CCMS systems exist in a country. To simplify our discussion, we use the *country border* to identify the issues. Figure 1 describes two cross-border scenarios. The symbols are shown in Table 1.

Table 1: Symbol Definitions

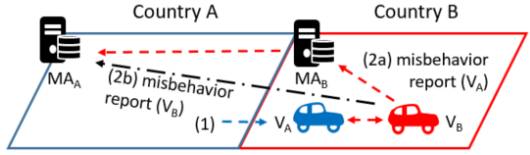
Symbol	Definition
V_A	A vehicle registered in country A
V_B	A vehicle registered in country B
MA_A	Misbehaviour Authority (MA) in country A
MA_B	Misbehaviour Authority (MA) in country B

4.1 Scenario 1

In the first scenario (Fig. 1(a)), a vehicle from country A (V_A) crosses a border to a neighboring country B (step 1). Subsequently, V_A detects a misbehaviour



(a) MR Reporting Scenario 1



(b) MR Reporting Scenario 2

Figure 1: Use Case Scenarios

of a local vehicle V_B in country B, and reports this event to the MA in country A (MA_A). In turn, MA_A forwards this report to MA_B to whom V_B belongs in order to enable MA_B to investigate the reported misbehaviour of V_B (step 2a). Alternatively, V_A sends the MR directly to MA_B (step 2b).

4.2 Scenario 2

This scenario (Fig. 1(b)) is similar to scenario 1 except that the vehicles' roles are swapped. It also starts with V_A crossing a border to a neighboring country B (step 1). Subsequently, a local vehicle (V_B) detects a misbehaviour of V_A, and reports it to MA_B in country B. In turn, MA_B forwards this report to MA_A to whom V_A belongs in order to enable MA_A to investigate the reported misbehaviour of V_A (step 2a). Alternatively, V_B sends the MR directly to MA_A (step 2b).

5 Issues of Misbehaviour Reporting in The ETSI ITS Standard

In the two scenarios in Sec. 4, the expected behavior of the MA is to either: (1) accept the report and conduct the misbehaviour investigation against the reported vehicle, or (2) forward the report to the MA in the system to which the reported vehicle belongs to enable this MA to trigger a misbehaviour

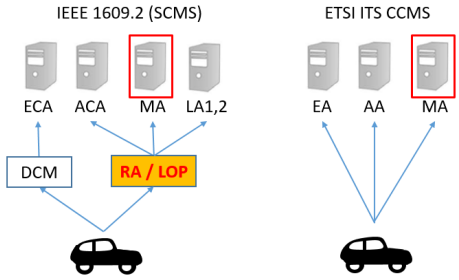


Figure 2: Architectural Difference between IEEE 1609.2 and ETSI ITS 102 940

investigation. However, according to the ETSI ITS specifications, this does not occur in either scenarios. There are four gaps in the standard that lead to this situation.

5.1 Absence of MA ID in Vehicles

The first gap is the architectural change and its implications. As stated in Sec. 3, the IEEE 1609 series standard was specified for the US. IEEE 1609.2 [27] specifies security aspects, specifically the certificate management. Subsequently, the ETSI ITS standard [8] adopted its solution.

While adopting the IEEE 1609.2 standard, ETSI ITS modified its system architecture. This modification can be characterized as a simplification, as shown in Figure 2, by reducing the number of entities and interactions among them. The left- and right-hand side show the entity hierarchy between a vehicle and the management system entities according to IEEE 1609.2 and ETSI ITS CCMS, respectively. The entity names are listed in Table 2.

In the IEEE 1609.2 architecture [27], vehicles communicate with system entities through either the Device Configuration Manager (DCM), or the Registration Authority (RA) and the Location Obscurer Proxy (LOP). Therefore, the communication between vehicles and system entities such as Enrollment Certificate Authority (ECA), Authorization Certificate Authority (ACA), and Misbehaviour Authority (MA), are *indirect* through the DCM or the RA and the LOP. In the case of misbehaviour, a vehicle sends a report to the RA via the LOP. Upon receiving a report, the RA selects an appropriate MA in the system and forwards it. This way, vehicles do not necessarily know the identity and contact information of the ECA, the ACA, and the MA as this information is managed within the DCM and the RA.

Table 2: Terminologies of Equivalent System Entities

IEEE 1609.2 [27] Entities	ETSI ITS CCMS [8] Entities
Authorization Cert. Authority (ACA)	Authorization Authority (AA)
Enrollment Cert. Authority (ECA)	Enrolment Authority (EA)
Misbehaviour Authority (MA)	Misbehaviour Authority (MA)
Linkage Authority (LA)	(does not exist)
Device Configuration Manager (DCM)	(does not exist)
Registration Authority (RA)	(does not exist)
Location Obscurer Proxy (LOP)	(does not exist)

On the other hand, due to the simplification in ETSI ITS CCMS, vehicles *directly* communicate with system entities such as Enrolment Authority (EA), Authorization Authority (AA), and MA. This change implies that vehicles need to know the contact information of these system entities. TS 102 941 Sec. 6.1.2 [12] specifies that the vehicle manufacturer configures the contact information of the EA and the AA in a vehicle prior to the enrolment process.[1] On the other hand, it does not specify how and at what timing the contact information for the MA is configured in the vehicle. Therefore, vehicles may not be able to send any MR at all. We consider this an omission in this specification [12] and assume that it is configured in a vehicle at the same time when the EA and the AA information are configured.

5.2 No Unique Information in the AT

The second gap is the AT definition. Specifically, the certificate definition in TS 103 097 [13] does not specify how an AT can be traced back to a unique vehicle or identify the CCMS that has issued the AT to the vehicle. Therefore, even if an MA receives an MR containing a specific AT of a misbehaving vehicle, it cannot determine: (1) whether the AT was issued by the system this MA is a part of, let alone identify which CCMS has issued it, and (2) which vehicle should be evicted from the system when the misbehaviour investigation result is positive. The reason of this problem is a combination of the intended privacy protection of vehicle owners and the simplification of the certificate definition.

TS 103 097 [13] adopts the certificate definition from IEEE 1609.2 [27]. The original definition of the `CertificateId` information element (IE) from [27] consists of four possible types: *linkageData*, *name*, *binaryId*, and *none*. TS 103

[1] In reality, the contact information of the CCMS system entities will most likely depend on which country or region a given vehicle is sold. Therefore, this configuration is likely done by entities such as auto dealers at the time of sales rather than at the time of manufacturing.

097 [13] removed the first and the third types, leaving only *name* and *none* as valid types.[2] According to [27], the *linkageData* type allows the system to trace an AT back to a specific vehicle. In other words, the exclusion of the *linkageData* type in the ETSI ITS standard caused this problem of not being able to identify a unique vehicle from an AT. Re-instating this data type is an obvious solution. However, doing so has a significant impact on the CCMS architecture. For further discussion of this issue, the reader is referred to Sec. 7.

5.3 Lack of Communication Models

The third gap is the lack of communication models that involves multiple CCMS systems. TS 102 940 [8] describes the relationship between a CCMS and vehicles that it manages. A given vehicle's perspective describes how a vehicle interacts with various system entities within a CCMS. Under this model, vehicles interact with entities in one CCMS only.

Vehicular communication is not limited to vehicles managed under a single CCMS. A notable example is the cross-border scenarios described in Sec. 4, where an MA under an CCMS forwards an MR to a second MA under a different CCMS. TS 102 940 [8] does not cover scenarios where a vehicle needs to communicate with multiple CCMSs or multiple entities across different CCMSs need to communicate, whether it is in the same or in another country.

5.4 Lack of Revocation Details

The fourth gap is the lack of a detailed specification for the revocation mechanism. TS 102 940 [8] includes the MA, responsible for investigating reported misbehaviours and determining whether the reported vehicle should be evicted from the system. However, the corresponding messages and procedures for vehicle revocation are not defined in TS 102 941 [12]. More precisely, this specification does not include communication involving MA and EA. Without it, the MA cannot communicate its decision to revoke a vehicle so that the EA can invalidate this vehicle's long-term certificate and deny future requests by the vehicle for additional ATs.

[2]The *name* type is used in EA, AA, and MA certificates to indicate a unique name of the entity with a UTF-8 encoded string that of at most 256 octets. The type *none* is used in ATs; it is a NULL value, reflecting the ATs' intended purpose of being anonymous for privacy purpose.

5.5 Problem Statement and the Root Cause

Based on the scenarios and gaps in the ETSI ITS standard discussed in Sec. 4 and Sec. 5.1 through 5.4, we summarize the underlying issues in the standard as a problem description and the corresponding root causes in Table 3. This root cause reflects missing functionalities to be added in the ETSI ITS standard.

Table 3: Problem Description and Root Cause

Problem Description	Root Causes
Vehicles do not know the MA's identity, thus cannot send MRs.	Lack of specification of vehicle configuration details.
The MA cannot trace the reported AT to a unique vehicle, thus it cannot investigate misbehaviour.	AT lacks information to trace back to a unique vehicle.
Detecting vehicles cannot identify the MA that issued the misbehaving vehicle's AT.	Lack of specification for vehicles to interact with more than one CCMS.
The MA cannot distinguish if the reported AT was issued by its own CCMS, or by another CCMS.	AT does not contains a unique information to identify the vehicle's origin.
The MA cannot identify the MA in the CCMS it which the vehicle belongs to,	Lack of specification to resolve the appropriate MA to forward the MR to.
Even if an MA can identify the specific MA under the specific CCMS, secure communication bteween CCMSs is not guaranteed.	Standard does not specify how inter-CCMS communication can be secured.

6 Solution

Based on the discussion in the previous sections, we now shift our focus to resolving these issues. Our solution addresses the root causes discussed in Table 3, and conforms to the architecture in the existing ETSI ITS standard [8] with minimum impact. Our solution involves two aspects: (1) a change in the certificate definition in TS 103 097 [13], and (2) an introduction of a new mechanism to resolve the linkage from an AT to the vehicle.

6.1 Design Goals

Our main goal is to keep the system simpler and lightweight comparable to that of IEEE 1609.2 [27] while achieving the intended functionalities. This list of goals also serves as a baseline to evaluate our solution. Specifically, the solution:

1. incurs minimum system impact.
2. is simple yet effectively addresses the gaps.
3. allows the reporting vehicle to autonomously identify the MA responsible for investigating the MRs.
4. handles the situation where a misbehaving vehicle may change its ATs. Thus MRs against the same vehicle may indicate different ATs.
5. supports all scenarios of vehicles' origin, including the same or different CCMS (i.e. *cross-border* scenarios).

6.2 Solution Part 1: Identifying an MA for a Vehicle

The first aspect is how to identify the MA from an AT – the MA responsible for handling MRs of the vehicle to which the reported AT belongs. For this purpose, we introduce a new IE, *maId*, in the AT. This concept is shown in Fig. 3. This MA is the one that belongs to the CCMS the vehicle has enrolled with and from whom it has received ATs. Further, this IE is of the type `Hostname` in an URL format. The corresponding IP address of the MA can be resolved by querying a DNS server.

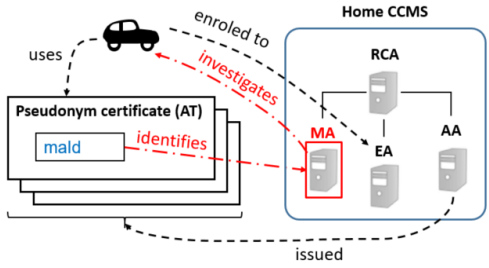


Figure 3: Determining the MA from an AT

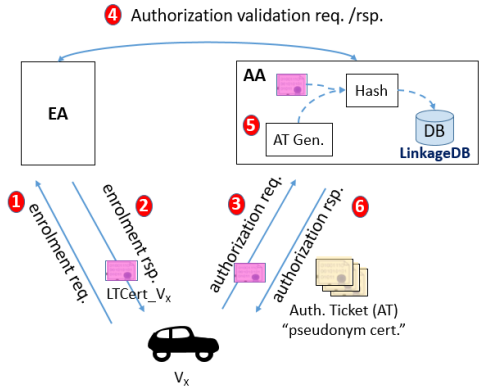
We further propose that the URL's content does not allow observers to easily infer the vehicle's origin, such as a country or a region name. For example,

geography-neutral domain names such as ".eu" and naming conventions without country or region names should be adopted. Because this point equally applies to all EU member countries, its administration and management are best coordinated at the EC level by incorporating it in the *Delegated Regulations* of ITS systems [5].

