future internet

MDPI

Article

Enabling Vehicle-to-Vehicle Trust in Rural Areas: An Evaluation of a Pre-Signature Scheme for Infrastructure-Limited Environments

Dimah Almani [1,*], Tim Muller [1], Xavier Carpent [1], Takahito Yoshizawa [2] and Steven Furnell [1]

[1] Cyber Security Research Group, School of Computer Science, University of Nottingham, Nottingham NG8 1BB, UK; tim.muller@nottingham.ac.uk (T.M.); xavier.carpent@nottingham.ac.uk (X.C.); steven.furnell@nottingham.ac.uk (S.F.)
[2] COSIC, KU Leuven, 3001 Leuven, Belgium; takahito.yoshizawa@esat.kuleuven.be
* Correspondence: dimah.almani@nottingham.ac.uk

Abstract: This research investigates the deployment and effectiveness of the novel Pre-Signature scheme, developed to allow for up-to-date reputation being available in Vehicle-to-Vehicle (V2V) communications in rural landscapes, where the communications infrastructure is limited. We discuss how existing standards and specifications can be adjusted to incorporate the Pre-Signature scheme to disseminate reputation. Addressing the unique challenges posed by sparse or irregular Roadside Units (RSUs) coverage in these areas, the study investigates the implications of such environmental factors on the integrity and reliability of V2V communication networks. Using the widely used SUMO traffic simulation tool, we create and simulate real-world rural scenarios. We have conducted an in-depth performance evaluation of the Pre-Signature scheme under the typical infrastructural limitations encountered in rural scenarios. Our findings demonstrate the scheme's usefulness in scenarios with variable or constrained RSUs access. Furthermore, the relationships between the three variables, communication range, amount of RSUs, and degree of home-to-vehicle connectivity overnight, are studied, offering an exhaustive analysis of the determinants influencing V2V communication efficiency in rural contexts. The important findings are (1) that access to accurate Reputation Values increases with all three variables and (2) the necessity of Pre-Signatures decreases if the amount and range of RSUs increase to high numbers. Together, these findings imply that areas with a low degree of adoption of RSUs (typically rural areas) benefit the most from our approach.

Keywords: V2V; SCMS; RSUs; reputation; trust; cryptographic signatures; certificates; vehicular communication; SUMO; disconnected areas

Citation: Almani, D.; Muller, T.; Carpent, X.; Yoshizawa, T.; Furnell, S. Enabling Vehicle-to-Vehicle Trust in Rural Areas: An Evaluation of a Pre-Signature Scheme for Infrastructure-Limited Environments. *Future Internet* **2024**, *16*, 77. https://doi.org/10.3390/fi16030077

Received: 31 December 2023
Revised: 10 February 2024
Accepted: 15 February 2024
Published: 26 February 2024

1. Introduction

The Vehicular Ad hoc Networks (VANETs) has been instrumental in advancing intelligent transportation systems, notably through Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications, as shown in Figure 1. However, disconnected areas, often remote or rural, face a significant challenge due to the scarcity of Roadside Units (RSUs). This scarcity hampers robust vehicular communication, making direct V2V interactions for message authentication crucial [1]. Such conditions highlight the need for reliable communication methods to ensure trust between vehicles. Our research introduces the Pre-Signature scheme, tailored to enhance secure V2V communication in areas with limited RSUs support. This scheme is central to building trust between vehicles, ensuring safety and operational integrity in disconnected environments. It hinges on the exchange of Reputation Values among vehicles, establishing a decentralized trust mechanism in the absence of RSUs. Additionally, the scheme incorporates Pseudonym Certificates (PCs) and the Security Credential Management System (SCMS) for secure offline communication.

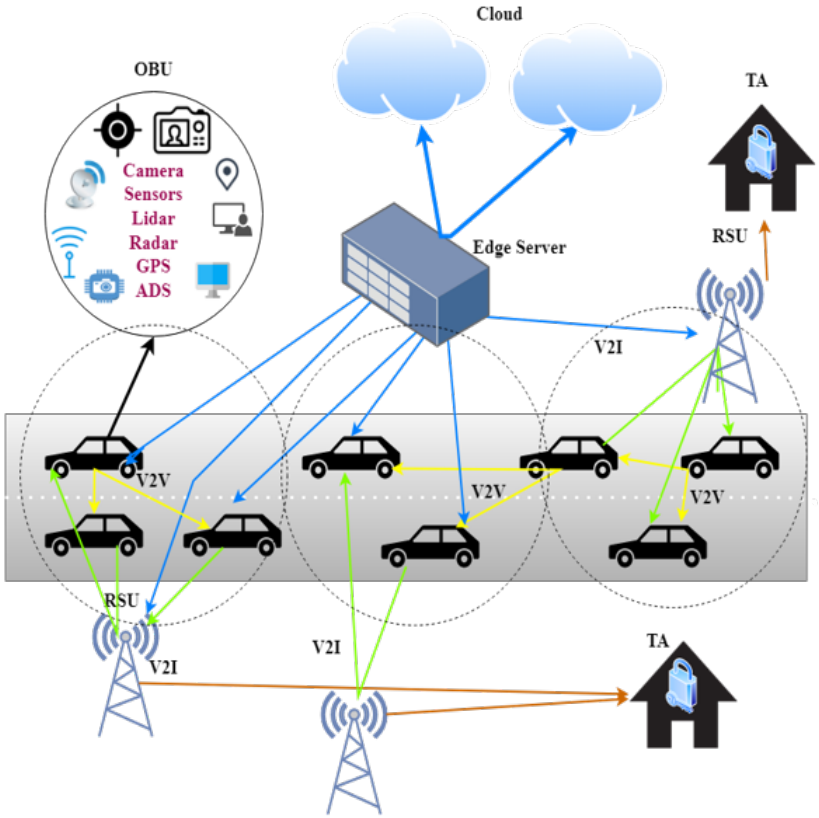

Figure 1. VANET Communications Infrastructure.

In SCMS, the Certification Revocation List (CRL) plays a key role in identifying and blocking misbehaving vehicles from the network. However, the synchronization of the CRL becomes imperative when vehicles gain access to the infrastructure, notably through *RSUs* [2,3]. A Pre-Signature scheme offers a more scalable and granular approach than CRLs by leveraging a reputation system. This system assesses vehicles based on their historical behavior, providing a more nuanced view of reliability and trustworthiness. Our focus is on effectively disseminating the Reputation Value (RV) for offline use while maintaining privacy. The goal is to develop a system to authenticate messages, which maintains privacy, works offline, and allows reputation to be used.

Referring to Figure 2, reputation+offline can be delivered by foregoing pseudonyms and providing medium-term (e.g., daily) Reputation Value certificates. Reputation+privacy can be delivered by requesting a short-term RV certificate every time a new Pseudonym Certificate is used. Finally, privacy + offline is delivered by systems like SCMS. The challenge is to deliver all three of these properties in a scalable way, with minimal changes to the standards. Our innovative solution involves a new cryptographic primitive—the Pre-Signature. This two-step process allows vehicles to verify Reputation Values offline, without compromising sender privacy. A significant contribution of this study is the employment of Simulation of Urban Mobility (SUMO) simulation on an aerial communication map of the Peak District, a National Park in central England.

It is worth noting that our work is based on the SCMS framework that relies on Dedicated Short-Range Communication (DSRC) rather than using the internet, e.g., via sattelite or GSM. The distinct advantages here are high-bandwidth and low-latency capabilities, even in challenging weather conditions, high-speed scenarios, or remote locations. The proposed scheme is based on real-world considerations regarding coverage. For example, in rural areas with limited connectivity or in disaster-hit regions where infrastructure is damaged, traditional methods of online verification are not feasible.

Through a detailed 24 h simulation, we analyze vehicle communication in rural areas under different conditions with limited RSUs connectivity. This simulation is pivotal in demonstrating the practical effectiveness and feasibility of the Pre-Signature scheme, showing its capacity to bolster trust and reliability in challenging and disconnected regions. The results play a pivotal role in demonstrating the scheme's ability to improve communication trust and reliability, providing significant insights into its practical application in real-world rural environments. Through this, our study not only contributes to the theoretical knowledge in the field but also offers practical solutions for improving V2V communications in challenging and disconnected areas.

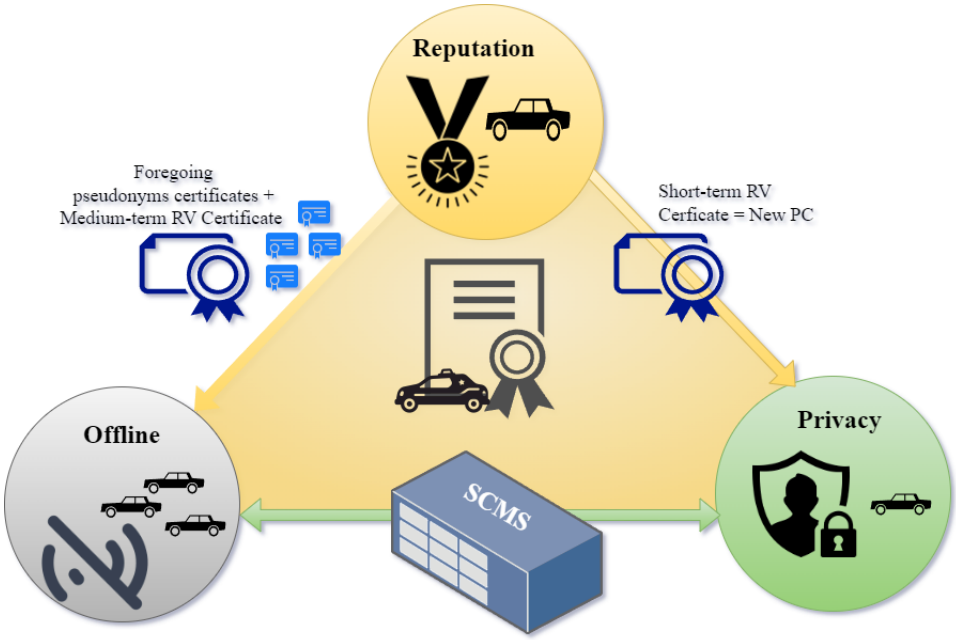

Figure 2. An Integrated Approach for Reputation, Offline Operation, and Privacy in V2V.