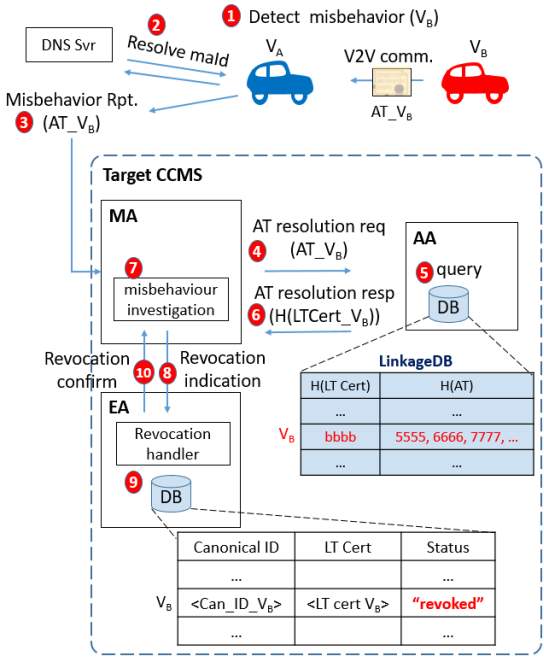
6.3 Solution Part 2: Resolving a Vehicle from an AT

The second aspect is to address the linkage from an AT to a unique vehicle. The MA needs to identify a vehicle to revoke its ATs if its misbehaviour investigation result is positive. In addition, it assists the MA when the reported vehicle changes ATs over time; if multiple MRs containing different ATs point to the same vehicle, the MA needs to be aware of this situation for misbehaviour investigation. For this purpose, we introduce a different approach from IEEE 1609.2 [27]. Our solution is illustrated in Fig. 4(a) and Fig. 4(b). The former describes how the CCMS establishes a link between a unique vehicle and its ATs. The latter describes the process of resolving this link from an AT back to a unique vehicle. The AA maintains a mapping database between these two pieces of information.

We first describe the steps to create the linkage as shown in Fig. 4(a). At the time of a successful enrolment, a vehicle (V_x) receives a long-term certificate ($LTCert_V_x$) from the EA (steps 1 and 2). Next, the vehicle sends an authorization request to the AA and attaches this $LTCert_V_x$ to this request (step 3). Upon receiving this request, the AA initiates the authorization validation procedure with the EA (step 4). After successfully validating the $LTCert_V_x$, the AA generates one or more ATs for this vehicle. These steps follow the existing procedures in TS 102 941 [12]. The key point of our solution lies in the following steps. At the time of the AT generation, the AA generates a hash of the $LTCert_V_x$ ($H(LTCert_V_x)$) and the hash of a newly created AT ($H(AT_V_{x,i})$), and stores these values in its database (step 5). If the AA creates multiple ATs for the vehicle, the step to create $H(AT_V_{x,i})$ is repeated. This way, the AA stores the mapping between $H(LTCert_V_x)$ and all hash values of all ATs for this vehicle ($\{g_x, \{h_{x,0}, ..., h_{x,i}, ..., h_{x,(n-1)}\}\}$, where $g_x = H(LTCert_V_x)$ and $h_{x,i} = H(AT_V_{x,i})$, and n is the number of ATs the AA issues simultaneously). Finally, all generated ATs are sent to the vehicle (step 6). This algorithm shows the scenario where the AA generates multiple ATs for a vehicle at a time due to the *butterfly key expansion* mechanism described in the SCMS [2] and TS 102 941 [12]. A simpler scenario where the AA generates only one AT at a time is a subset of this algorithm where the value of n is set to 1.



(a) Linkage Generation



(b) Linkage Resolution

Figure 4: Linkage Generation and Resolution

When a vehicle detects the misbehaviour of another vehicle, the following steps are taken to resolve the reported AT to a unique vehicle. This process is illustrated in Fig. 4(b) based on the cross-border scenario of Fig. 1(a) in Sec. 4. First, when a vehicle (V_A) detects a misbehaving vehicle (V_B), it uses the `maId` value in the V_B's AT ($AT_V_{B,i}$) to resolve the MA's URL. It sends an MR to the MA (MA_B) by attaching the $AT_V_{B,i}$ in the report (steps $1 \sim 3$). We propose that this communication between the V_A and the MA_B is protected by TLS [18]. Furthermore, both V_A and MA_B exchange their certificates at the time of TLS establishment so that they can mutually verify each other's authenticity. From MA_B's perspective, doing so allows it to detect and reject unauthorized vehicles from reporting fake MRs.

Upon accepting this report, MA_B queries AA_B for the corresponding $H(LTCert_V_B)$ value (step 4). The AA_B calculates $h_{B,i} = H(AT_V_{B,i})$ and queries its database to extract the corresponding g_B value ($H(LTCert_V_B)$), and returns it to MA_B (steps 5 and 6). With this step, MA_B can identify a unique vehicle without AA_B sharing the $LTCert_V_B$ itself with the MA_B, thus limiting the exposure of vehicle-identifying information to a minimum. With this information, MA_B can conduct a misbehaviour investigation of V_B. Due to the 1-to-N relationship between the vehicle-identifying information (g_B) and its associated ATs ($\{h_{B,0}, ..., h_{B,i}, ..., h_{B,(n-1)}\}$), any AT assigned to V_B will trace back to the same g_B value, successfully identifying a unique vehicle. This way, even if a misbehaving vehicle changes ATs over time, they are resolved to the same vehicle; this allows MA_B to conduct a misbehaviour investigation of a vehicle irrespective of the reported AT. The resulting improvement in this solution is illustrated in Fig. 5. With this improvement, V_A reports an MR directly to MA_B that is responsible for investigating misbehaviour of V_B. This is in contrast to Fig. 1(a) in Sec. 4 where the MR is sent to MA_A that cannot process it as V_B belongs to another CCMS. This solution also avoids two-hop reporting where MA_A needs to relay the received report to MA_B, reducing the number of messages, processing, and entities involved with the reporting.

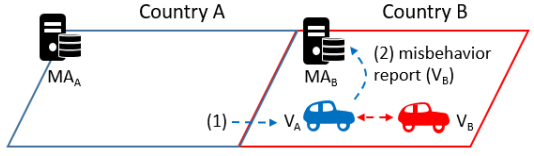


Figure 5: Improved MR Reporting in Scenario in Fig. 1(a)

If the misbehaviour investigation is positive, MA_B starts the revocation steps. It sends a revocation request to EA_B (step 8) so that the latter invalidates the vehicle's long-term certificate ($LTCert_V_B$) by changing the status of V_B as

"revoked" (step 9). This step will deny V_B's future requests for additional ATs. Finally, EA_B returns a confirmation back to MA_B (step 10).

7 Discussion and Evaluation

Our solution discussed in Sec. 6 fulfills the gaps identified in Sec. 5.5 and goals stated in Sec. 6.1. Our solution has a number of advantages. First, it is simpler and more efficient than the IEEE 1609.2 [27] standard. It realizes the necessary functionality within the existing system entities (goal 1). The procedure to carry out MR reporting, investigation, and revocation of ATs require only 7 messages as shown in Fig. 4(b). On the other hand, re-introducing *linkageData* type in `CertificateId` IE, as specified in the IEEE 1609.2 [27] standard, implies introducing three additional entities to the CCMS architecture, resulting in 7 interconnections among system entities and a total of 17 messages to support the same functionality. It will make the architecture more complex, negating the ETSI's conscious choice to simplify it [8].

Second, our solution effectively addresses the gaps (goal 2). The introduction of `maId` in the AT allows reporting vehicles to autonomously identify the MA responsible for resolving misbehavior reports of a particular vehicle (goal 3). In addition, the MA can identify a unique vehicle even if the misbehaving vehicle changes ATs over time (goal 4). Moreover, it seamlessly addresses all possible scenarios of vehicles involved in misbehaviour detection and reporting (goal 5). This includes vehicles from different countries or different CCMSs within a country, thus addressing the cross-border scenarios discussed in Sec. 4.

Third, a simpler solution also means that it has a smaller attack surface and thus it is more robust against adversaries and hardware or software failures in any of the system entities.

Fourth, the reported vehicle's long-term certificate exposure in our solution is limited to the minimum level. The AA shares the hash value of the vehicle's long-term certificate ($H(LTCert_V_x)$) to the MA; the latter then uses it to recognize the vehicle's uniqueness. This way, the reported vehicle's long-term certificate is kept within EA and AA only.

Fifth, the use of TLS [18] secures communication between the reporting vehicle and the MA. It is a proven technology that has been widely deployed. It offers additional robustness with its option to exchange certificates in both directions to ensure mutual authentication. This step gives the MA an opportunity to verify the reporting vehicle's authenticity. This way, the MA can detect and ignore reports from fake vehicles, preventing them from negatively influencing

the misbehaviour detection algorithm, and preventing the MA from evicting innocent vehicles.

As a potential disadvantage of our solution, the use of `maId` to hold an URL would be a concern if its content would directly indicate the country or region of the vehicle's origin, thus allowing passive observers to identify an attribute of the vehicle. In this respect, as we stated in Sec. 6, we propose to expand the existing EU regulation [5] so that the URL is defined and managed in a country- or location-neutral manner. We acknowledge that this area needs further research to ensure that the introduction of this IE does not lead to a vulnerability from the privacy perspective.

8 Recommendations

We recommend the following points to the ETSI ITS standard to address the gaps in the MR mechanism.

1. Update the CCMS architecture in TS 102 940 [8] by addressing a cross-border communication model where vehicles may communicate with multiple CCMSs.
2. Clarify how and when the contact information for the MA is configured to a vehicle in TS 102 941 [12].
3. Add an architectural description of MR reporting and revocation of misbehaving vehicles in TS 102 940 [8].
4. Introduce `maId` IE in the certificate definition in TS 103 097 [13], and define the reporting vehicle's mechanism to identify the MA for MR reporting.
5. Specify procedures and detailed definitions of revocation and confirmation messages between the MA and the EA in TS 102 941 [12].
6. Resolve redundant descriptions of the MR message definition in TS 102 731 [7] and TR 103 460 [11]. Section 7.1 in [7] already defines the functional model and content of the *report misbehaviour* message. This makes the message definition in TR 103 460 [11] redundant. It makes the most sense to update TS 102 941 [12] to include the message definition and its ASN.1 definition.

9 Conclusion

This paper highlighted gaps in the existing ETSI ITS standard in the MR reporting mechanism and presented a solution. Our solution conforms to the existing ETSI ITS architecture as it does not require any additional new entities. It requires fewer interactions than the IEEE 1609.2 standard but is equally effective in achieving its goals. The gaps we address in our solution include a fundamental oversight of not being able to trace back to a unique vehicle from an AT. In addition, our solution design is generic; it covers all cross-border scenarios where vehicles involved with MR reporting belong to multiple CCMSs. These scenarios are especially relevant in Europe where vehicles frequently cross country borders. Furthermore, it limits exposing the vehicle's long-term certificate while allowing the MA to conduct a misbehaviour investigation.

We propose that our solution be adopted by the ETSI ITS standard to ensure uniform implementation and deployment across Europe. Our future research area is to improve the robustness of URL information in ATs from privacy perspective.

Acknowledgments

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203 and by the Research Council KU Leuven C1 project on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058. Authors thank Dave Singelée of COSIC group in KU Leuven and Dimah Almani of University of Nottingham for their valuable comments and insights.

References

[1] 5G-Mobix. 5G for Cooperative & Connected Automated MOBIility on X-border Corridors. `https://www.5g-mobix.com`.

[2] Benedikt Brecht, Dean Therriault, André Weimerskirch, William Whyte, Virendra Kumar, Thorsten Hehn, and Roy Goudy. A Security Credential Management System for V2X Communications. In *IEEE Transactions on Intelligent Transportation Systems*, volume 19, pages 3850–3871. IEEE, 2018.

[3] 5G Carmen. 5G for Connected and Automated Road Mobility in the European UnioN. https://5gcarmen.eu/.

[4] European Commission. Connected and Automated Mobility. https://digital-strategy.ec.europa.eu/en/policies/connected-and-automated-mobility.

[5] European Commission. C(2019) 1789 Final, Commission Delegated Regulation (EU) of 13.3.2019 Supplementing Directive 2010/40/EU of the European Parliament and of the Council with Regard to the Deployment and Operational Use of Cooperative Intelligent Transport Systems. Technical report, European Commission, 03 2019.

[6] 5G CroCo. Fifth Generation Cross-Border Control. https://5gcroco.eu/.

[7] ETSI. TS 102 731: Intelligent Transport Systems (ITS); Security; Security Services and Architecture; V1.1.1. Standard, European Telecommunications Standards Institute, 09 2010.

[8] ETSI. TS 102 940: Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management; V2.1.1. Standard, European Telecommunications Standards Institute, 07 2018.

[9] ETSI. EN 302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, V1.4.1. Standard, European Telecommunications Standards Institute, 04 2019.

[10] ETSI. EN 302 637-3: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service; V1.3.1. Standard, European Telecommunications Standards Institute, 04 2019.

[11] ETSI. TR 103 460: Intelligent Transport Systems (ITS); Security; Pre-Standardization Study on Misbehaviour Detection; Release 2; V2.1.1. Standard, European Telecommunications Standards Institute, 10 2020.

[12] ETSI. TS 102 941: Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; V2.1.1. Standard, European Telecommunications Standards Institute, 10 2021.

[13] ETSI. TS 103 097: Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats; Release 2; V2.1.1. Standard, European Telecommunications Standards Institute, 10 2021.