The paper begins with a review of related work in Section 2. Section 3 lays the groundwork for vehicular communications, followed by Section 4, which details a reputation-based system model. Section 5 presents the novel signature scheme, leading into Section 6, which introduces the simulation experiments showcasing the approach's effectiveness. Section 7 delves into the simulation discussion, exploring various aspects of the results related to the operational effectiveness of the Pre-Signature scheme. The paper culminates in Section 8 , summarizing the key findings and suggesting avenues for future research.

2. Related Works

Within this section, we discuss the limitations of relevant proposals from the existing literature from three perspectives in relation to our study.

2.1. Security Credential Management System for V2V Communications

In prior investigations, researchers delved into the Security Credential Management System SCMS, and, according to references [4,5], SCMS proves to be a promising solution for ensuring secure information exchange in V2V scenarios. Despite its objective to provide secure authentication, authorization, and data integrity for V2V communication, the challenges outlined in [6,7] persist and demand attention. Within the SCMS framework, vehicles are issued 20 certificates weekly to sign messages, with these certificates rotating every 5 min [8]. Consequently, a vehicle utilizes a fresh set of 20 certificates every 100 min, allowing SCMS to analyze all the certificates used by a vehicle in a day. While the SCMS system confirms the entity signing these certificates, verifying the accuracy or reliability of messages from the vehicle remains problematic.

The authors in [9] introduced a conditional privacy protection authentication scheme using short-term SCMS certificates. However, the process requires certificate exchange, posing a notable drawback. The authors in [10,11] also proposed SCMS certificate-based authentication protocols for V2V messaging, but their schemes necessitate infrastructure. The work by [12] devised an efficient V2V network scheme with an event trigger mechanism, incorporating PKI-based signatures for emergency message validation and identification of revoked certificates for malicious vehicles. However, addressing the revocation of certificates for malicious vehicles presents challenges. Distributing CRLs to all vehicles is time- and bandwidth-intensive. As the number of revoked vehicles increases, the efficiency of identification diminishes. Ensuring prompt and secure receipt of updated CRL copies poses challenges, especially in offline areas. Some scenarios necessitate solutions beyond relying solely on SCMS to identify misbehaving vehicles.

2.2. Disconnected Vehicular Network

Previous studies have extensively delved into the communication challenges within Disconnected VANETs. They focused on identifying reasons for disconnections, such as insufficient deployment of RSUs and the unpredictability of RSUs potentially failing. These investigations also examined the consequences of these disconnections, including message delays and inadequate message propagation. To tackle these issues, various advanced algorithms were proposed. It is critical to note, however, that none of these studies have specifically addressed the enhancement of communication reliability in the absence of RSUs. One notable study [13] concentrated on determining the mean length of clusters by exclusively relying on V2V communication. Additional research [14–17] investigated network connectivity using a generic radio channel model. Despite achieving full connectivity during high-vehicle-density periods, configurations with sparser vehicles led to inefficient message propagation, resulting in significant delays [18,19]. While specific investigations [20,21] scrutinize overall delay and frame the placement of RSUs as an integer linear programming problem, there is a significant void in the literature regarding the assessment of the speed at which alert messages propagate. This gap is particularly pronounced in scenarios where vehicles communicate directly with each other in the absence of RSUs.

2.3. Reputation in V2V Communications

The V2V reputation system is categorized into centralized and decentralized models. The centralized approach, pioneered by [3], revolves around a scheme that centrally distributes, updates, and stores vehicles' reputation scores. That study introduces a reputation announcement scheme for VANETs using Time Threshold to assess message reliability. The researchers in [22] recently proposed a centralized system for highways and urban roads, relying on a central Trusted Authority to calculate feedback scores from various vehicles and update the target's reputation. Moreover, Ref. [23] proposed an incentive provision method where the RSU updates the sender's reputation score based on observed actions validated by vehicles.

Conversely, distributed reputation systems operate without infrastructure dependence. In this model, vehicles autonomously collect, maintain, and update reputation scores in an ad hoc manner. The authors in [24] developed a node reputation system to evaluate the reliability of vehicles and their messages. They grouped vehicles with similar mobility patterns that are close to each other into platoons to minimize propagation overhead. The authors in [25] introduced a framework for self-organized vehicles that filters out malicious vehicles based on standard scores.

2.4. RSUs Deployment in Rural Areas

Roadside Units (RSUs) are pivotal in vehicular networks, enabling short-range wireless communications via IEEE 802.11p and a DSRC spectrum, essential for both data processing and internet connectivity [26]. These units are integral in managing traffic data and

facilitating connections with larger networks. RSUs further improve network performance through inter-unit communications. The deployment of RSUs is sophisticated, the NP-hard combinatorial optimization challenge [27] demands strategies like Voronoi diagrams [28] and Constrained Delaunay Triangulation for optimal placement [29]. Voronoi diagrams involves partitioning the map into regions based on distances to a specified set of points (potential RSU locations). Each point (RSU) would have a corresponding Voronoi cell such that any location within this cell is closer to that RSU than to any other RSU. It is useful for understanding and optimizing coverage. Constrained Delaunay Triangulation (CDT) is an extension of Delaunay Triangulation where some edges are constrained in the triangulation process. This is especially useful when there are natural barriers or roads that must be considered in the network layout. CDT can help to ensure that the network connectivity is maintained while considering these constraints.

In contrast to earlier studies, this paper delves into the effectiveness of utilizing a novel Pre-Signature scheme in disconnected areas, elucidating its role in enhancing the reliability of vehicular communication in rural settings without the constant need for RSUs. We offer a comprehensive comparative analysis with existing systems, focusing on both efficiency and the strategic deployment of RSUs. Through detailed simulations, our study clearly demonstrates the practical advantages and enhanced feasibility of this approach in real-world scenarios, distinguishing it from prior methodologies.

3. Vehicular Communications: Core Concepts and Challenges

This section highlights the critical role of Pseudonym Certificates PCs in the Security Credential Management System SCMS and delves into the intricacies of Dedicated Short-Range Communications DSRC. Additionally, it offers a concise overview of the challenges associated with rural areas and the sparse presence of Roadside Units RSUs, setting the stage for further exploration in subsequent sections.

3.1. SCMS: Pseudonym Certificates

Vehicular Public Key Infrastructure (V-PKI) networks are deployed globally for secure vehicle communication, with initiatives such as ETSI, C2C-CC, SCMS, and SCME leading the way [30–32]. Among these, SCMS stands out as a standardized solution for securing V2V communication. The system ensures trust among vehicles by exchanging anonymized data and utilizing Pseudonym Certificates PCs with short durations. Within the SCMS framework, the Pseudonym Certificate Authority (PCA) collaborates with the Misbehavior Authority (MA), Linkage Authorities (LA1 and LA2), and Registration Authority (RA) to identify linkage values for adding vehicle information in the Certificate Revocation List CRL in case misbehavior is detected [23].

In the implementation of SCMS in disconnected vehicular networks, two primary challenges arise as depicted in Figure 3. Firstly, maintaining and synchronizing the CRL is crucial for identifying the misbehaving vehicles. The CRL must be constantly updated and shared with all vehicles, a process that requires regular access to network infrastructure, typically via RSUs. This becomes problematic in areas with limited connectivity as the CRL grows with the number of misbehaving vehicles, necessitating frequent online updates. Secondly, SCMS demands the use of multiple PCs for each vehicle to ensure message integrity and privacy. These PCs require regular updates—as often as every five minutes—to prevent message linkability, posing a significant challenge in disconnected areas. Vehicles must either preload a long-term supply of PCs or obtain them on demand, which requires substantial storage capacity or consistent online access, respectively [31]. This dual challenge of managing the CRL and PCs effectively underscores the complexity of deploying SCMS in environments with limited network connectivity.

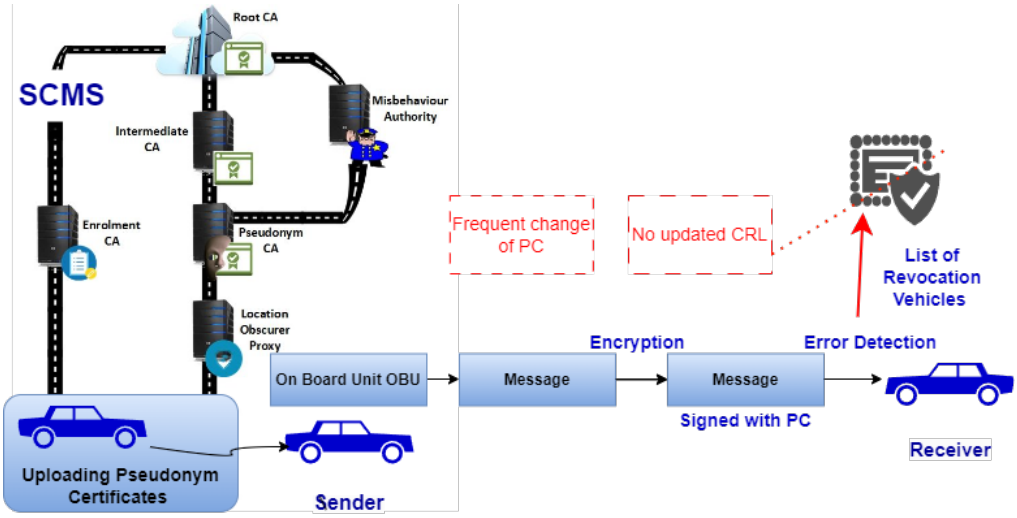

Figure 3. Challenges of SCMS in Disconnected Vehicular Network.

3.2. DSRC Communication

Dedicated Short-Range Communication (DSRC) serves as a wireless protocol specifically designed to facilitate high-speed communication over short distances, both between vehicles and between vehicles and infrastructure. Traditional cellular technologies like LTE and GSM are limited to the unique advantages of DSRC: high-bandwidth and low-latency capabilities, especially in difficult weather circumstances or high-speed situations. Unlike GSM or LTE, DSRC is the international Wireless Access in Vehicular Environments (WAVE) initiative standard. To illustrate, DSRC's protocol stack is designed to handle the rapid changes and high mobility in the system topology characteristics of vehicular networks. It operates in a dedicated spectrum—the 5.9 GHz band—explicitly allocated for vehicular communication. This allocation blocks interference from other wireless devices, ensuring uninterrupted and reliable communications needed for safety-critical applications.

The primary objective of DSRC is to enable the instantaneous exchange of critical information, with a particular focus on applications like collision avoidance and traffic management. Operating within a range of 300–900 m, DSRC allows vehicles to communicate effectively when in close proximity [33]. However, a notable challenge arises in offline conditions where the absence of nearby RSUs complicates or renders impossible the standard verification process for received messages. Despite this challenge, DSRC remains pivotal in advancing safety and efficiency within connected vehicle systems.

3.3. Disconnected Areas of Vehicular Networks

As the prevalence of connected vehicles continues to expand, there is a growing recognition of the essential role that infrastructure, particularly RSUs, plays in ensuring the reliability and trustworthiness of vehicular communication systems [34]. RSUs are pivotal in verifying message authenticity and confirming the eligibility of the sender, contributing significantly to the overall integrity of VANETs [35].

However, the communication landscape becomes markedly challenging in geographical areas characterized by tunnels, mountainous terrain, and remote locations. In such regions, satellite and GSM communications, although theoretically available, suffer from inconsistencies in availability and quality of service. In addition, the strategic deployment of RSUs becomes a critical and intricate challenge. The absence or inadequate deployment of RSUs in these disconnected areas poses a significant risk to the efficiency and reliability of VANETs. This, in turn, compromises the overall service capability for a substantial number of vehicles operating in these challenging environments.

This underscores the urgent need to address connectivity challenges in areas where RSU deployment is insufficient or suboptimal. Enhancing the robustness of VANETs

in disconnected or challenging terrains requires innovative solutions to overcome the limitations imposed by the sparse distribution of RSUs. Addressing these challenges is paramount to ensuring the trust and reliability of communication systems in diverse geographical settings, thereby maximizing the potential benefits of connected vehicles.

4. Proposed System Model

In response to the identified challenges in disconnected vehicular areas, this section introduces our proposed system mode. This innovative approach, Pre-Signature scheme, is designed to effectively manage trust and reputation in areas with limited or intermittent connectivity, thereby enhancing both security and operational efficiency. We introduce a new entity, the Reputation Server (RS), which provides the Reputation Values (RVs). The RS will be linked to the SCMS. During the reputation retrieval process, the RV will be pre-signed by the RS; then, the RV will be sent to the requested vehicle to complete the signature and attach it to PCs, as explained in Section 5.

IEEE 1609 and ETSI Intelligent Transport Systems (ITS) are two key standards that specify the vehicular communication. The former is for the US market and the latter is for the European market. Specifically from the security architecture perspective, IEEE 1609.2 [36] and ETSI TS 102 940 [37] define the V-PKI system architecture, procedures, and messages. These V-PKI architectures are the building blocks for the security solution of V2X communication. Figure 4 illustrates the extension of the ETSI ITS V-PKI architecture [37] by introducing the RS in this system. It should be noted that the incorporation of the RS into the process would necessitate updates to the related standards, namely IEEE 1609.2 [36] and the related ETSI specifications for system architecture (TS 102 940) [37] and protocol message formats and contents (TS 102 941) [38]. As shown in Figure 4, a new section should be created to capture the functional description of the RS.

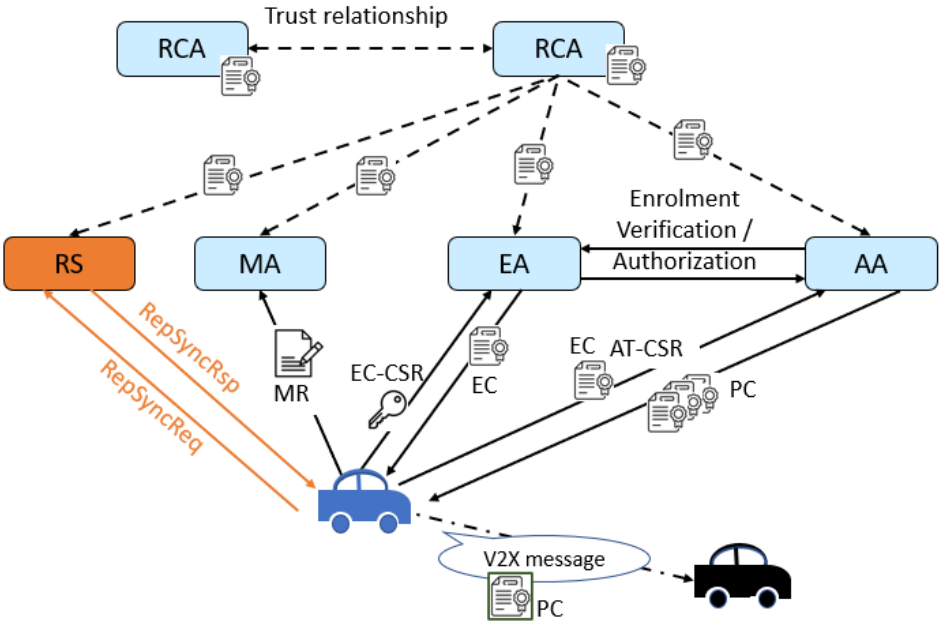

Figure 4. V-PKI Architecture with RS.

Figure 5 illustrates the procedure in which a vehicle retrieves its RV from the RS.

Steps 1 and 2: When vehicle V contacts an RSU, it requests a reputation synchronization by sending a *RV_Sync_Request* message with the RS. The vehicle first encrypts its V_{ID} using its private key V_{SK} to the RSU ($V'_{ID} \leftarrow enc(V_{ID}, V_{SK})$). The RSU then forwards the vehicle's request to the RS.

Step 3: Upon receiving this request from the vehicle, the RS extracts the V_{ID} by decrypting the received value using the corresponding public key ($V_{ID} \leftarrow dec(V'_{ID}, V_{PK})$).

Steps 4 to 6: Using the V_{ID} as a key, the RS retrieves the RV value for this vehicle and computes the timestamp ($TS \leftarrow CT - round(7log_2(RV_{VID}))$). The RS derives the Pre-Signature of this TS value (σ) and returns it to the vehicle in the *RV_Sync_Response* message.

Step 7: When the vehicle receives *RV_Sync_Response* message, it uses the Pre-Signature value (σ) to complete the signature ($\bar{\sigma}$).

Step 8: The vehicle transmits DENM message to vehicles within its communication range ($DENM(M, sig(M), PC, \bar{\sigma}, v)$). The signature in this DENM message is generated using the Elliptic Curve Digital Signature Algorithm (ECDSA) according to clause 5.2 and 7.1.2 in ETSI TS 103 097 [39].

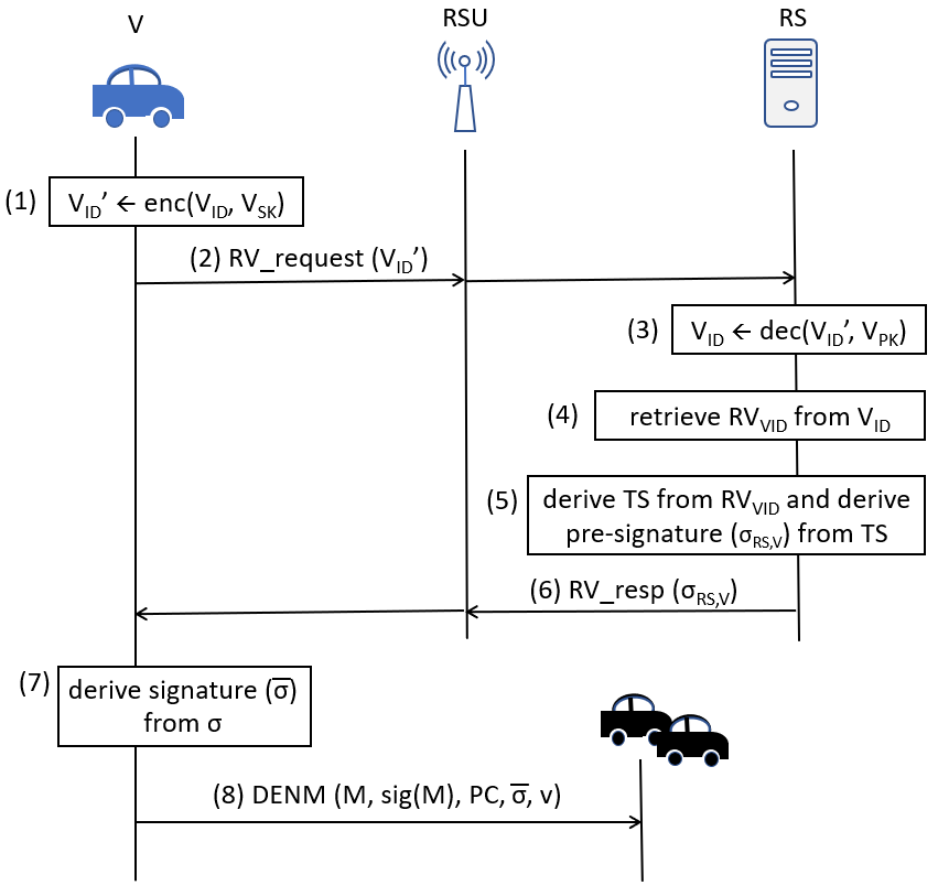

Figure 5. RV Retrieval.