[14] Mikal Fallgran, Markus Dillinger, Zexian Li, Guillaume Vivier, Taimoor Abbas, Jesus Alonso-Zarate, Toktam Mahmoodi, Sylvain Alli, Tommy Svensson, and Gabor Fodor. On Selected V2X Technology Components and Enablers from the 5GCAR Project. In *2018 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, pages 1–5. IEEE, 2018.

[15] Dirk Hetzer, Maciej Muehleisen, Apostolos Kousaridas, and Jesus Alonso-Zarate. 5G Connected and Automated Driving: Use Cases and Technologies in Cross-Border Environments. In *2019 European Conference on Networks and Communications (EuCNC)*, pages 78–82. IEEE, 2019.

[16] IEEE. IEEE 1609 Series Guide for Wireless Access in Vehicular Environments (WAVE) Architecture. `https://standards.globalspec.com/std/13372696/IEEE1609Series`.

[17] Vehicular Technology Society IEEE Standards Association. IEEE Std. 1609.2.1-2020, Standard for Wireless Access in Vehicular Environments (WAVE) — Certificate Management Interfaces for End Entities. Technical specification, IEEE, 2020.

[18] IETF. RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3. Standards track, Internet Engineering Task Force, 08 2018.

[19] Apostolos Kousaridas, Mikael Fallgren, Edwin Fischer, Francesca Moscatelli, Ricard Vilalta, Maciej Mühleisen, Sokratis Barmpounakis, Xavier Vilajosana, Sebastian Euler, Bruno Tossou, and Jesus Alonso-Zarate. 5G Vehicle-to-Everything Services in Cross-Border Environments: Standardization and Challenges. *IEEE Communications Standards Magazine*, 5(1):22–30, 2021.

[20] Apostolos Kousaridas, Andreas Schimpe, Sebastian Euler, Xavier Vilajosana, Mikael Fallgren, Giada Landi, Francesca Moscatelli, Sokratis Barmpounakis, Francisco Vázquez-Gallego, Roshan Sedar, Rodrigo Silva, Laurent Dizambourg, Stefan Wendt, Maciej Muehleisen, Kurt Eckert, Jérôme Härri, and Jesus Alonso-Zarate. 5G Cross-Border Operation for Connected and Automated Mobility: Challenges and Solutions. *Future Internet*, 12(1):5, 2019.

[21] Leo Mendiboure, Mohamed Aymen Chalouf, and Francine Krief. A Scalable Blockchain-Based Approach for Authentication and Access Control in Software Defined Vehicular Networks. In *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, pages 1–11. IEEE, 2020.

[22] Raul Muñoz, Francisco Vázquez-Gallego, Ramon Casellas, Ricard Vilalta, Roshan Sedar, Pol Alemany, Ricardo Martinez, Jesús Alonso-Zárate, Apostolos Papageorgiou, Miguel Catalan-Cid, Francesca Moscatelli, Giada Landi, Xavier Vilajosana, Andrea Bartoli, Denis Guilhot, Soumya Kanti Datta, Jérôme Härri, Rodrigo Silva, Laurent Dizambourg, Antonio Fernández, and Maciej Muehleisen. 5GCroCo Barcelona Trial Site for Cross-Border Anticipated Cooperative Collision Avoidance. In *2020 European Conference on Networks and Communications (EuCNC)*, pages 34–39. IEEE, 2020.

[23] Sebastian Peters, Fikret Sivrikaya, and Xuan-Thuy Dang. SEP4CAM-A Simulative/Emulative Platform for C-V2X Application Development in Cross-Border and Cross-Domain Environments. In *2021 IEEE/ACM 25th International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, pages 1–4. IEEE, 2021.

[24] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux. Securing Vehicular Communications. *IEEE wireless communications*, 13(5):8–15, 2006.

[25] SAE. J2735, Surface Vehicle Standard, V2X Communications Message Set Dictionary. Standard SAE J2735:2006, SAE International, 2006.

[26] IEEE Computer Society. IEEE Std. 802.11p-2010, Standard for Information Technology - Telecommunication and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. Technical specification, IEEE, 2010.

[27] IEEE Vehicular Technology Society. Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Services. Technical specification, Institute of Electrical and Electronics Engineers, Piscataway, NJ, United States, 03 2016.

[28] Konstantinos Trichias, Demestichas Panagiotis, and Mitrou Nikolaos. Inter-PLMN Mobility Management Challenges for Supporting Cross-Border Connected and Automated Mobility (CAM) over 5G. *Journal of ICT Standardization*, pages 113–146, 2021.

[29] Rens W van der Heijden, Felix Engelmann, David Mödinger, Franziska Schönig, and Frank Kargl. Blackchain: Scalability for Resource-Constrained Accountable Vehicle-to-X Communication. In *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, pages 1–5, 2017.

[30] Rens Wouter van der Heijden, Stefan Dietzel, Tim Leinmüller, and Frank Kargl. Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. *IEEE Communications Surveys & Tutorials*, 21(1):779–811, 2018.

Publication

A New Approach To Pseudonym Certificate Management in V2X Communication

Publication Data

Yoshizawa, T., and Preneel, B. A New Approach To Pseudonym Certificate Management in V2X Communication. In 2023 IEEE Vehicular Networking Conference (VNC), IEEE, pp. 25–32, 2023.

Contributions

- Principal author.

A New Approach To Pseudonym Certificate Management in V2X Communication

Takahito Yoshizawa and Bart Preneel

KU Leuven, ESAT/COSIC, Leuven, Belgium

Abstract. This paper proposes a new solution to the pseudonym certificate management and usage in Vehicle-to-Everything (V2X) communication. This solution is a result of our critical analysis of the Issue First Activate Later (IFAL) pseudonym certificate management scheme, which is mentioned in an ETSI Intelligent Transport System (ITS) pre-standardization document. While the IFAL scheme improves over the existing ETSI ITS Security Credential Management System (CCMS) for Europe and the Security Credential Management System (SCMS) for the US, it still has significant issues when real-world deployment is considered. To address these issues, we propose a novel activation scheme that improves the security properties by combining the OAuth concept and Authentication Encryption with Associated Data (AEAD) solution to provide confidentiality and authenticity of data. Our analysis and simulation show that our scheme significantly improves the security properties and efficiency of certificate usage. As a result, our solution is more robust, reliable, and efficient. We propose this solution for adoption in the ETSI ITS specifications.

1 Introduction

V2X communications wirelessly connect vehicles and road-side devices to improve overall road safety. IEEE has published the Wireless Access in Vehicular Environments (WAVE) standard in the 1609 series using IEEE 802.11p as the access layer technology. Since 2015, the 3rd Generation Partnership Project (3GPP) started standardization for V2X communication using mobile technology, called Cellular-V2X (C-V2X). The representative applications are the Dedicated Short Range Communications (DSRC) Basic Safety Message (BSM) [20] in the US, and the Cooperative Awareness Messages (CAM) [10] in Europe.

V2X communications rely on a Public Key Infrastructure (PKI) to protect the security of communications and the privacy of vehicle owners. Broadcast messages such as BSM and CAM require data authentication but do not require confidentiality. It is achieved by digitally signing these messages; the verification of this digital signatures requires the public key of the sender. An authenticated copy of this public key is distributed in a digital certificate issued by a Certification Authority (CA). To protect vehicle owners' privacy, vehicles are required to use pseudonyms and change them periodically along with their associated certificates.

The existing standards for certificate management in V2X communication include SCMS in IEEE 1609.2 [23] in the US, and CCMS in ETSI TS 102 940 [9] in Europe. In addition, IFAL [24] proposes a new approach as stated in the pre-standard report in ETSI TR 103 415 [8]. These schemes achieve the same goal of issuing and delivering certificates to vehicles while using different approaches.

In this paper, we specifically focus on an analysis of IFAL for several reasons. First, it is considered as the leading candidate for ETSI specification [8, 21, 27]. Its approach to separate the distribution and the activation of certificates into two distinct stages has merits over the SCMS [3] and the CCMS schemes [9]. However, a close examination shows that the IFAL scheme has a number of issues, some of which have already been addressed in the SCMS [3]. Second, several key issues in the ETSI's CCMS design [9] are left unresolved. Third, some of its aspects contradict the European Commission's (EC) policy on certificate use [6]. These points motivated us to examine the IFAL design in detail. This paper is our critical analysis on IFAL; we identify its issues, and propose improvements to address them.

The rest of the document is organized as follows. We first discuss related work in Sec 2. We then review the existing standards including IFAL in Sec. 3, and analyze the IFAL scheme in detail in Sec. 4. In Sec. 5 and 6, we present a novel solution and evaluate it. Finally, Sec. 7 concludes this paper.

2 Related Work

Schmidt [21] summarizes the status of ETSI ITS standard specification, and briefly mentions IFAL as the state-of-the-art certificate management schemes. However, it does not offer a detailed analysis. Other than this, we have identified only one article that analyzes the IFAL scheme in detail, raise issues, and propose an alternative approach to it. Yao et al. [27] proposes an optimized solution called Lightweight Pseudonym Changing (LPC) as an alternative scheme. Its

improvement over IFAL can be summarized as: (1) introducing both backward and forward secrecy by using a unique *transport key* to encrypt the *activation key* for each *epoch* using a Pseudo-Random Function (PRF) chain, (2) reduction of the storage requirement in the vehicle OBU by issuing ATs per *epoch* basis, (3) ensuring the *activation key* delivery with the use of asynchronous key agreement, and (4) reduction of signature generation time by using a chameleon hash function.

The first and the second points stem from adopting a per-*epoch*-basis AT generation, delivery, and activation. Although it is a valuable proposal, its improvement is limited. In addition, the performance evaluation on the third point indicates mixed results. Moreover, the paper overlooks more fundamental issues that we point out in Sec. 4, e.g. the inflexible AT usage policy (Sec. 4.4). This issue is closely related to the *epoch* concept in IFAL. To resolve it and other issues, our proposed solution removes this concept. In this sense, the level of improvement and impact of our solution is more fundamental than that of [27].

3 Background and Related Standards

3.1 IEEE 1609.2, 1609.2.1 (SCMS)

The IEEE 1609.2 [23] specifies the certificate management solution for V2X communication in the US, called SCMS [3]. It adopts the pseudonym certificate pool concept proposed by C2C-CC [2] with a minimum of 20 simultaneously active pseudonym certificates. The activation of the certificate is implicit, i.e. vehicles start and stop using certificates based on the validity period in each certificate. This solution [3] allows preloading of up to 3 years worth of pseudonym certificates. For the generation and distribution of certificates, it introduces *butterfly expansion*. This concept allows a vehicle to send one request for which the management system generates multiple pseudonym certificates; it reduces the communication overhead between vehicles and the management system compared to the conventional Certificate Signing Request (CSR). SCMS supports active revocation with the use of a Certificate Revocation List (CRL).

The IEEE 1609.2.1 [17] is another specification that defines detailed operations in end entities, e.g. vehicles, under the SCMS system. For activation of pseudonym certificates, it defines a mechanism called Activation Codes for Pseudonym Certificates (ACPC). It explicitly allows vehicles to operate V2X communication by providing *unlocking values* using binary hash tree as a data structure to convey these values. Although it significantly differs in details with

Issue First Activate Later (IFAL) scheme we examine detail in this paper, their objectives and ideas are equivalent – both mechanisms provide a way to convey keys to *unlock* pseudonym certificates in vehicles unless they are revoked. Due the space limitation, we examine exclusively on IFAL in this paper, and plan to analyze ACPC in detail as a follow-up future work.

3.2 ETSI ITS (CCMS)

In CCMS architecture for Europe, pseudonym certificate is called an Authorization Ticket (AT). For AT generation, TS 102 941 [11] supports both the conventional CSR and the *butterfly expansion* approaches. In the former case, a vehicle generates a private/public key pair and sends the latter to the management system to request a certificate, while the vehicle securely stores the private key, in a tamper-proof Hardware Security Module (HSM).

Unlike SCMS, CCMS does not actively revoke ATs; TS 102 941 [11] specifies the exclusive use of passive revocation where the management system denies future requests by a vehicle to obtain additional ATs if the vehicle has been revoked. This way, as its current ATs expire, a vehicle is excluded from V2X communication.[1]

3.3 Issue First Activate Later (IFAL)

IFAL [24] is a certificate management scheme proposed for ETSI ITS standardization [8].[2] As the name implies, its main characteristic is a clear separation of generation and loading of ATs to vehicles and the subsequent activation and usage of them. Hence, we discuss the following points in sequence: (1) generation and preloading, (2) activation, and (3) revocation. Time is divided into *epochs*; the IFAL paper proposes its duration of 90 days [24].

Generation and Preloading of ATs

A batch of ATs is generated at the time of successful vehicle enrolment with the Enrolment Authority (EA). Preloading of up to 5-year worth of ATs is foreseen. Each AT is assigned to a fixed 12-minute period with 1-minute overlap with

[1] In this sense, the target of revocation is a vehicle, and not individual certificates. This is a notable point as, in a PKI context, certificates are revoked rather than the entity that use them.