Figure 6 illustrates the handling of Decentralized Environmental Notification Message (DENM) messages at the receiving vehicle when it receives the same message from multiple vehicles. This figure shows only two transmitting vehicles. However, in reality, it can be generalized to have n vehicles originating or relaying the same DENM message.

Step 1: Multiple vehicles ($V_{s1}, V_{s2}, ...$) transmit (either originate or relay) the same Decentralized Environmental Notification Message (DENM) message ($M_{Vs1}, M_{Vs1}, ...$). The generation of DENM message payload and its message signature are according to ETSI EN 302 637-2 [40] and ETSI TS 103 097 [39], respectively.

Step 2: The receiving vehicle (V_{rcv}) receives all messages from these vehicles. It verifies the message signature according to clause 5.2 and 7.1.2 in ETSI TS 103 097 [39] and verifies the TS signature ($\bar{\sigma}$) from each vehicle. Based on the verified TS signature, it determines whether to accept or reject the received message from each transmitting vehicle.

Step 3: If the vehicle accepts the received message in the previous step, the receiving vehicles forwards the message.

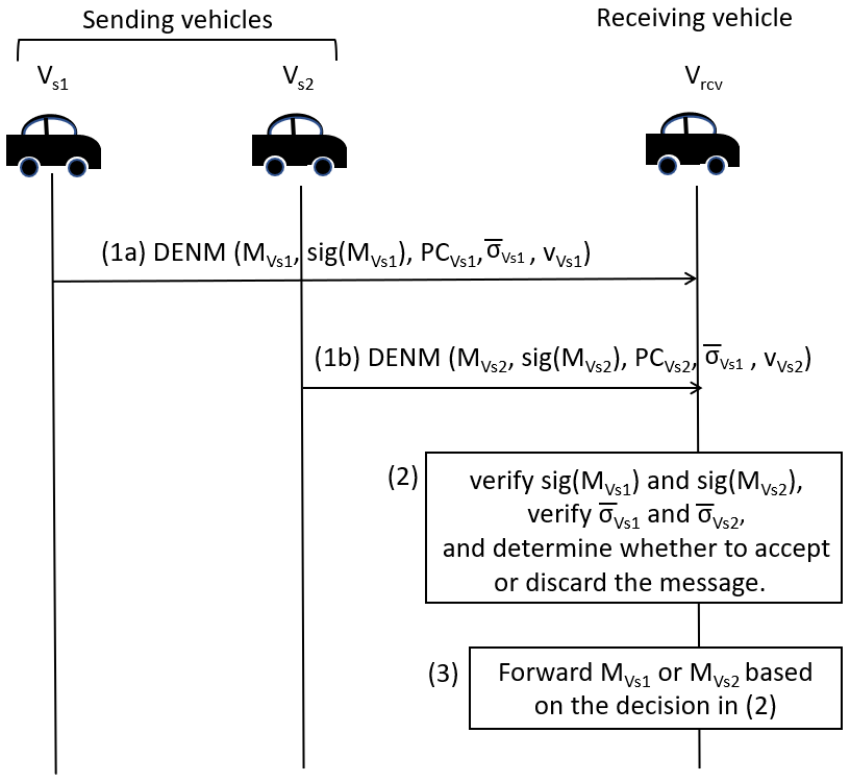

Figure 6. DENM Message Handling.

5. A Novel Signature Scheme

This section further develops and extends the concepts introduced in our previous work [41], providing a means for trustworthy V2V communications in offline contexts.

In SCMS, a vehicle's PCs allow other vehicles to be confident that the messages originate from that vehicle and have not been altered. Similarly, the RSU could supply vehicles with certificates with up-to-date reputation, but this creates a double challenge: (1) linking the reputation certificate to PCs without breaking pseudonymity; and (2) the reuse of the reputation certificate itself compromises privacy. An alternative approach would be that the RS regularly updates and signs the RV for each PC. However, this in turn poses a scalability issue as there are typically as many as 100,000 such PCs for each vehicle [42].

In this section, we introduce a unique two-step signature scheme that addresses this privacy/scalability compromise. Many variations in regular signature schemes exist, to name a few: ring signatures [43], group signatures [44], delegatable signatures [45], blind signatures [46], or proxy signatures [47]. Unfortunately, to the best of our knowledge, no existing variation addresses the specific challenge at hand. We thus introduce a new construction, the Pre-Signature scheme, which we succinctly describe below. Although motivated by the specific needs highlighted above, the scheme may be of independent interest and is introduced in a generic context.

A Pre-Signature scheme involves three parties: an Issuer I, a Prover P, and a Verifier V. The Issuer I is considered honest. The Prover P and the Verifier V may behave maliciously.

We assume familiarity with certain concepts such as *cryptographic hardness*. These are taken with the usual definitions; see e.g., [48].

Definition 1. *A Pre-Signature scheme $\mathcal{PS}$ consists of the following five algorithms:*

- $(pk, sk) = \text{keygen}(\ell)$*: I generates a public/private key pair with a security parameter (the security parameter ℓ is a variable determining the level of security in a cryptographic system. Increasing ℓ increases resistance against attacks, at the expense of increased computational and communication costs. In the specific context of the RSA-based implementation of the*

scheme introduced below, ℓ relates to the size of the RSA modulus.) ℓ, then keeps sk secret and distributes pk;

- $(k, \{(b_i, v_i)\}_{i=1}^n) = \text{register}(P, n)$*: I registers a prover P by generating a* hidden key *k, and a set of n (*blinding key, verification code*) pairs. I keeps k secret and sends the send of blinding keys and associated verification codes $S_P := \{(b_i, v_i)\}_{i=1}^n$ to P, and the verification codes on their own $\{v_i\}_{i=1}^n$ to V;*
- $\sigma = \text{pre-sign}(m, P)$*: I pre-signs a message m and sends it to P;*
- $\bar{\sigma} = \text{complete}(\sigma, b)$*: P chooses a blinding key b and completes a Pre-Signature σ, then sends the resulting ocmpleted signature $\bar{\sigma}$ it to V. In practice, the completed signature is also accompanied with an indicator for the verification code v corresponding to the chosen blinding key b;*
- $\text{verify}(\bar{\sigma}, m, v)$*: V verifies completed signature $\bar{\sigma}$ of message m using the associated verification code v.*

Figure 7 depicts the operations and interactions between the three parties in a Pre-Signature scheme.

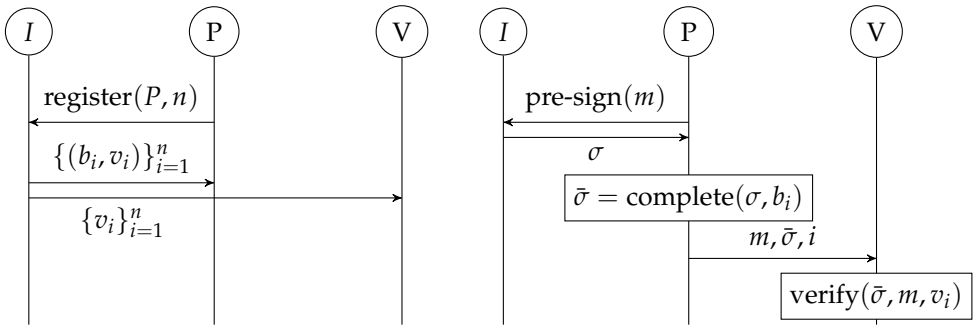

Figure 7. Sequence Diagram for Typical Operation of a Pre-Signature Scheme.

Definition 2. *The scheme $\mathcal{PS}$ is a secure Pre-Signature scheme if and only if it satisfies the following properties:*

Correctness *Completed signatures succeed verification iff valid, i.e., given* $(k, S_P) = \text{register}(P, n)$,

$$\text{verify}(\text{complete}(\text{pre-sign}(m, P), b), v) = \textit{True} \iff \exists (b, v) \in S_P.$$

In other words, given a message m, a valid Pre-Signature σ on m, and a valid completed signature $\overline{\sigma}$ on m and σ using b_i, the verification $\text{verify}(\overline{\sigma}, m, v_i)$ *succeeds if and only if (b_i, v_i) is a pair of blinding key, verification code in S_P.*

Unforgeability *For a malicious prover $\tilde{P}$, creating a valid completed signature for m^* using any $(b^*, v^*) \in S_{\tilde{P}}$ without* $\text{pre-sign}(m^*, \tilde{P})$ *is* hard.

Non-transferability *For a malicious prover $\tilde{P}$ knowing any* $\text{pre-sign}(m^*, \tilde{P})$ *and* $\text{pre-sign}(m^*, P' \neq \tilde{P})$*, creating a valid completed signature for m^* and a target $(b', v') \in S_{P'}$ is* hard.

Indistinguishability *Let $\sigma_0 = \text{pre-sign}(m_0, P_0)$, $\bar{\sigma}_0 = \text{complete}(\sigma_0, b_0)$, v_0 the associated verification code, and k_0, P_0's hidden key. Similarly for P_1, σ_1, $\bar{\sigma}_1$, b_1, v_1, and k_1. Given only pk, $(m_0, \bar{\sigma}_0, v_0)$ and $(m_1, \bar{\sigma}_1, v_1)$, determining whether $P_0 = P_1$ (or, equivalently, whether $k_0 = k_1$) is hard.*

We propose below a construction of $\mathcal{PS}_{\text{RSA}}$, a Pre-Signature scheme based on the RSA encryption/signature scheme:

- keygen: $pk = (e, N)$ and $sk = (d, N)$ with $(e, d, N) = \text{keygen}_{\text{RSA}}(\ell)$;
- register: k and $(b_i)_{i=1}^n$ are chosen at random in $\mathbb{Z}_N$, and $v_i = (kb_i)^e \pmod N$;
- pre-sign: $\sigma = h(m)^d k \pmod N$, with k the hidden key associated with P, and h a secure hash function;

- complete: $\bar{\sigma} = \sigma b \pmod{N}$;
- verify: returns True if and only if $\bar{\sigma}^e \equiv h(m)v \pmod{N}$.

Theorem 1. *$\mathcal{PS}_{RSA}$ is a secure Pre-Signature scheme.*

Proof. The four properties from Definition 2 are satisfied:

Correctness $\bar{\sigma}^e \equiv (\sigma b)^e \equiv (h(m)^d kb)^e \equiv h(m)(kb)^e \equiv h(m)v \pmod{N}$.

Unforgeability Without knowing σ^* or its own hidden key k, for $\tilde{P}$ to compute a valid completed signature $\bar{\sigma}^* \equiv (h(m^*)v^*)^d \pmod{N}$ would require computing the eth root of $h(m^*)v^*$. This reduces to the RSA problem.

Non-transferability Creating a completed signature for m^* and a target $(b', v') \in S_{P'}$ requires knowing the blinding key b' associated with the target verification code v'. The blinding key can be isolated by $\tilde{P}$ as $v'/v(b\sigma/\sigma')^e \equiv (k'b')^e/(kb)^e(bk/k')^e \equiv (b')^e \pmod{N}$ using known quantities. Computing b' from $v'/v(b\sigma/\sigma')^e \pmod{N}$ reduces to the RSA problem.

Indistinguishability The problem of determining r and s from $rs \pmod{N}$ (given r and s randomly distributed in $\mathbb{Z}_N$) solves integer factorization.

Under this reduction, since the blinding keys are randomly selected (in advance, by I), one cannot determine the blinding key or the Pre-Signature from a completed signature.

It follows that one cannot compute k_0^e from v_0 since b_0^e is secret (idem for k_1^e), and therefore distinguish k_0^e from k_1^e.

□

We note that, since the hidden key k is static for a given Prover, a message m always has the same Pre-Signature. It is up to the Prover to protect its own privacy by changing the blinding key appropriately.

6. Establishing the Simulation Environment

This section discusses the simulation scenario, focusing on rural areas with varying RSU deployments. It introduces the simulation's core concept and explains the selection and configuration of the simulation tool. It also discusses RSU placement using Voronoi diagrams and details the setup of the experiments.

6.1. Simulation Concept Overview

This section presents a simulation focused on vehicular communication in the Peak District, a National Park in central England, as shown in Figure 8, aiming to measure the impact of our scheme in a rural scenario with limited RSUs density. The simulation, spanning a 24 h period, mimics real-world driving conditions to evaluate connectivity challenges due to sparse RSUs availability. By concentrating on the Peak District, we aim to explore situations where vehicles frequently find themselves outside the range of RSUs, necessitating reliance on direct communication with other vehicles. The simulation is intended to demonstrate the effectiveness of the proposed Pre-Signature scheme, particularly in rural settings where RSU support is limited. This scheme enables vehicles to authenticate and verify reputation independently, a crucial feature in environments where RSU-based communication is not consistently available.

We ran multiple 24 h simulations under various conditions to assess how the scarcity of RSU infrastructure impacts communication reliability. These scenarios were evaluated with different RSU location availabilities. Additionally, we considered various hypotheses for overnight connectivity, accounting for the likelihood of vehicles connecting to the internet at night or in parking lots. This approach helped us to gauge the risk of being out of RSU range and its effect on communication reliability. Our objective is to measure the effectiveness of our proposed solution in addressing these challenges in areas with sporadic connectivity.

Figure 8. Peak District Map Extracted from OpenStreetMap (OSM) and Implemented in SUMO.

6.2. Selection and Configuration of the Simulation Tool

Simulation of Urban Mobility (SUMO) is a tool used worldwide for realistically simulating traffic and transport in urban environments [49]. While the tool is able to model multi-modal transport routes in urban environments, it is also able to simulate the simpler rural area, where cars alone are the primary mode of transportation [50]. As far as the authors are aware, SUMO is the most appropriate state-of-the-art tool for generating realistic traffic for our simulation [51]. Utilizing SUMO, we can import real maps from OpenStreetMap, integrating them into our simulations. This integration enables a comprehensive evaluation of vehicle communication, both with RSUs and among vehicles, across diverse rural and urban environments. See Figure 9.

As we are not measuring how the vehicles may respond to messages based on reputation, the behavior of the individual vehicles on the road is independent from our system. This means that it is possible to record all vehicle behavior over a 24 h timespan, putting this into a single XML output file, and then have custom Python script analyze the output files to generate the measurements. The output of the Python scripts includes (xlsx) files, allowing further analysis of the measurements completed by the scripts using Excel and Python scripts.

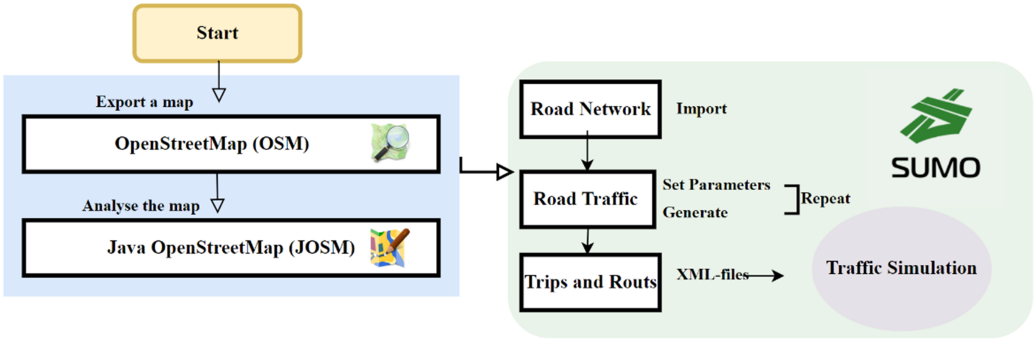

Figure 9. SUMO Architecture: Simulation Processes.

6.3. RSU Placement Using Voronoi Diagrams

Voronoi diagrams can be used as a tool for strategically deploying RSUs in connected vehicular networks, as discussed in [28]. To address the challenge of optimizing RSU placement, we employ Voronoi diagrams in a rural area. This geometric method divides the network area into convex polygons, each representing the coverage area of an individual RSU. Voronoi diagrams ensure that any point within a polygon is closer to its respective RSU than to any other, thereby maximizing network coverage efficiency.

Considering the possibility of 100 potential locations for 10 RSUs, we encounter 1.73×10^{13} configurations. Figure 10 visually illustrates this Voronoi-based approach, estimating the distribution of 10 RSUs within a 10 km square rural area, specifically, the Peak District. In the figure, red dots denote RSU locations, and blue-bordered Voronoi cells delineate their unique coverage areas, each with a radius of approximately 900–1000 m. This strategic placement ensures efficient wireless communication coverage, facilitating seamless vehicle connectivity throughout the Peak District.

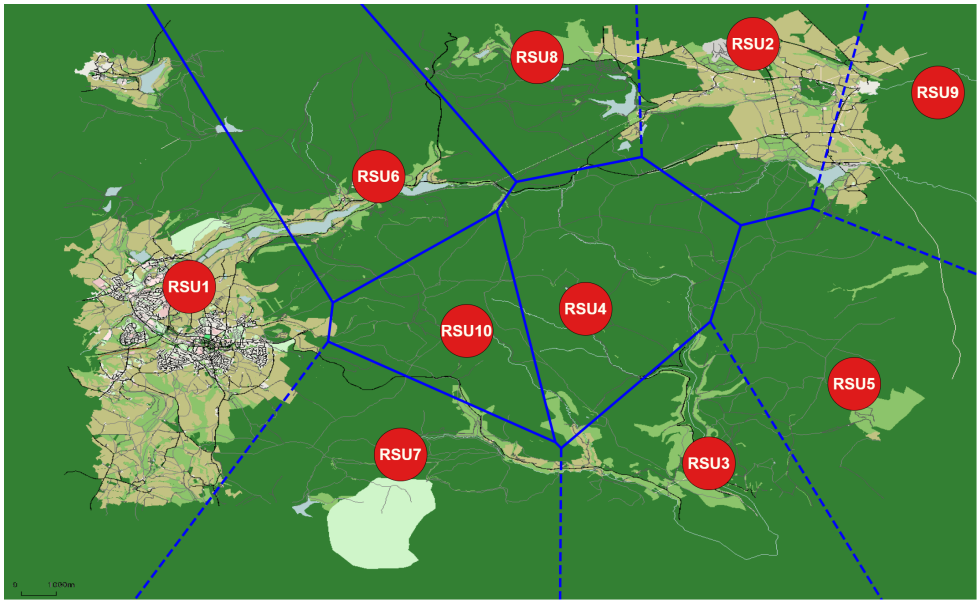

Figure 10. Strategic RSU Deployment Map for Optimal Coverage in a 10 km² Area of the Peak District.