[2] Its original version appeared in 2016. In this paper, we reference and analyze the latest version published in 2019 [24].

the next AT. In other words, only one AT is active at a time, and it is used only once.

Activation of ATs

The activation of ATs is done per *epoch*. To do so, the certificate management system sends an *epoch*-specific *activation key* to each vehicle. The derivation of an *epoch key* is illustrated in Fig. 1. An *activation key* for vehicle v for *epoch* i ($K_{ACT_v_i}$) consists of the *epoch key* for vehicle v for *epoch* i ($K_{EP_v_i}$), encrypted by the *transport key* for vehicle v (K_{TR_v}). After decryption of the *activation key*, the vehicle uses the *epoch key* to derive the private key that corresponds to each AT's public key within *epoch* i. Thus, explicit delivery of an *activation key* at each *epoch* allows the vehicle to generate valid signatures for its messages within the *epoch*. In other words, the absence of a valid activation key for an *epoch* prevents the vehicle from generating valid signatures for its messages, effectively revoking a vehicle. The *transport key* is statically fixed for a vehicle at the time of successful enrolment.

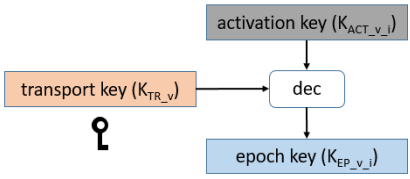


Figure 1: Epoch Key Derivation in IFAL

Revocation of ATs

In IFAL, only passive revocation of ATs is supported. This aligns with both the ETSI ITS specification [11] and the EC's certificate policy [6]. In other words, the management system denies to provide future *activation keys* if the requesting vehicle is identified as revoked.

4 IFAL Issues

4.1 Wasted Certificates

The IFAL's approach to generate ATs is highly inefficient as it does not take the actual vehicle usage into account. Typically, passenger vehicles are driven no more than a few hours a day, e.g. daily commuting. Studies show that the average daily commute times in Europe is 46.1 minutes per day for employees [12]; in the US, it is 27.6 minutes one-way (55.2 minutes round trip) [4]. Under the IFAL scheme, this translates to not using 95.2% of the generated ATs for employees in Europe, which represents a significant amount of unneeded computation, distribution, and storage of certificates.

According to the latest statistics, the total number of vehicles in EU countries is approximately 277.8 million [1]. If the IFAL scheme were deployed in all vehicles in all EU countries, ∼13.27 trillion (13.27×10^{12}) ATs, or ∼1.95 petabytes (1.95×10^{15} bytes) of ATs would require storage and transmission per year. Out of these, ∼1.85 petabytes of data, are discarded without being used. This waste of energy is also undesirable from an environmental impact perspective.

4.2 Transfer of Private Key Information over Activation

As discussed in Sec. 3.3, in the IFAL scheme, the vehicle receives *activation key* per *epoch* and derives *private keys* to sign messages. In other words, the information to derive private keys is transmitted to the vehicle during the activation process. This is in contrast to the conventional CSR process where the entity that requests a certificate generates and securely stores the private key. If an adversary successfully breaks this *transport key*, all private keys that correspond to all ATs in the *epochs* for the specific vehicle are revealed. This opens an opportunity to compromise vehicles' operation.

4.3 No Forward and Backward Secrecy

The issue discussed in Sec. 4.2 further implies that the IFAL scheme fails to guarantee both *forward* and *backward secrecy*. The *transport key* is generated during the initial vehicle enrolment with the EA. As the IFAL scheme does not renew this *transport key*, it is static per vehicle once it is generated. This has a significant implication – if an adversary breaks a vehicle's *transport key*, all private keys that correspond to all ATs in all past, present, and future *epochs* for this vehicle are revealed. This adversary can generate valid signatures for all

ATs within the current and future *epochs* by obtaining current and future *epoch keys* by decrypting *activation keys*. Therefore, the IFAL scheme offers neither *forward* nor *backward secrecy*. Further, it offers no solution to recover from this situation due to the absence of a mechanism to re-key the *transport key*.

4.4 Inflexible AT Usage Policy

The AT usage in the IFAL scheme is one-time only in a strictly sequential manner with each AT valid for a specific 12-minute interval. This regular and periodic time-based AT change behavior may allow observers to link ATs, hence compromising the unlinkability property. From the perspective of maintaining unlinkability, it is better to introduce variability or randomness in change intervals.

4.5 Gap Period in Passive Revocation

The IFAL scheme adopts only passive revocation for ATs (Sec. 3.3). This creates its own issue – it leaves a time gap between the time when a vehicle is revoked and when the vehicle stops transmission. As discussed in Sec. 3.3, an *activation key* is delivered to a vehicle per *epoch* of 90 days. This implies that a revocation event of a vehicle will not stop the vehicle from transmitting messages until the end of the current *epoch*. In the worst-case scenario, this time gap is as long as the *epoch* duration, i.e. 90 days. This implies that the *epoch* duration significantly influences the timeliness of the revocation. The shorter the *epoch* duration, the better from a revocation perspective. However, it comes at the cost of more frequent *activation key* distribution. There is a clear trade-off between the revocation timeliness and the activation frequency. The same issue applies to the ETSI standard as it relies on passive revocation only [11]. In this case, a vehicle becomes aware of its revoked condition when the Authorization Authority (AA) denies the next AT request from the vehicle.

4.6 Sub-optimal and Unreliable Activation Channels

The IFAL scheme [24] uses SMS and manual operation as activation mechanisms. However, it does not address potential situations where SMS messages are not delivered, nor does it address recovery mechanisms from such conditions.

The IFAL paper [24] justifies the use of SMS given the mandate of EU eCall directive in 2018 [5]. This directive clarifies that the in-vehicle mobile terminal stays dormant unless an accident occurs [5, 19]. This statement implies that

the vehicle's mobile device is not registered to the mobile network under normal circumstance; thus SMS messages cannot be delivered to it. In addition, there are well-known security vulnerabilities in SMS as multiple ways exist to circumvent SMS-based multi-factor authentication (MFA) [13, 22]. As a result, the US National Institute of Standards and Technology (NIST) recommends to not use SMS-based MFA.

5 A Novel Activation Scheme

5.1 Goals and Assumptions

The goals we aim to achieve include addressing all issues we identified in Sec. 4. In addition, we include the following elements into the solution design: (1) automatic activation without human intervention, (2) detection and recovery from failure conditions, and (3) taking usage scenarios into account where vehicles may not be driven every day.

As security assumptions, we consider that the HSM can be potentially malicious, thus can possibly disrupt the activation procedure by launching active attacks such as replay attack or intentionally causing the procedure to fail. A fake HSM may attempt to impersonate another vehicle's HSM to create a DoS type situation to a victim vehicle. In addition, there can be adversaries that may passively monitor the communication between the HSM and the management system to obtain information that identifies vehicles or compromise vehicle owners' privacy. We take our design by taking these points into consideration.

5.2 Solution Description

Our solution combines existing concepts in a novel manner to address the issues identified in Sec. 4 and goals stated in Sec. 5.1. We introduce a different approach to the activation; activation serves as a mean for the management system to periodically and explicitly give permission to the vehicle to transmit V2X messages. For this purpose, we combine the OAuth model [16] and the use of a user's device (remote key) as means of authorization. Involving a user's device for authorization aligns with the trend in MFA solutions to be applied in V2X context [18].

The OAuth model views the signature generation as a service that the HSM provides to the OBU. This way, our solution realizes the equivalent end result of revoking the vehicle's ATs by the HSM denying its service. Figure 2 illustrates

the overall concept and the mapping of OAuth entities to the vehicle context. In OAuth terminology, the *resource owner* is the user (e.g. driver); the *client* or the *user agent* is the vehicle's On-Board Unit (OBU); the *resource server* is the vehicle's HSM; the *authorization server* is the AA in the certificate management system, respectively.

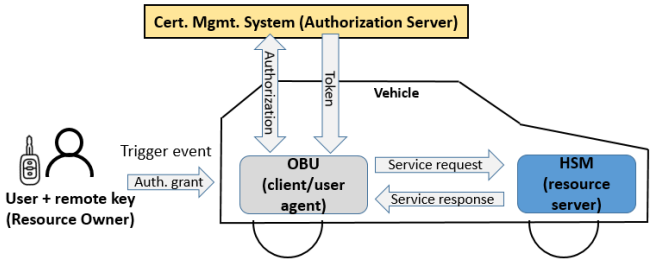


Figure 2: OAuth Model in Vehicle Context

We use a modified version of the OAuth framework for the activation procedure. The procedure is triggered by the user unlocking the vehicle's door using the remote key and starting the engine. This user's action is considered as an implicit authorization to the vehicle OBU (*user agent*). This event triggers the OBU to initiate the HSM (*resource server*) to query its *activation status* to the AA (*authorization server*). Then the AA checks the revocation status of the vehicle and returns it to the HSM as the *activation status*.[3] Upon receipt, the HSM reflects this status to its operation: whether to enable or disable signature generation for messages that the OBU generates. Finally, the HSM returns an acknowledgment to the AA.

5.3 Detailed Description – Activation

We use AES Galois/Counter Mode Synthetic Initialization Vector (AES-GCM-SIV) specified in RFC 8452 [15] as a building block of the mechanism to generate, deliver, and verify the vehicle's *activation status*. AES-GCM-SIV is a type of Authentication Encryption with Associated Data (AEAD) which assures both confidentiality and authenticity of data. AES-GCM-SIV has been integrated in Google's BoringSSL library and in QUIC [14]. It is designed to be resistant to potential reuse of nonce when its uniqueness is not guaranteed. It uses a vehicle-specific key generation key (KGK, $k_{KG_v,i}$) to derive a pair of keys for encryption ($k_{enc,i}$) and authentication ($k_{auth,i}$) for each nonce. In addition, we also re-key this KGK at every iteration (i) of this procedure. This dynamic

[3] An *activation status* is semantically equivalent to an activation key in the IFAL scheme.

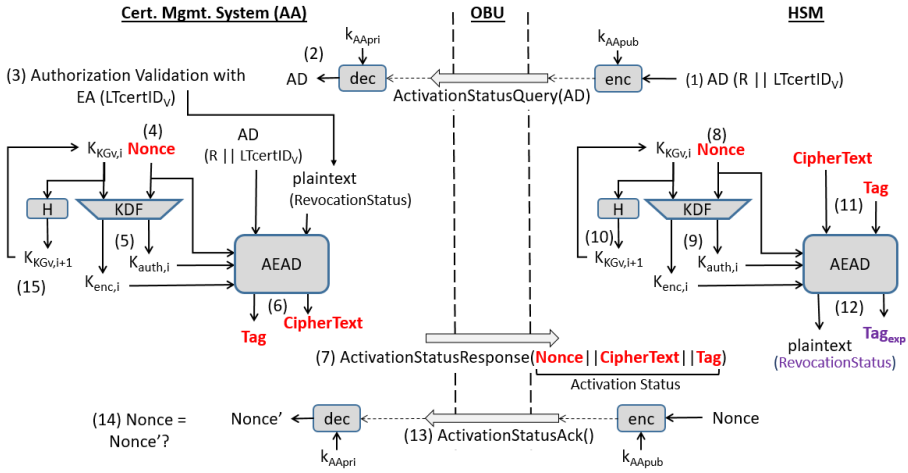


Figure 3: Activation Status Generation and Verification

update of KGK is the main difference in our solution while the *transport key* remains static in the IFAL scheme.

Figure 3 illustrates the processing in both the AA and the HSM according to RFC 8452 [15].[4] This procedure is strictly between the AA and the HSM; the vehicle OBU is simply a pass-through. Table 1 shows the notations.

Table 1: Notation Definitions

Notation	Definition
AD	additional data
$AEAD$	Authentication Encryption with Associated Data
$H()$	hash function
$k_{KG_v,i}$	key generation key for vehicle v for iteration i
$k_{enc,i}$	encryption key (per RFC 8452) for iteration i
$k_{auth,i}$	authentication key (per RFC 8452) for iteration i
k_{AApub}	public key in AA's server certificate [11]
k_{AApri}	private key of AA [11]
$KDF()$	Key Derivation Function
$LTcertID_v$	long-term certificate ID of vehicle v
R	random value

[4]RFC 8452 [15] defines detailed building blocks and operations such as POLYVAL, padding, and truncation. However, in this figure, we restrict ourselves to the description at a high-level abstraction that is sufficient to understand the scheme.