Figure 10 provides an estimated optimization for deploying RSUs in rural regions, where connectivity is typically sparse and the undulating terrain presents significant barriers to signal transmission. In the context of the Peak District, with its rugged landscapes and limited existing infrastructure, the diagram anticipates the optimal locations for RSUs to maximize coverage and minimize the impact of natural obstructions like hills and valleys. This approach is crucial for improving vehicle communication in such rural areas. The estimation acknowledges the unique challenges of RSU deployment in these environments, offering a strategic method to overcome nature's impediments to connectivity.

6.4. Experimental Setup

The simulation was conducted using SUMO to validate the proposed model utilizing IEEE 802.11p/1609.4 protocols [52]. The simulation parameters are chosen to reflect the characteristics of a rural area like the Peak District and are detailed in Table 1. Key parameters include the network size, mobility model tailored to the Peak District's geography, vehicle communication standards, transmission range, and the simulation time, which spans a 24 h period. In our simulation, Vehicle-to-Roadside units (V2R) interactions are tracked at each time step (i.e., every second), meaning vehicles connect to RSUs whenever possible. V2V communications occur every 5 min; there is no universal standard for the frequency of exchanging, e.g., basic safety messages, and, moreover, occasional emergency messages are not sent on regular

intervals but as an average; 5 min seems to be in the right order of magnitude for most applications. Importantly, all collected data throughout the simulation are systematically saved in an XML file format.

Table 1. Simulation Parameters.

Parameter	Value
Network size (km^2)	10
Mobility model	Peak District
Vehicle communication standard	(DSRC) IEEE 802.11 P
Road Type	Multiple ways
Transmission Range: R (m)	250
Simulation Time (s)	90,464
Total Number of vehicles	21,650
Number of vehicles per kilometer	10, 15, 20, 25, 30, 50
Vehicle Length	2.5
Roadside Units (RSU)	0, 1, 2, 3, 4, 5, 7, 10, 15
Overnight Connectivity Percentage	0% to 100%

The simulation mirrors real-time rural traffic conditions, with vehicles entering the network from various directions and lanes under different conditions. One key aspect is the vehicles' potential to pass within a 300 m or 900 m range of an RSU, in line with DSRC standards' minimum and maximum values. Upon passing an RSU within range, a vehicle's Reputation Value RV is updated, and the RSU pre-signed the RV before transmitting it to the targeted vehicle. Subsequently, these vehicles could encounter other vehicles within the same range and initiate communication by exchanging messages while providing an updated RV. This means that the recipient vehicle has evidence of the sender vehicle having an up-to-date and accurate reputation. We refer to this as a 'reputable communication'.

This experiment assesses the influence of varying numbers of RSUs on rural vehicular communication systems. Our scenarios included setups with approximately 21,650 vehicles and different number of RSUs (0, 1, 2, 3, 4, 7, 10, and 15). We focused on metrics such as total vehicle count, overall communications, reputable communications, the application of Pre-Signature schemes, overnight connectivity percentages, and the availability of online communication.

To comprehensively evaluate these metrics, we developed a robust Dynamic Rural Area Connectivity scheme. This scheme employs mathematical and computational methods to analyze vehicular communications in a rural setting:

- **Parameters**: Set RSU coordinates, communication ranges (`rangeRSU`, `rangeSRC`, e.g., 900), and `overnight`, e.g., (0.0).
- **Initialisation**: Vehicles have the 'reputable' status with probability `overnight`.
- **Data Processing**: Parse 'xml file' and initialize arrays for vehicle states and communication metrics.
- **Simulation Loop**: Iterate over time steps, updating vehicle distances to RSU; if a vehicle is within range of an RSU, its status is set 'reputable'. Every 300th timestep (every 5 min), loop through all pairs of vehicles; if a pair is within range of each other, 'total communications' is increased, and, if the sender has status reputable, then 'reputable communications' is increased. Finally, if the recipient was also in range of an RSU, then 'online communications' is increased.
- **Aggregation**: Compute total communication and engagement metrics from accumulated data.

This scheme enables us to calculate and analyze communication patterns based on data collected from a 24 h simulation conducted under various parameter settings. The aggregated data allow us to answer various questions, including how effective our approach is in the scenario. Furthermore, this approach efficiently processed large datasets, allowing for a rapid assessment of dynamic communication patterns over time. This capability was crucial for understanding how different parameters, such as vehicle density and RSU placement, impact overall network connectivity and performance.

7. Simulation Results Discussion: Analysis and Evaluation

In this section, we delve into the key findings from our simulation of vehicular communication in the Peak District. Our focus is on understanding the impact of our approach within a rural setting, with limited availability of RSUs. The following analysis synthesizes the data collected from various 24 h simulation scenarios, providing insights into the effectiveness of our proposed Pre-Signature scheme in enhancing connectivity under diverse conditions.

The following figures derived from SUMO simulation GUI provide a visual representation of the communication scenarios enabled by the Pre-Signature scheme, illustrating its application and impact.

1. V2R Communication, Figure 11: Vehicles communicate with RSUs to update their RVs and obtain preliminary authentication credentials, ensuring network integrity within the RSU's service area.
2. Online V2V Communication, Figure 12: Vehicles within the RSU's range exchange information based on their RVs, guaranteeing the reliability of the communication.
3. Offline V2V Communication, Figure 13: Vehicles communicate outside the RSU's range, utilizing a Pre-Signature system to maintain dependable communication without RSU real-time supervision. Whether the communication has an up-to-date reputation available depends on whether the sender obtained a Pre-Signature prior.

These illustrative figures are a testament to the Pre-Signature scheme's critical role in enhancing vehicular network resilience, demonstrating the feasibility of reliable communication under varying RSU support conditions.

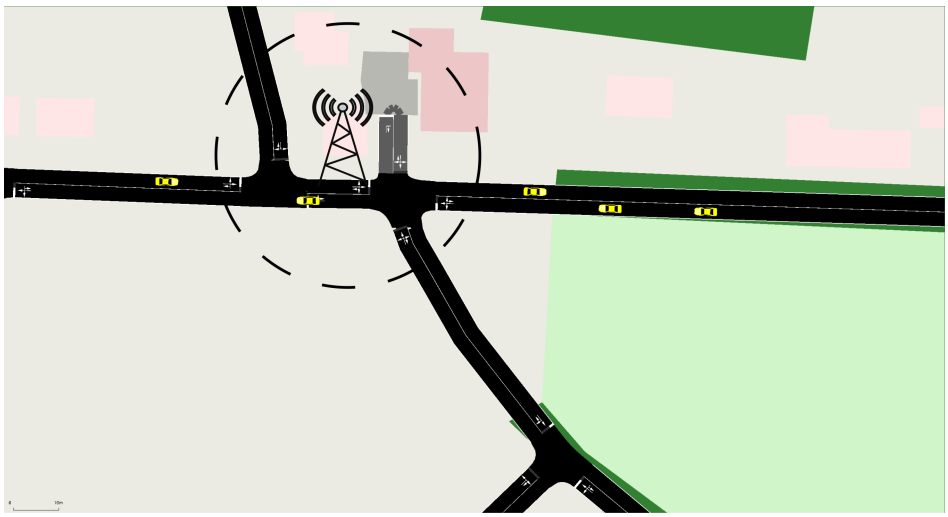

Figure 11. V2R Communication for Updating RV and obtaining Pre-Signature from RSU.

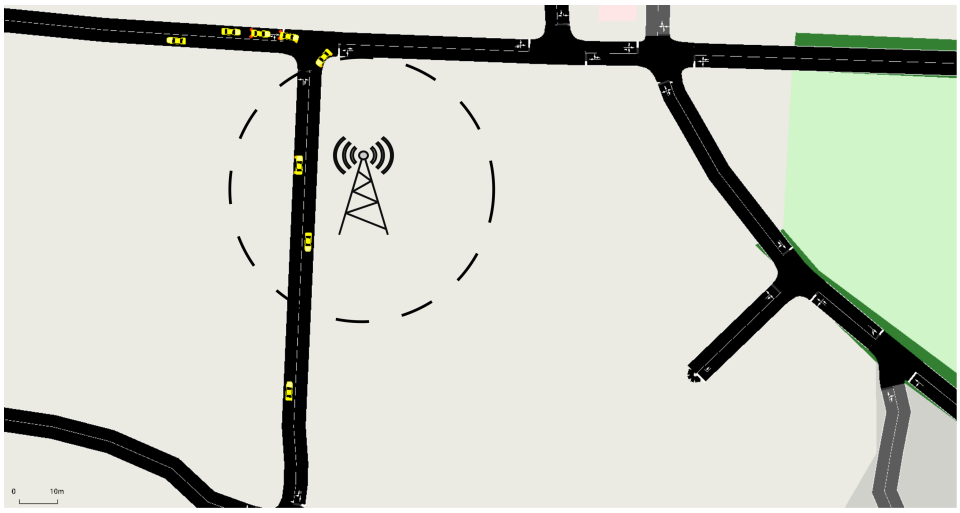

Figure 12. V2V Reputable Communication: Within RSU Range.

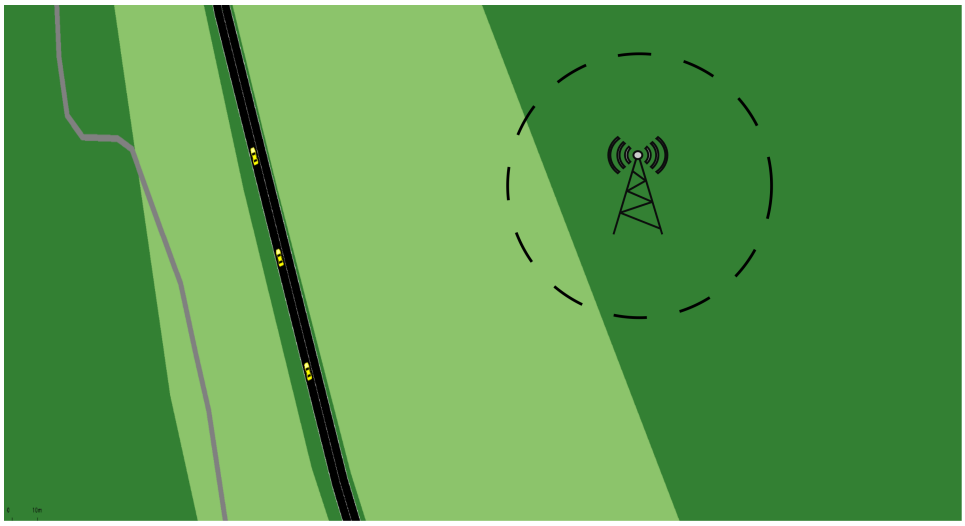

Figure 13. Offline V2V Reputable Communication: Outside RSU Range.

7.1. Key Metrics Analyzed

Our study conducted a comprehensive analysis of key factors to enhance the understanding of vehicular communication networks in rural areas:

- Vehicle Count (CV): We meticulously recorded the total number of vehicles at each second during the simulation.
- Vehicles with Pre-Signature (CPV): Special emphasis was placed on scenarios in which vehicles, upon encountering an RSU, received an updated RV or were accessible through overnight connectivity.
- Total Number of Communications (TC): Indicates the total number of V2V communications.
- Reputable Communications (RC): We focused on 'reputable communications', where vehicles with an updated RV successfully sent a message.
- Online Reputable Communications (ONRC): The extent of online communication availability was evaluated, signifying instances where vehicles with an RV communicated within the RSU's range. Here, reputation could be accessed via the RSU, meaning that—while the communication is reputable—our scheme was not necessary to accomplish this.
- Offline Reputable Communications (ORC): A pivotal element of our research was 'offline reputable communications,' referring to the exchange of RVs between vehicles located outside the RSU's range. These represent communications where a valid up-to-date reputation is available thanks to our scheme, where it otherwise would not be.

7.2. Evaluating RSU Availability and Overnight Connectivity

The analysis explored different scenarios of RSU availability and overnight connectivity percentages, from 0% (non-existent) to 100% (all vehicles have up-to-date Pre-Signatures at the start of day). These factors were assessed at every second of the simulation. This granular monitoring of parameters at each one-second interval allowed us to gain detailed insights into the dynamics of vehicular communications across different RSU density scenarios.

7.2.1. Vehicle and Communications over Time with Limited Connectivity

Figure 14 illustrates vehicle communication metrics over a 24 h period under a scenario of low connectivity with one RSU.

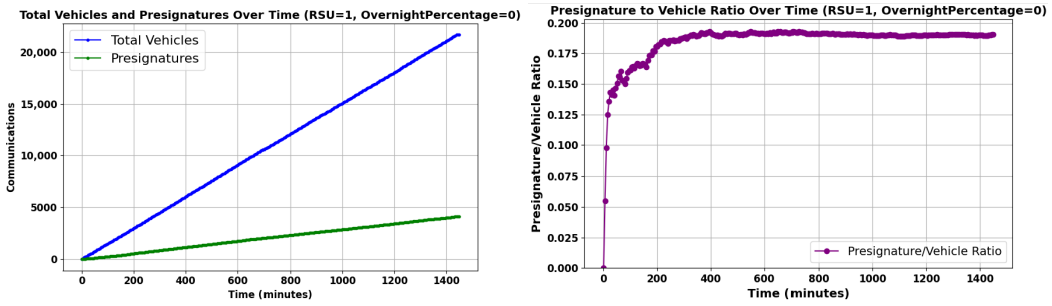

Figure 14. Vehicle Communication Activity Over Time with Limited Connectivity.

The left graph in Figure 14 shows a time series over 24 h, charting the growth of CV and CPV (see Section 7.1 for abbreviations). The CV increases steadily, whereas the CPV count grows more slowly, which could be indicative of the limited presence of only one RSU. Despite the increasing number of vehicles, the ratio of CPV to CV remains constant, suggesting a uniform Pre-Signature distribution over time. This is further supported by the right graph, where the ratio between CV and CPV quickly converges to be constant.

An argument could be made that the fraction/number of vehicles with a Pre-Signature is not the quantity of interest as some vehicles may never/rarely communicate with other vehicles, and the presence of an up-to-date reputation is less relevant in such a case. One should not expect the presence of a Pre-Signature to be independent from the amount of communication a vehicle carries out as an isolated vehicle far from a town is less likely to have a Pre-Signature and is expected to communicate less—and vice versa for a vehicle in a town.

Figure 15 offers a view of various communication metrics over time. It encompasses the TC, depicted in blue, which represents the total number of communications. The RC, in green, indicates those communications deemed reputable; the goal of any reputation system is to have this value as high as possible. The ONRC, shown in purple, highlights reputable communications accessible online. This is the performance of a naive reputation system without Pre-Signatures. Crucially, the offline reputable communications ORC shown in red represents the reputable communications conducted offline, which were enabled by our Pre-Signature scheme. This metric, underpinning the Pre-Signature scheme, emphasizes the strength and reliability of communications in offline settings. The steady or increasing trend of the red line on the graph underscores the robustness and adaptability of our Pre-Signature scheme, ensuring effective and secure transactions even without online connectivity. In the graph on the right, the line displays the ratio of RC to TC, providing a measure of communication quality relative to its quantity.

The ratios CPV:CV and RC:TC converge to similar values. However, there are two opposing effects at play. A vehicle could receive the Pre-Signature near the end of its lifetime, decreasing RC:TC relative to CPV:CV. Conversely, cars receiving Pre-Signatures are close to RSUs, which tend to be in busier areas, meaning a higher degree of communication for vehicles with a Pre-Signature. For the parameters chosen for this specific scenario,

they happen to cancel out; this is not generally the case. It is important to understand the relationship between the parameters.

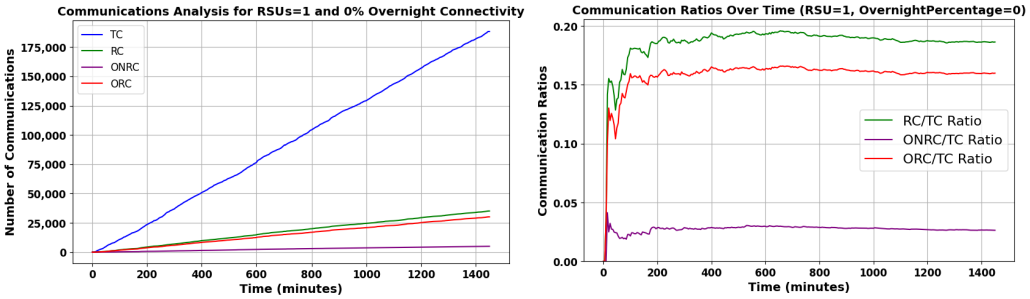

Figure 15. Time-Based Analysis of Communications Metrics for RSU 1 with 0% Overnight Connectivity.

7.2.2. Evaluating RSU Deployment in Rural Areas

This section presents the outcomes of our simulation study focusing on RSU deployment in a rural setting, exemplified by the Peak District. The simulation explores the impact of RSU density on communication patterns within two different range scenarios—300 m, representing limited coverage, and 900 m, for extended coverage. The RSU deployment strategy commences with nothing and progressively increases the number of units, reflecting a realistic expansion towards 15 RSUs.

Figures 16–18 show an analysis of vehicular communication efficacy by RSU density and range (300–900 m). These figures offer insights into how different types of vehicular communications perform in scenarios where the overnight connectivity factor varies at 30%, 50%, and 70%, respectively. The analysis delineates three principal communication categories—Online Available, Reputable, and Offline Reputable. The RSU densities are varied to simulate different deployment stages:

- 0 RSUs: Represents an absence of RSU presence.
- 1 RSU: Indicates a very low RSU density, with minimal coverage.
- 3 RSUs: Depicts a low RSU density, offering limited communication capabilities.
- 5 RSUs: Corresponds to a medium RSU density, reflecting an improving infrastructure.
- 7 RSUs: Demonstrates a high RSU density, nearing effective coverage.
- 15 RSUs: Signifies a very high RSU density, with a robust communication network.

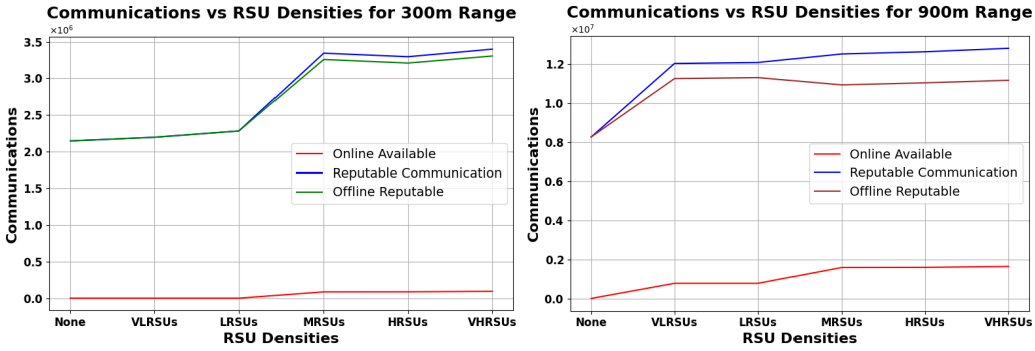

Figure 16. Analysis of Vehicular Communication Efficacy under 30% Overnight Connectivity Across Various RSU Densities, with Comparisons at 300 m Range (**Left**) and 900 m Range (**Right**).