First, the HSM generates a random value (R) and concatenates it with the vehicle-specific long-term enrolment certificate ID ($LTcertID_v$)[5] to generate the associated data (AD), and sends it to the AA in ActivationStatusQuery message (Step 1 in Fig. 3). This message is encrypted using the public key in the AA's server certificate (k_{AApub}) as defined in TS 102 941 [11] to conceal signaling messages. The AA first decrypts this message using the corresponding private key (k_{AApri}) and runs the authorization validation with the EA, as defined in [11], to check the requesting vehicle's revocation status using the received $LTcertID_v$, and reflects this status to the plaintext (Step 2, 3). Next, the AA generates a nonce and, along with the current KGK, creates a key pair ($k_{enc,i}, k_{auth,i}$) (Step 4, 5). Using inputs of a tuple (plaintext, AD, nonce, $k_{enc,i}$, $k_{auth,i}$), the AA generates a *tag* and a *ciphertext* [15] (Step 6). Finally, the AA encrypts the concatenation of (*nonce*, *ciphertext*, *tag*) using k_{AApri} and send its output to the HSM as the *activation status* in the ActivationStatusResponse message (Step 7).

The receiving side follows the reverse operation to obtain the plaintext and verify its authenticity. Upon receiving this response message, the HSM decrypts it using k_{AApub}, extracts the nonce, and follows the same procedure to derive $k_{enc,i}$, $k_{auth,i}$, and $k_{KG_v,i+1}$ (Steps 8–9). It also derives the next KGK ($k_{KG_v,i+1}$) using a cryptographic hash function (Step 10). Then it decrypts the ciphertext to obtain the plaintext and generates the expected tag (Tag_{exp}), and verifies if the received tag and the expected tag match (Step 11, 12). If they match, the HSM reflects the received revocation status to the operation of signature generation function, i.e. if this status indicates the vehicle is revoked, the HSM disables its signature generation function; otherwise, it enables this function.

Finally, the HSM encrypts *nonce* and sends its output as an ActivationStatusAck message to the AA (Step 13). The AA decrypts it using k_{AApri} to obtain $nonce'$ and verify if $nonce = nonce'$ holds (Step 14). If so, the AA updates $k_{KG_v,i+1}$ (Step 15). This final step ensures the AA that the HSM has successfully received the activation status and updated the KGK. This three-way handshake prevents the KGK mismatch condition, which may be caused by an error event, e.g. a temporary communication failure. Further, if this procedure fails, the HSM may retry the procedure as a recovery action. At the end of a day (or a 24-hour cycle since the last successful activation), the HSM resets its state so that it requires a new activation to continue the normal signature generation and this activation procedure is repeated.

[5]This $LTcertID_v$ is issued by the EA at the time of the vehicle's successful enrolment. Thus, HSM's possession of it is a pre-condition. As a part of our solution, we also require that this ID is stored in the tamper-resistant HSM.

5.4 Detailed Description – OBU Tx Operation

When the OBU constructs a new V2X message, it requests the HSM to generate a signature by passing a message digest d. If the activation is successful, according to the procedure in Sec. 5.3, the HSM generates a valid ECDSA signature (r, s) to the message and returns it to the OBU; the OBU then transmits the message. If the activation is unsuccessful, then the HSM ignores the OBU's request to generate a signature, which triggers a time-out event at the OBU; thus it is not able to transmit the message.

5.5 Detailed Description – Certificate Use

In our solution, we observe the EC recommendation in which the maximum preloading period of ATs is 3 months [6]. It reduces the AT storage requirement in vehicles compared to longer period, e.g. 5 years as proposed in the IFAL scheme [24]. Each AT is assigned to a longer period by *floating* them within the intended usage period, e.g. a period of a week. This is the approach proposed by C2C-CC [2] (Sec. 3.1), and has a benefit of reducing waste of unused ATs (Sec. 4.1).

6 Analysis and Discussion

6.1 Security Properties

We now analyze the security properties of our solution described in Sec. 5. Based on the security assumptions in Sec. 5.1, we analyze our solution based on the following types of attacks: (1) replay attack, (2) impersonation attack, (3) intentional procedure failure, (4) suppressing the activation procedure, and (5) passive observation to obtain privary information. In addition, we also consider the scenario to cause the KGK misalignment.

First, to prevent replay attack, our procedure uses two unique numbers in each execution of this procedure to prevent this type of attack; one is R generated by the HSM and *nonce* used by the AA. Specifically, the HSM sending the *nonce* value received in ActivationStatusResponse message (Step 7) in ActivationStatusAck message (Step 14) prevents this type of attack by a fake HSM.

Second, impersonation as another vehicle is mitigated as the attacker requires the $LTcertID_v$ for this purpose. This value is delivered to the vehicle at the

time of successful enrolment with the management system, implying that only the legitimate vehicles possess this value, and it is unique to each vehicle. As this ID is stored in the vehicle's tamper-resistant HSM, impersonation attack requires successfully breaking into the HSM module, which goes against the fundamental security tenet described in TS 102 940 [9].

Third, intentional procedure failure situations can be caused by a compromised or a fake HSM. As stated above, resistance against tampering of HSM is a fundamental tenet of the V2X certificate management system [9]. Therefore, the HSM's use of the $LTcertID_v$ in the procedure and the corresponding verification in the AA will prove the HSM's legitimacy.

Fourth, a compromised vehicle may suppress this activation procedure. However, our solution sets an expectation in the AA that each vehicle executes this procedure periodically, e.g. daily. This way, an absence of this activation triggers the AA to suspect a malicious vehicle. At the same time, a daily execution of this procedure is not guaranteed in reality as vehicles are not necessarily driven every day. Furthermore, temporary unavailability of communication with the management system at the time of vehicle use results in the similar situation. To address this variability, the management system can configure a maximum time interval to the vehicle as a system parameter. At every successful activation, the AA resets this timer. From the AA's perspective, the absence of this procedure longer than this interval can indicate that a vehicle is potentially malicious.

Fifth, our solution prevents passive observers from compromising vehicle owner's privacy. The only potential information that may lead to privacy in the activation procedure is $LTcertID_v$ in the ActivationStatusQuery message. However, obtaining this information requires successfully decrypting this message which require k_{AApri} that is secretly stored in the AA. This implies an adversary needs to successfully break into the AA to steal this private key. This is clearly beyond the scope of passive observation.

Finally, update of KGK ($k_{KG_v,i+1}$) requires careful consideration as its misalignment will cause future execution of this procedure to fail. For example, a fake ActivationStatusAck message by a fake HSM sent at the right timing can create this situation as the AA updates its KGK but the real HSM may not. In this respect, the three-way handshake described in Sec. 5.3 requires the AA to verify this ack message is a valid one. In our solution, we ensure this condition by the HSM re-sending R that was sent in the earlier step of the procedure. However, this time, R value is encrypted without other information, unlike AD as shown in the first message in Fig. 3. As these messages are encrypted, this makes it difficult for passive eavesdroppers to correlate or identify this value. Verifying the R value in the first message against the one obtained in the ActivationStatusAck message ensures that this message is sent by the same

entity that started the procedure.

6.2 Storage and Bandwidth Comparison

Table 2 summarizes the quantitative analysis of IFAL and our solution. From storage capacity perspective, the IFAL scheme requires over 1.5 Mbytes in a vehicle to store 3 months amount of ATs while our scheme requires 34 Kbytes for the same period, i.e. ∼2.2% of the former. Furthermore, if we follow the IFAL scheme [24] in which vehicles are preloaded for 5-year worth of ATs, the vehicle's storage requirement exceeds 31.5 Mbytes, while our scheme requires less than 700 Mbytes. Furthermore, our scheme reloads ATs on a weekly basis after the initial preloading period of EC-recommended 3 months ends [6]. This means that the storage requirement in vehicles will reduce from 3 months to one week worth of ATs, which is merely ∼2.6 Kbytes.

Next, we consider the bandwidth usage required to transfer ATs to vehicles. For this comparison, we base our traffic calculation at the certificate management system rather than at the vehicle to avoid possible variations of communicate path, such as wide-area mobile network or V2I connection to Road Side Units (RSU).[6] Given that the signaling messages in our solution (ActivationStatus-Query, ActivationStatusResponse, and ActivationStatusResponse) are newly introduced messages, we use the message lengths of Authorization Request and Response messages defined in [11] as the baseline for comparison. The *activationCode* message as described in [24] is sent to vehicles per epoch (90 days).

6.3 Simulation Result of AES-GCM-SIV

We conducted a simulation to evaluate the performance of our AES-GCM-SIV-based activation solution. It was run on a pair of PCs, equipped with Intel i7-6600U dual-core CPU at 2.6 GHz with 32GB of RAM running Windows 10, and the AES-GCM-SIV is based on an implementation in [26]. We corrected several bugs in this code, and added a communication functionality. We executed three sets of simulation run with varying amount of delays in the response message: (1) no delay, (2) 10 msec, and (3) 15 msec, respectively. These intentional delays are inserted at the server side to simulate the database query

[6]The MTU of Ethernet frame and IPv6 packet are 1500 and 1280 bytes, respectively. We also account for the extra IPv6 headers for fragmentation. Additionally, TS 102 941 [11] specifies that the security management-related messages are encrypted using the respective server certificates; therefore, we assume that generic security protocols such as Transport Layer Security (TLS) is not used for the protection of signaling messages.

Table 2: Comparison of Required Storage and Bandwidth

Content	Size (bytes)	
	IFAL	Our solution
Storage Capacity Requirement		
# of certs, 1 week	916[1]	20[1]
Cert size, 1 week	120,960	2,640
# of certs, 3 months	11,782[1]	257[1]
Cert size, 3 months	1,555,200	33,943
# of certs, 5 years	238,909[1]	5,214[1]
Cert size, 5 years	31,536,000	688,286
Effective storage required	31,536,000	33,943
Bandwidth Usage Requirement		
Message headers (Eth/IPv6/TCP)	94	94
ActivationStatusQuery message	n/a	258
ActivationStatusResponse message	n/a	149
ActivationStatusAck message	n/a	149
Single cert. req/resp	n/a	595
Batch cert. req/resp	n/a	11,900
ActivationCode message	149	n/a
5-year cert. download	33,413,481	3,102,500[2]

Note 1: The unit is number of certificates (all others are bytes).
Note 2: This number is shown strictly for comparison purpose only as our solution support maximum of 3-month worth of ATs.

and communication latency. For each case, we executed 2000 message exchanges and took an average. The resulting performance numbers are shown in Table 3.

Table 3: Simulation Result of Authorization Query / Response

Case	Avg. Request /Response Time (sec)	Avg # of Requests/sec	Condition
1	0.005231	196.803	no delay
2	0.015935	63.086	10 msec delay
3	0.021882	46.102	15 msec delay

We describe the performance in terms of the number of activation procedures per second as it provides indication of how much processing capacity the management system needs in order to account for the number of queries the system receives from vehicles. With no delay in response (case 1), one procedure run takes slightly over 5 msec, which translates to 196 interactions per second.

With 10 msec and 15 msec delay (case 2, 3), the number of procedures per second reduces to 63 and 46, respectively.

Forty-six queries/sec. with 15 msec delay translates to 165,600 queries/hr. As an estimate, we use the statistics of Germany [7] given that it has the largest number of registered vehicles and population in Western Europe (48.427 million registered vehicles for the population of 83.3 million (58.14%)). The most populated state is North Rhine-Westphalia which has 17.926 million people [25]; it translates to 10.421 million registered vehicles according to this vehicle/population ratio. If all of these vehicles issues one query per day, then it translates to 434,215 queries/hr. Our simulation result indicates that 3 servers of this performance will suffice to serve all queries for the vehicle population. This simulation result indicates that applying our solution is a viable one.

Table 4: Comparison of Key Points in Solutions

Characteristics	IFAL Solution	Our Solution
Advantages of Our Solution		
Key in activation, freshness, forward & backward secrecy	Static transport key, re-key not supported, Forward and backward secrecy not supported.	Use of random and nonce, KGK key pair and re-key at every activation. Forward and backward secrecy are maintained.
Activation key derivation, key encryption	SMS or manual operation, using asymmetric encryption, potential key leakage.	AEAD-based (AES) solution over control channel, implicit re-key prevents leakage.
Private key derivation	Seed info (*activation key*) sent at activation.	Securely stored in the vehicle's HSM.
Passive revocation time gap	Max. of 1 *epoch* long (90 days).	Max. of 1 activation cycle (e.g. 1 day).
Activation interval	Per-*epoch*-based (90 days).	Shorter (daily) activation, remove *epoch* concept.
AT preloading & storage	5-year worth of ATs.	Max. 3-month worth of ATs.
AT usage & waste	Fixed 12-min period, large waste.	Vehicle-centric flexible usage policy.
Activation trigger	SMS or manual operation.	User's action to use the remote key.
Activation failure handling	Not addressed.	Failure detection and retry.
Disadvantages of Our Solution		
Activation cycle	Per-*epoch*-based (90 days).	Shorter (daily) activation.
AT generation	5-year worth of ATs preloaded before activation.	CSR approach needs scalability improvement.

6.4 Advantages

Table 4 summarizes the advantages and disadvantages of our solution. Our solution has a number of advantages over both the IFAL scheme and the CCMS in the ETSI ITS standard, and addresses all issues we identified in Sec. 4. As a result, it has a higher level of security and is more robust than the IFAL scheme for the following reasons.

Our solution significantly shortens the latency to evict misbehaving vehicles due to the change of the semantics of *activation* on a daily basis. Thus, a negative outcome of the activation procedure immediately stops the vehicle's transmission by denying the HSM from generating valid signatures. Furthermore, our solution minimizes the inefficient use of ATs and alleviates the vehicle storage due to the combination of longer validity period to ATs (e.g. a week) and following the EC recommended preloading period of 3 months [6]. The exact AT usage is delegated to vehicles based on the actual driving and usage, rather than being dictated by the inflexible validity period set in ATs. Activation occurs automatically without user intervention, triggered by the user's remote key to unlock the vehicle door and start the engine. The solution also mitigates failure conditions by retrying the procedure.

Deploying our solution requires implementations only in the vehicle HSM and the AA; no other system entities are impacted as the solution is transparent to them. A software-only solution incurs no hardware retrofitting or replacement. Finally, our solution accounts for realistic vehicle usage scenarios where a vehicle may not be driven every day.

6.5 Disadvantages

Our proposed scheme includes a few downsides compared to the IFAL scheme. However, they are relatively minor and can be mitigated. The first is concerning the shorter activation period; a more frequent activation increases the processing in vehicles and the management system and network traffic between them. However, as shown in Sec. 6.2, activation procedure consisting of three messages requires a small amount of data ($\sim$550 bytes) only. In addition, as the *connected vehicle* usage (e.g. infotainment) increases, the short daily activation procedure will be a negligible increase with respect to the total data volume a vehicle generates in a day.

The second downside is the nature of the CSR-based AT request. It is supported in the ETSI ITS standard along with the *butterfly key expansion* scheme [9]. Although the latter is more efficient in terms of generating an arbitrary number

of ATs in a single request, it requires transferring the activation key for the vehicle to dynamically generate private keys from it. However, this scheme does not suit well to our solution due to the change of *activation* semantics. This situation implies that the vehicle requires repeating the AT request procedure n times to obtain n ATs during the preloading period, which is less scalable than the *butterfly key expansion* scheme. However, as the number of ATs simultaneously active is rather limited (∼20 ATs per week according to C2C-CC [2]), this situation is considered as a trade-off of all advantages our solution offers.

7 Conclusion and Future Work

In this paper, we introduced a novel solution for pseudonym certificate management. Our solution combines OAuth concept and an efficient AEAD scheme (AES-GCM-SIV) along with modified activation semantics. It addresses all identified issues from our close examination of the IFAL scheme. Our analysis and simulation result show that our solution improves in security property, communication volume, and storage requirement perspectives. The issues we identified in the IFAL scheme and thus addressed in our solution are significant to an extent that the former introduces negative impacts in various aspects, including lack of robustness as a security solution as well as its environmental impact due to its highly inefficient use of certificates. We propose that our new enhanced scheme is considered for adoption in the ETSI ITS standard. As our future work, we plan to investigate further improvements in the use of CSR in our solution. In addition, detail analysis of ACPC in IEEE 1609.2.1 as discussed in Sec 3.1 and performance comparison of our solution against it is our next step.

Acknowledgments

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203 and by the Research Council KU Leuven C1 project on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058. Authors thank Dave Singelée of COSIC group in KU Leuven and Dimah Almani of University of Nottingham for their valuable comments and insights.

References

[1] European Automobile Manufacturers Association. ACEA Report Vehicles in Use Europe, [ONLINE] https://www.acea.auto/files/report-vehicles-in-use-europe-january-2021-1.pdf. https://www.acea.auto/files/report-vehicles-in-use-europe-january-2021-1.pdf.

[2] Norbert Bißmeyer, Hagen Stübing, Elmar Schoch, Stefan Götz, Jan Peter Stotz, and Brigitte Lonc. A Generic Public Key Infrastructure for Securing Car-to-X Communication. In *18th ITS World Congress on Intelligent Transport Systems*, volume 14, 2011.

[3] Benedikt Brecht, Dean Therriault, André Weimerskirch, William Whyte, Virendra Kumar, Thorsten Hehn, and Roy Goudy. A Security Credential Management System for V2X Communications. In *IEEE Transactions on Intelligent Transportation Systems*, volume 19, pages 3850–3871. IEEE, 2018.

[4] Charlynn Burd, Michael Burrows, and Brian McKenzie. Travel Time to Work in the United States: 2019. *American Community Survey Reports, United States Census Bureau*, 2:2021, 2021.

[5] European Commission. Mobility and Transport, [ONLINE] https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en. https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.

[6] European Commission. Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1.1. *European Commission*, June 2018.

[7] CEIC Data. Germany, [ONLINE] https://www.ceicdata.com/en/country/germany. https://www.ceicdata.com/en/country/germany.

[8] ETSI. TR 103 415: Intelligent Transport Systems (ITS); Security; Pre-standardization Study on Pseudonym Change Management; V1.1.1. Standard, European Telecommunications Standards Institute, 04 2018.

[9] ETSI. TS 102 940: Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management; V2.1.1. Standard, European Telecommunications Standards Institute, 07 2018.

[10] ETSI. EN 302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, V1.4.1. Standard, European Telecommunications Standards Institute, 04 2019.

[11] ETSI. TS 102 941: Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; V2.1.1. Standard, European Telecommunications Standards Institute, 10 2021.

[12] José Ignacio Giménez-Nadal, José Alberto Molina, and Jorge Velilla. Commuting and Self-Employment in Western Europe. *Journal of Transport Geography*, 88:102856, 2020.

[13] Roger Grimes. The Many Ways to Hack 2FA. *Network Security*, 2019(9):8–13, 2019.

[14] Shay Gueron, Adam Langley, and Yehuda Lindell. AES-GCM-SIV: Specification and Analysis. *Cryptology ePrint Archive*, 2017.

[15] Shay Gueron, Adam Langley, and Yehuda Lindell. AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption, RFC 8452. Technical report, Internet Research Task Force (IRTF), 2019.

[16] Dick Hardt. RFC 6749: The OAuth 2.0 Authorization Framework, Oct. 2012.

[17] Vehicular Technology Society IEEE Standards Association. IEEE Std. 1609.2.1-2020, Standard for Wireless Access in Vehicular Environments (WAVE) — Certificate Management Interfaces for End Entities. Technical specification, IEEE, 2020.

[18] Aleksandr Ometov and Sergey Bezzateev. Multi-Factor Authentication: A Survey and Challenges in V2X Applications. In *2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 129–136. IEEE, 2017.

[19] Risto Oorni and Ana Goulart. In-Vehicle Emergency Call Services: eCall and Beyond. *IEEE Communications Magazine*, 55(1):159–165, 2017.

[20] SAE. J2735: Dedicated Short Range Communications (DSRC) Message Set Dictionary. Standard SAE J2735:2009, SAE International, 2009.

[21] Oliver Schmidt. An ETSI Look at the State of the Art of Pseudonym Schemes in Vehicle-to-Everything (V2X) Communication, [ONLINE] https://git.orlives.de/schmittlauch/hs-pseudonym-schemes-in-v2x/src/branch/master/main.pdf. *TU Dresden*, 2018.

[22] Syed Wajid Ali Shah, Jongkil Jay Jeong, and Robin Doss. How Hackers Can Use Message Mirroring Apps to See All Your SMS Texts — and Bypass 2FA Security. `https://theconversation.com/how-hackers-can-use-message-mirroring-apps-to-see-all-your-sms-texts-and-bypass-2fa-security-165817`.

[23] IEEE Vehicular Technology Society. Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Services. Technical specification, Institute of Electrical and Electronics Engineers, Piscataway, NJ, United States, 03 2016.

[24] Eric Verheul, Christopher Hicks, and Flavio D Garcia. IFAL: Issue First Activate Later Certificates for V2X. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 279–293. IEEE, 2019.

[25] Wikipedia.org. States of Germany. `https://en.wikipedia.org/wiki/States_of_Germany`.

[26] Chris Wood. AES-GCM-SIV, [ONLINE] https://github.com/chris-wood/aes-gcm-siv. `https://github.com/chris-wood/aes-gcm-siv`.

[27] Yingying Yao, Xiaolin Chang, Jianhua Wang, Jelena Mišić, Vojislav B Mišić, and Hong Wang. LPC: A Lightweight Pseudonym Changing Scheme with Robust Forward and Backward Secrecy for V2X. *Ad Hoc Networks*, 123:102695, 2021.

Publication

Post-Quantum Impacts on V2X Certificates – Already at The End of The Road

Publication Data

Yoshizawa, T., and Preneel, B., Post-Quantum Impacts on V2X Certificates - Already at The End of The Road. In 2023 IEEE Vehicular Technology Conference (VTC), IEEE, pp. 1–6, 2023.

Contributions

- Principal author.

Post-Quantum Impacts on V2X Certificates – Already at The End of The Road

Takahito Yoshizawa and Bart Preneel

KU Leuven, ESAT/COSIC, Leuven, Belgium

Abstract. The current certificate definition for vehicle-to-everything (V2X) communication does not support forward compatibility as it does not take migration toward Post Quantum Cryptography (PQC) into account. As a result, introducing PQC-compatible certificates in V2X can result in similar to Distributed Denial-of-Service (DDoS) attack to both legacy and PQC-ready vehicles. This situation will make the deployment of PQC certificates a stalemate situation. In addition, due to the larger public key and signature sizes in PQC algorithms, V2X message size will significantly increase, causing the channel capacity and effective transmission range to decrease. This situation will negatively impact the operation of V2X communication. In this sense, any unnecessary channel usages need to be avoided. We propose to revise the certificate definitions in IEEE 1609 and ETSI Intelligent Transport System (ITS) standards to address and mitigate these issues and pave the way for the migration toward PQC algorithm.

1 Introduction

Vehicular communication is intended to improve road safety by reducing accidents [8]. This is achieved by vehicles sharing their information with one another to establish and maintain situational awareness of their surroundings, and disseminate warning situations when needed so that receiving vehicles can assess the situation and take necessary action.

Vehicles protect the message integrity using digital certificates and digital signatures. Transmitting vehicles generate a message, calculate a message signature for it, and attach a certificate upon transmission. Using this information, receiving vehicles verify the transmitting vehicle's authenticity and message integrity by verifying the certificate chain and the received signature using the public key in the certificate. In this sense, the generation and

distribution of certificates in the PKI system is an essential part of the security mechanism in the V2X communication.

In recent years, advancing capabilities of quantum computers pose significant threats to the security of computer systems. Specifically, public-key-based algorithms are vulnerable to quantum computers [7]. This situation led governments, industries, and academia to research and investigate alternative algorithms that can withstand against the threats and attacks using quantum computers [3].

To address the continuing evolution of quantum computers and their threats, migration to PQC algorithms will occur in the future, although its capability to run Shor's algorithm is expected to be still 25 to 30 years away [10]. To stay ahead of this situation, the National Institute of Standards and Technology (NIST) recommends migrating to post-quantum algorithms by 2030 [20].

We have examined the existing V2X standards from the perspective of migrating to PQC algorithms, and identified issues in the existing certificate definitions. We believe these issues are significant to the extent that its migration itself will cause major disruption to the normal operation of both legacy and new PQC-ready vehicles. In this sense, we propose that IEEE 1609 and ETSI ITS address the necessary changes to support forward compatibility in these standards immediately. In addition, we propose to reduce any unnecessary use of communication channel from these standards to minimize the impact of increasing channel use due to large certificates.

The rest of this paper is organized as follows. We describe the background and issues in the existing standards in Sec. 2, propose the solution to address these issues in Sec. 3, and give proposals in Sec. 4. In Sec. 5, we discuss related work, followed by a conclusion in Sec. 6.

2 Background

2.1 Certificate Definition in V2X Standards

The IEEE 1609.2 standard for the US [28] and the ETSI TS 103.097 [17] for Europe define certificate formats used in V2X communication. The former was standardized first in 2006, leading the latter to adopt and modify it as a European standard in 2013. Instead of reusing an existing certificate format such as X.509 [22], IEEE 1609.2 defined a custom-tailored certificate format. Certificates from these standards [28, 17] are used by entities in the V2X certificate management system including Root Certificate Authority (RCA)

and Intermediate CAs (ICA) to secure the communication among them, as well as end-entities such as vehicles and Road Side Units (RSUs). Certificates used by end entities such as vehicles are called *pseudonym certificates* due to the intended purpose of being anonymous in order to protect vehicle owners' privacy. For message integrity protection purposes, these standards require to use Elliptic Curve Digital Signature Algorithm (ECDSA) to generate digital signatures. In ECDSA, the public key (PK) and the signature length are 32 and 64 bytes, respectively.

2.2 Emergence of PQC Algorithms

Since 2012, standardization work has been in progress, organized by the NIST, to select PQC algorithms that are resistant to attacks using post-quantum computers. This competition includes both Key-Encapsulation Mechanisms (KEM) and signature algorithms. In June 2022, the third round evaluation result was finalized and published [1]. Signature algorithms selected for the fourth round include: CRYSTALS-Dilithium [12], Falcon [13], and SPHINCS+ [11]. The first two are lattice-based and the last one is a hash-based scheme.

One notable characteristic of these PQC algorithms is that their PK and signature are longer than conventional signature algorithms such as ECDSA. Their exact sizes vary from one algorithm to another. In an extreme case, PK size reaches close to 2 Mbytes in the Rainbow-V signature algorithm.[1] From V2X communication's perspective, this implies that a PQC certificate and its corresponding digital signature will make messages significantly longer than the ones using conventional ECDSA. This incurs additional processing burden and certificate storage in the vehicle On-Board Unit (OBU). Furthermore, this will incur a higher load on the communication channel. This is a concern from the perspective of real-time systems such as V2X communication in which messages among moving vehicles need to be processed in the order of milliseconds to avoid accidents and improve road safety.

2.3 Migration to PQC Algorithm

There will be a transition period in which a new PQC signature algorithm is introduced and disseminated. As different types of vehicles made by multiple vehicle manufacturers coexist on the road, V2X communication will be a mixture of both *legacy* vehicles (ECDSA-based PKs and signatures) and the new *PQC-capable* vehicles (PQC-based PKs and signatures) during this transition period.

[1] Rainbow was not selected to the fourth round in the NIST competition [1], but we mention it for comparison purpose.

As introducing new technologies can take a long time, especially when durable goods such as automobiles are involved, this transition period can last years. In fact, as vehicles are driven for as long as 23 years [23], this migration needs to occur seamlessly. This implies that new *PQC-capable* vehicles need to be backward compatible as well as *legacy* vehicles need to be forward-compatible. Doing so will ensure that migration from the legacy to a new PQC algorithm over a long period does not impact the overall functionalities of V2X communication. As discussed in Sec. 1, NIST recommends that mitigation against quantum attacks should be in place by 2030 [20]. This implies V2X PKI systems must also migrate to the PQC algorithm according to this time frame.

3 Discussion

A close examination of the existing standards for V2X communication [28, 17] indicates that this intended smooth migration we discussed in Sec. 2.3 will not occur. On the contrary, introduction of a new PQC algorithm likely create significant disruptions to both *legacy* and new *PQC-capable* vehicles equally. The observable symptom is equivalent to a variation of DDoS attacks.

3.1 Absence of Forward Compatibility

The most prominent issue in the existing certificate format is the absence of *forward compatibility*. Forward compatibility means that legacy implementations accept and process certificates used by newer implementations. This is ensured by the use of an optional *extension* field. In fact, X.509 certificate definition [22] includes an extension field. This field allows newer version certificate to include additional data as *non-critical* information. As a comparison, the existing certificate definition in IEEE 1609.2 [28] is shown in Fig. 1.[2] It is also used as a baseline of ETSI ITS certificate definition [17].

In the context of PQC migration, a PK and an issuing CA's signature using the new PQC algorithm can be carried in this field. Legacy implementations that do not understand any *non-critical* extension ignore it, while accepting and using legacy content. This enables an introduction of *hybrid* certificates, as shown in Fig. 2.(a), which contains a PK and an issuing CA's signature of both legacy ECDSA (PK_E, $CASig_E$) and PQC algorithms (PK_P, $CASig_P$). The resulting message format of Cooperative Awareness Message (CAM) [15] or Basic Safety Message (BSM) [26] is shown in Fig. 2.(b). This message contains signatures of both ECDSA ($MsgSig_E$) and PQC ($MsgSig_P$), implying that the message format

[2] Only the essential part of the ASN.1 definition is shown.

```
Certificate ::= CertificateBase (ImplicitCertificate |
                                 ExplicitCertificate)
SequenceOfCertificate ::= SEQUENCE OF Certificate

CertificateBase ::=
      SEQUENCE  { version                 Uint8(3),
                  type                    CertificateType,
                  issuer                  IssuerIdentifier,
                  toBeSigned              ToBeSignedCertificate,
                  signature               Signature OPTIONAL
                }


ToBeSignedCertificate ::= SEQUENCE  {
  id                      CertificateId,
  cracaId                 HashedId3,
  crlSeries               CrlSeries,
  validityPeriod          ValidityPeriod,
  region                  GeographicRegion OPTIONAL,
  assuranceLevel          SubjectAssurance OPTIONAL,
  appPermissions          SequenceOfPsidSsp OPTIONAL,
  certIssuePermissions    SequenceOfPsidGroupPermissions OPTIONAL,
  certRequestPermissions SequenceOfPsidGroupPermissions OPTIONAL,
  canRequestRollover      NULL OPTIONAL,
  encryptionKey           PublicEncryptionKey OPTIONAL,
  verifyKeyIndicator      VerificationKeyIndicator,
  ...
}
(WITH COMPONENTS { ..., appPermissions PRESENT} |
 WITH COMPONENTS { ..., certIssuePermissions PRESENT} |
 WITH COMPONENTS { ..., certRequestPermissions PRESENT})
```

Figure 1: Certificate Definition in IEEE 1609.2

is also extended to carry the second signature. This type of *hybrid certificate* based on X.509 to address migration toward PQC algorithm has already been tested and verified to work for TLS, OCSP and other protocols [18, 27].

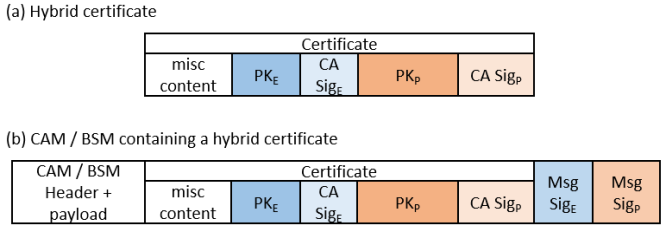


Figure 2: Hybrid Certificate and a Message That Contains It

3.2 Impacts on Pseudonym Certificates

In this section, we examine the impacts of the absence of an optional *extension* field in V2X certificates [28, 17] from the perspective of direct communication

among vehicles using pseudonym certificates. It has two implications.

First, *legacy* vehicles will consider that *hybrid* certificates do not conform to the standardized format, and thus reject them. Moreover, these *legacy* vehicles most likely consider new *PQC-capable* vehicles as misbehaving due to constantly sending *malformed* certificates and messages. A plausible reaction by these vehicles is to report these *PQC-capable* vehicles to the Misbehaviour Authority (MA) for investigation. This means that the MA also needs to be able to treat these alleged *misbehaviour* reports as invalid and ignore such reports rather than accepting them. A possible outcome of erroneously judging as misbehaviour can result in the MA to revoke all certificates of all *PQC-capable* vehicles soon after they start using this new certificate type. In this case, these *PQC-capable* vehicles can no longer transmit V2X messages, resulting in a type of DDoS attack situation.

One possible approach is for *PQC-capable* vehicles to duplicate every message, one using the legacy ECDSA and another using the PQC algorithm to generate signatures. However, it does not solve the problem as *legacy* vehicles still consider messages containing PQC-compatible certificates as malformed, thus may consider these transmitting vehicles as misbehaving. In addition, this approach requires the PKI system to issue two sets of pseudonym certificates to every *PQC-capable* vehicle. It further implies that communication channel usage will grow even faster. Therefore, it is clearly a sub-optimal and unscalable solution.

Second, because *hybrid* certificates are significantly larger in size, their usage will decrease the effective communication channel capacity. As the number of *PQC-capable* vehicles increases on the road, the proportions of these *PQC-compatible* messages increase in the communication channel, and the rate of increase in the channel usage is significantly higher than legacy messages due to their larger message size. Consequently, the communication channel will saturate quicker, the number of legacy messages that can access the channel will decrease, resulting in a type of DDoS attack situation from *legacy* vehicles' perspective. Table 1 lists the PK and signature size of three PQC signature algorithms and their resulting CAM message sizes [15] using *hybrid* certificates discussed in Sec. 3.1. The use of *hybrid* certificates will reduce the number of vehicles that can occupy the communication channel, effectively reducing the transmission range of V2X communication. The amount of reduction in the channel capacity is directly proportional to the PK and signature size increase in each PQC algorithm.

As a simple comparison, if we consider the increase in CAM message size directly translates to the channel usage, then PHINCS+128f has the worst case where the message size increase by a factor of 95 times compared to the legacy

ECDSA. The least impacting case is Falcon-512 with a factor of 7 times. From the perspective of communication channel capacity, Figure 3 illustrates the relationship between the proportion of certificate types (i.e. % of *PQC-capable* vehicles vs. *legacy* vehicles) and its impact on the channel capacity (i.e. the maximum number of vehicles before the channel is saturated) for various PQC signature algorithms.[3] This figure shows that the channel capacity decreases rapidly even when a relatively small proportion (∼10%) of *legacy* vehicles are replaced by *PQC-capable* vehicles. For example, even the least impacting algorithm (Falcon-512) will reduce the channel capacity to half when 30% of vehicles become PQC-capable. In effect, the transmission range will decrease by approximately 30% assuming the vehicle density is the same.

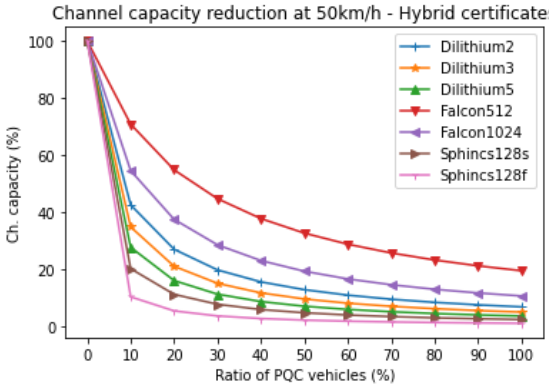


Figure 3: Channel Capacity Reduction (Hybrid Certificates)

[3]We calculated vehicle speed of 50, 70, 90, and 110 km/h each. However, we only show the 50 km/h case as an example as the results are similar.

Table 1: Certificate and Message Size for The Legacy and PQC Algorithms

Algorithm	Security Level	|PK| (byte)	|Sig| (byte)	|Cert| (byte)	|Hybrid cert| (byte)	|CAM_f| (byte)	Ratio_f	|CAM_d| (byte)	Ratio_d
ECDSA	n/a	32	64	150	n/a	364	x1.00	222	x1.00
Dilithium2	2	1,312	2,420	3,786	3,882	6,516	x17.90	2,842	x12.80
Dilithium3	3	1,952	3,293	5,299	5,395	8,902	x24.46	3,795	x17.09
Dilithium5	5	2,592	4,594	7,240	7,336	12,144	x33.36	5,200	x23.42
Falcon-512	1	897	666	1,617	1,713	2,593	x7.12	972	x4.38
Falcon-1024	5	1,793	1,280	3,127	3,223	4,717	x12.96	1,666	x7.50
SPHINCS+128s	1	32	7,856	7,942	8,038	16,108	x44.25	8,499	x38.28
SPHINCS+128f	1	32	17,088	17,174	17,270	34,572	x94.98	18,224	x82.09

Note: CAM_f: CAM message with full certificate, CAM_d: CAM message with certificate digest.
Ratio_f: message length increase compared to ECDSA-based full certificate.
Ratio_d: message length increase compared to ECDSA-based certificate digest.

3.3 Mitigating Ineffective Channel Usage

Another approach to mitigate the increasing communication channel usage is to re-evaluate the existing mechanisms in the standards and eliminate functionalities that ineffectively uses the communication channel. One example is the resolution of unknown certificate digests, called Peer-to-Peer Certificate Distribution (P2PCD). The current standards [28, 17] specify that CAM and BSM messages are sent up to 10 times/sec. However, only one message in every second contains a full certificate, leaving the remaining messages to contain a certificate *digest*. A certificate *digest* is a compact representation of a certificate by taking the least significant 8 bytes of the hash output of the certificate (i.e. *digest* $\leftarrow$ *LSB8(Hash(cert))*). The use of this *digest* effectively reduces the overall message size. On the other hand, its use implies that receiving vehicles may need to resolve a *digest* if this vehicle does not have the corresponding certificate. Such situation occurs when the first CAM or BSM message from a vehicle contains a *digest*. In this situation, P2PCD mechanism dynamically resolves the unknown certificate by querying vehicles within the communication range to send the missing certificate for a *digest*.

Despite its usefulness, its effectiveness is limited in certain scenarios, resulting in an ineffective use of communication channel. An analysis in [29] shows that a large majority ($\sim$89%) of pseudonym certificate digest resolution events of received CAM messages occur for vehicles moving in the opposite direction in highway scenarios. The use of P2PCD mechanism to dynamically resolve unknown digests in this scenario is not beneficial due to the short lifetime vehicles stay in each other's communication range. In such situation, it makes sense to withhold P2PCD mechanism by being aware of the relative vehicle movement, e.g. vehicle's direction and speed, and determine if its usage is effective or not. Such decision helps mitigate the communication channel usage when its load is already high.

3.4 Impacts on RCA and ICA Certificates

We now shift our attention to the communication among CAs in the PKI system due to the absence of compatibility in *legacy* and *PQC-capable* certificates. Similar migration issue exists in the PKI system entities. RCAs, ICAs, and vehicles use certificates to verify their authenticity and deliver a public key to encrypt messages between them. ICAs include entities such as Enrolment Authority (EA), Authorization Authority (AA), and Misbehaviour Authority (MA) in ETSI architecture [14]. Without forward compatibility in the legacy certificates, migration toward PQC requires significantly tighter coordination among them. Because legacy entities do not recognize or accept *hybrid*

certificates, all RCAs and ICAs need to be upgraded at the same time to a new implementation that can process them. In addition, all RCAs and ICAs first need to be upgraded so that pseudonym certificates to vehicles using the PQC algorithm can be generated and distributed to vehicles. In a large system where there are number of RCAs and ICAs exist, it becomes a significant challenge from the system administration perspective.

4 Proposals

Based on the discussion in the previous sections, we propose that IEEE 1609 and ETSI C-ITS working groups to take the following actions.[4]

1. Revise IEEE 1609.2 [28] and ETSI TS 103 097 [17] by including a *non-critical extension* in the certificate definition. We believe this change requires an urgent attention so that legacy vehicle implementations will not reject future PQC-ready pseudonym certificates and report them as a misbehaviour. In addition, introduce a new clause in [28] and [17] to discuss a future need to extend the existing certificate definition by adding a PQC public key and issuing CA's signature.[5]

2. Revise BSM (SAE J2735 [26]), CAM (ETSI TS 302 637-2 [15]) and DENM (TS 302 637-3 [16]) specifications by introducing an extension field to their respective message formats for future extensibility, such as the inclusion of a message signature using a PQC algorithm.

3. Revise [28] and [17] by recommending not to use P2PCD and inlineP2PCD mechanisms when the usage level of communication channel is high. Such provision covers multiple situations: (1) reduce unnecessary overhead in the channel even in the legacy vehicles, and (2) migitate impacts when migration to PQC algorithm occurs by eliminating less effective channel usage.

4. Investigate the usability of NIST competition round 4 candidates [1] from the real-time cyber-physical systems' perspective, such as V2X communication, specifically focusing on the impact of communication channel usage and OBU message processing, and define a path toward PQC migration.

[4]Some of these activities, such as investigating and evaluating solutions, may be conducted by other industry groups such as C2C-CC [6].

[5]Given that the NIST competition is still in progress, it is prudent to leave specifications of this new public key size unspecified in these standards.

5. When the NIST competition is finalized and the PQC algorithms are selected, make further updates to the relevant specifications such as [28] and [17] by reflecting the result of the investigation mentioned above.

5 Related Work

There are several literature on hybrid certificates in the context of migration toward PQC. Alnahawi et al. [2] present comprehensive coverage of PQC and their issues such as downgrade attack. Fan et al. [18] discuss their experiment of hybrid certificates on protocols such as TLS1.2, OCSP, CMP, and EST, and showed that most of the protocols and libraries worked with hybrid certificates using X.509 certificate with post-quantum extensions. Yunakovsky et al. [30] recommend using hybrid cryptographic schemes using current and post-quantum solutions for PKI against attacks using quantum computers. They also emphasize the importance of the concept of crypto-agility.

From the perspective of PQC impacts on V2X communication, Bindel and McCarthy [4] explain that they failed to construct implicit certificates from lattice-based algorithms (Dilithium and Falcon). Oliveira [24] also reached the same conclusion in his PhD thesis. This situation is significant given that explicit certificates will be the only choice with PQC algorithms. Bindel et al. [5] discuss an approach to split a certificate into multiple frames due to its larger PK size in PQC algorithm. This approach introduces a new vulnerability where a potential loss of any fragmented frame will render transmission of the large certificate void. In this sense, further improvement of this idea is needed. Dharminder et al. [9] proposes a new approach to introduce edge computing into V2X message verification by offloading this task to RSUs rather than receiving vehicles to do it themselves. This idea necessarily creates a dependency on the presence and availability of RSUs for vehicles' normal operation, thus limiting its practicality.

From the perspective of the hardware implementation of PQC algorithm, Ravi et al. [25] implemented Kyber for KEM and Dilithium for signature algorithm on an automotive-grade platform. They conclude that, compared to the existing cipher suites, the performance reduces by half when post-quantum cipher suites are used due to the communication channel as the bottleneck. Fritzmann et al. [19] also implemented PQ algorithms on a vehicle platform and recommended that a specific HW product to be used as a PQC implementation due to its higher performance with an optimization. Gonzalez et al. [21] implemented NIST round-3 candicate algorithms on a hardware platform with 8 KB of

RAM. Their work shows an interesting insight into the level of constraints PQC algorithms pose on limited hardware resources.

All of the work mentioned above does not address the certificate format and compatibility issue in the IEEE 1609.2 and ETSI C-ITS standards. We consider our paper is the first to identify this issue and proposed changes in these standards.

6 Conclusion and Future Work

We have identified an issue in the existing certificate definition in V2X communication standards. Future migration to PQC algorithm will not be possible unless this issue is resolved in the standards. Otherwise, the introduction of PQC algorithm will create significant disruption in which both legacy and new PQC-capable vehicles potentially face unintentional DDoS attack situation. This is a *lose-lose situation* we need to avoid. We propose IEEE 1609 and ETSI ITS standards to update the relevant specifications. Specifically, the *non-critical extension* should be introduced to the certificate definition at the earliest opportunity so that legacy vehicles will not erroneously report the use of PQC-capable pseudonym certificates as a misbehaviour. Further, implication of incompatible certificates among the CAs will cause operational issues when PQC algorithm is introduced in the V2X PKI system.

Longer public key and signature in PQC signature algorithm will significantly reduce the channel capacity and hinder performance of the real-time cyber-physical systems (CPS) such as V2X communication. In this sense, mitigation approaches of the use of PQC algorithms in real-time CPS are an important open research question.

Acknowledgments

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203 and by the Research Council KU Leuven C1 project on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058.

References

[1] Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, and Daniel Smith-Tone. NIST IR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. *US Department of Commerce, NIST*, 2022.

[2] Nouri Alnahawi, Alexander Wiesmaier, Tobias Grasmeyer, Julian Geißler, Alexander Zeier, Pia Bauspieß, and Andreas Heinemann. On the State of Post-Quantum Cryptography Migration. *INFORMATIK 2021*, 2021.

[3] Daniel J Bernstein and Tanja Lange. Post-Quantum Cryptography. *Nature*, 549(7671):188–194, 2017.

[4] Nina Bindel and Sarah McCarthy. The Need for Being Explicit When Communicating. *ninabindel.de*, 2021.

[5] Nina Bindel, Sarah McCarthy, Geoff Twardokus, and Hanif Rahbari. Drive (Quantum) Safe!–Towards Post-Quantum Security for V2V Communications. *Cryptology ePrint Archive*, 2022.

[6] C2C-CC. TR2052, Survey on ITS-G5 CAM Statistics. Technical report, Car 2 Car Communication Consortium, 12 2018.

[7] L Chen, S Jordan, Y Liu, D Moody, R Peralta, R Perlner, and D Smith-Ton. NIST IR 8105, Report on Post-Quantum Cryptography. NIST (2016). *US Department of Commerce, NIST*, 2016.

[8] European Commission. COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the Document, Commission Delegated Regulation, Supplementing Directive 2010/40/EU of the European Parliament and of the Council with Regard to the Deployment and Operational Use of Cooperative Intelligent Transport Systems. Technical report, European Commission, 2019.

[9] Dharminder Dharminder, Saru Kumari, and Uddeshaya Kumar. Post Quantum Secure Conditional Privacy Preserving Authentication for Edge Based Vehicular Communication. *Transactions on Emerging Telecommunications Technologies*, 32(11):e4346, 2021.

[10] Ericsson. Ensuring Security in Mobile Networks Post-Quantum. *Ericsson Technology Review*, 12, 2021.

[11] Jean-Philippe Aumasson et al. SPHINCS+. `https://sphincs.org/`.

[12] Peter Schwabe et al. Crystals Dilithium. `https://pq-crystals.org/dilithium/`.

[13] Thomas Pornin et al. Falcon. `https://falcon-sign.info/`.

[14] ETSI. TS 102 940: Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management; V2.1.1. Standard, European Telecommunications Standards Institute, 07 2018.

[15] ETSI. EN 302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, V1.4.1. Standard, European Telecommunications Standards Institute, 04 2019.

[16] ETSI. EN 302 637-3: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service; V1.3.1. Standard, European Telecommunications Standards Institute, 04 2019.

[17] ETSI. TS 103 097: Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats; Release 2; V2.1.1. Standard, European Telecommunications Standards Institute, 10 2021.

[18] Jinnan Fan, Fabian Willems, Jafar Zahed, John Gray, Serge Mister, Mike Ounsworth, and Carlisle Adams. Impact of Post-Quantum Hybrid Certificates on PKI, Common Libraries, and Protocols. *International Journal of Security and Networks*, 16(3):200–211, 2021.

[19] Tim Fritzmann, Jonas Vith, and Johanna Sepúlveda. *Post-Quantum Key Exchange Mechanism for Safety Critical Systems*. Ruhr-Universität Bochum, 2019.

[20] Michael Gardiner, Alexander Truskovsky, George Neville-Neil, and Atefeh Mashatan. Quantum-Safe Trust for Vehicles: The Race is Already On. *Communications of the ACM*, 64(9):54–61, 2021.

[21] Ruben Gonzalez, Andreas Hülsing, Matthias J Kannwischer, Juliane Krämer, Tanja Lange, Marc Stöttinger, Elisabeth Waitz, Thom Wiggers, and Bo-Yin Yang. Verifying Post-Quantum Signatures in 8 KB of RAM. In *Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings 12*, pages 215–233. Springer, 2021.

[22] ITU-T. Recommendation ITU-T X.509, Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks. Standard, International Telecommunication Union - Telecommunication, 2019.

[23] Masahiro Oguchi and Masaaki Fuse. Regional and Longitudinal Estimation of Product Lifespan Distribution: A Case Study for Automobiles and A Simplified Estimation Method. *Environmental Science & Technology*, 49(3):1738–1743, 2015.

[24] Jefferson Evandi Ricardini Fernandes de Oliveira. *qSCMS: Post-Quantum Security Credential Management System for Vehicular Communications.* PhD thesis, Universidade de São Paulo, 2019.

[25] Prasanna Ravi, Vijaya Kumar Sundar, Anupam Chattopadhyay, Shivam Bhasin, and Arvind Easwaran. Authentication Protocol for Secure Automotive Systems: Benchmarking Post-Quantum Cryptography. In *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–5. IEEE, 2020.

[26] SAE. J2735: V2X Communications Message Set Dictionary. Standard SAE J2735:2022, SAE International, 2022.

[27] Dimitrios Sikeridis, Panos Kampanakis, and Michael Devetsikiotis. Post-Quantum Authentication in TLS 1.3: a Performance Study. *Cryptology ePrint Archive*, 2020.

[28] IEEE Vehicular Technology Society. Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Services. Technical specification, Institute of Electrical and Electronics Engineers, Piscataway, NJ, United States, 03 2016.

[29] Takahito Yoshizawa and Bart Preneel. On Handling of Certificate Digest in V2X Communication. In *2022 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 160–165. IEEE, 2022.

[30] Sergey E Yunakovsky, Maxim Kot, Nikolay Pozhar, Denis Nabokov, Mikhail Kudinov, Anton Guglya, Evgeniy O Kiktenko, Ekaterina Kolycheva, Alexander Borisov, and Aleksey K Fedorov. Towards Security Recommendations for Public-Key Infrastructures for Production Environments in the Post-Quantum Era. *EPJ Quantum Technology*, 8(1):14, 2021.

Curriculum

Takahito Yoshizawa obtained his BSc in Information and Computer Science degree from Georgia Institute of Technology in 1992, and MSc in Telecommunication from Southern Methodist University in 2002 while working full time. His career and education are highly convoluted due to what he considers as a repechage[6] of his earlier decision of not going to a university when he was a teenager. He has spent a number of years in mobile communication industry as an engineer and has done numerous types of engineering work associated with the life cycle of mobile infrastructure systems and products. He has worked for both large multi-national and small start up companies and has seen pros and cons of both sides. He also participated and contributed to standardization organizations and has multiple patents on communication systems. His has spent many years in the US and Europe, and has accumulated a rather large number of ex-colleagues, friends, and acquaintances, all scattered around in various parts of the world he can no longer keep track of. He considers his repechage journey comes to an end with the pending completion of PhD at KU Leuven. Despite this highly inefficient and convoluted trajectory of his education and professional career, he has no regret for it, although he does not recommend doing the same.

[6]Definition according to Merriam-Webster: a trial heat (as in rowing) in which first-round losers are given another chance to qualify for the semifinals.



FACULTY OF ENGINEERING SCIENCE
DEPARTMENT OF ELECTRICAL ENGINEERING
IMEC-COSIC
Kasteelpark Arenberg 10
B-3001 Leuven
takahito.yoshizawa@esat.kuleuven.be
https://www.esat.kuleuven.be/cosic