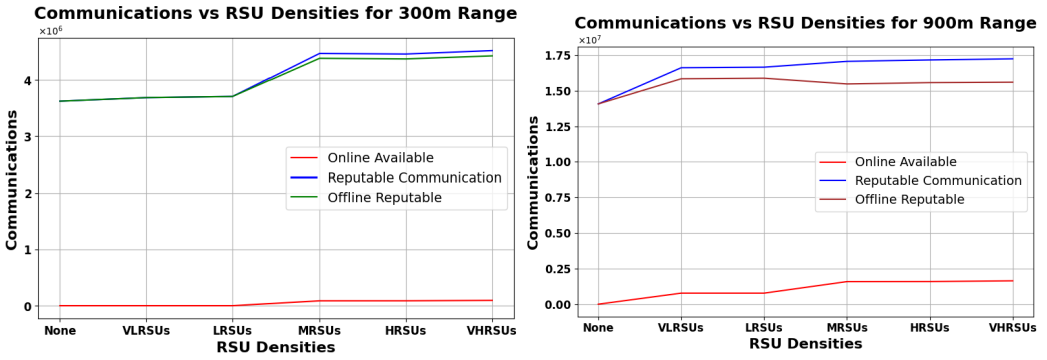

Figure 17. Analysis of Vehicular Communication Efficacy under 50% Overnight Connectivity Across Various RSU Densities, with Comparisons at 300 m Range (**Left**) and 900 m Range (**Right**).

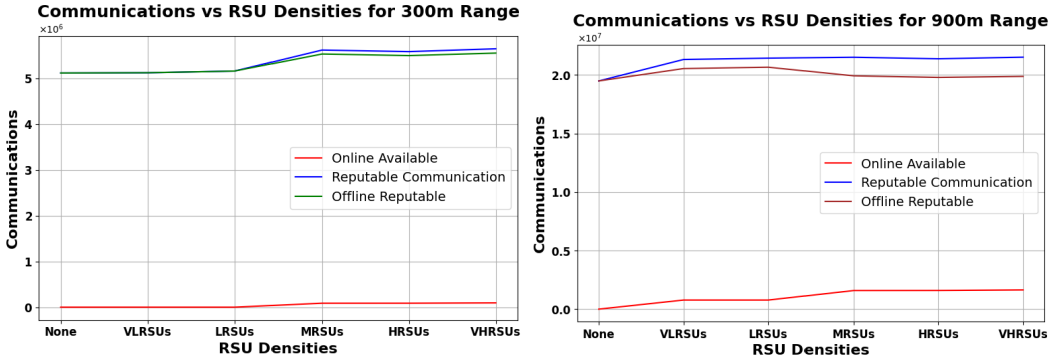

Figure 18. Analysis of Vehicular Communication Efficacy under 70% Overnight Connectivity Across Various RSU Densities, with Comparisons at 300 m Range (**Left**) and 900 m Range (**Right**).

Figures 16–18 (left) show that, for the 300 m range, RSU density has a small impact on online communications, while the number of reputable communications generally increases with increasing RSUs. At the 900 m range (right graphs), both online and reputable communications experience a slight enhancement at lower RSU densities with diminishing gains as density increases. The line for ORC is fairly close to RC in all the graphs, meaning that our scheme is the primary contributor to the availability of reputation in the rural scenario. In Figure 18 (right), we can see ORC decreasing a bit, suggesting a unimodal curve, where a very high RSU density allows for increasingly more reputation to be available online, diminishing the need for our scheme. Note that, in an urban scenario, the density of RSUs may be orders of magnitude higher, allowing the ONRC to overtake the ORC—which would imply that our scheme has less benefit in such an environment. However, as long as ORC is larger than zero, the impact is positive (and if zero, the impact is nil).

Overall, RSU impact is more significant at lower densities and diminishes with greater range and density. Our analysis indicates that deploying even a single RSU can significantly enhance communication patterns in rural areas. As RSU density increases, the efficiency of our Pre-Signature scheme improves, particularly within the RSU range. This improvement is evidenced by the increase in reputable communications, both online and offline. However, the most notable enhancement is observed in the online reputable communications, highlighting the benefits of RSU proximity.

Notably, even in the absence of RSU presence ('None'), the graph denotes a substantial count of ORC. This phenomenon accentuates the Pre-Signature scheme's strength in fostering trust and reliability in vehicular communications devoid of centralized infrastructure support. The scheme's resilience is further corroborated by the consistent level of ORC observed across all RSU densities, which is critical for the autonomous management of Reputation Values.

These findings articulate the Pre-Signature scheme's critical role in enhancing vehicular network resilience, particularly under the stringent different cases of overnight connectivity.

This resilience ensures reliable communication channels in scenarios where RSU deployment is either sparse or entirely absent, which is a common challenge in rural and underserved regions.

7.2.3. Analysis of Communication Types over Overnight Percentage

Figures 19 and 20 offer a visual analysis of how overnight connectivity percentages affect communication patterns for vehicles in rural areas, where internet access is often conditional on being near home networks or designated parking lot hotspots. This research measures connectivity on a scale from complete absence (0) to full coverage (100), revealing a direct relationship between the degree of connectivity and the quantity of reputable communications (RC). This trend suggests that, as vehicles gain better internet access overnight, they are more capable of updating their reputation metrics, showcasing the Pre-Signature scheme's potential in enhancing vehicular communication.

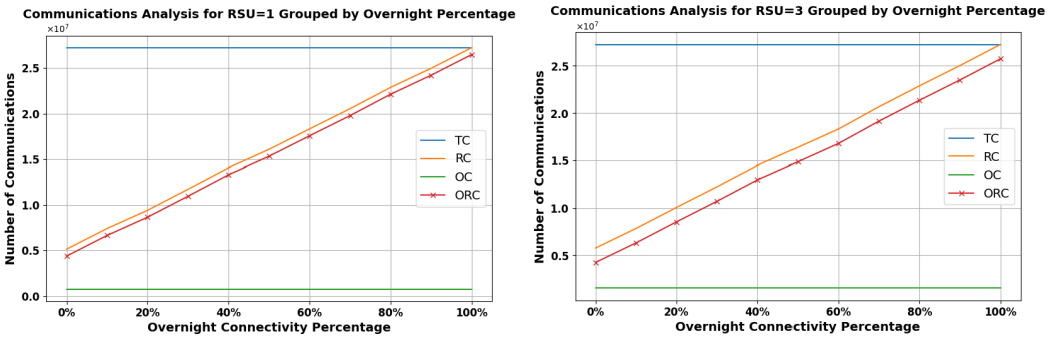

Figure 19. Analysis of Communication Types over Overnight Percentage in High RSU Range = 900 m for 1 RSU (**Left**) and 3 RSUs (**Right**).

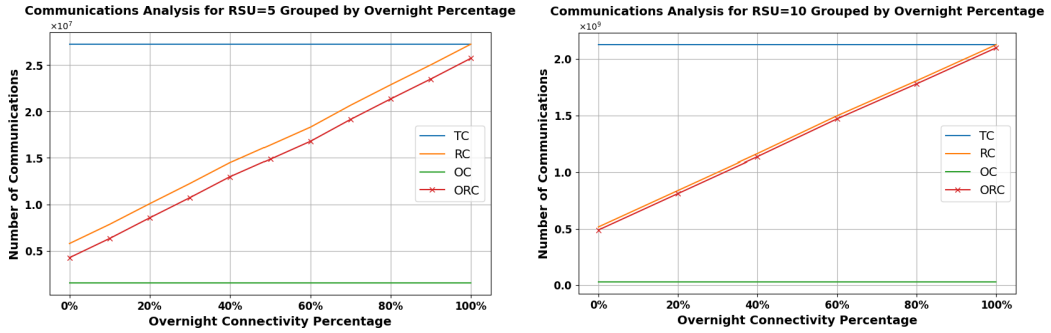

Figure 20. Analysis of Communication Types over Overnight Percentage in Low RSU Range = 300 m for 5 RSUs (**Left**) and 10 RSUs (**Right**).

Notably, the graph sheds light on ORC, signifying that, even without RSU range, vehicles can still engage in trustworthy exchanges by leveraging pre-signed data, ensuring secure and dependable communication in areas with limited connectivity.

Observe that all graphs in Figures 19 and 20 are approximately linear. Having a large proportion of vehicles update their reputation overnight is one of the most effective ways to boost the quality of our approach.

7.3. Results Summary: Pre-Signature Scheme in Rural Vehicular Communication Areas

The study on vehicular communication systems in rural settings places significant emphasis on the effectiveness of the Pre-Signature scheme, particularly in enhancing reputable communications in environments with sparse or non-existent RSU support. This scheme emerges as a pivotal solution for maintaining reliable and secure vehicular communication channels, especially in offline scenarios prevalent in rural areas.

The experiments show the effectiveness of our scheme with different parameters and in different ways. In particular, we showed to what extent reputation disseminates over time in a 24 h period and how this affects the number and proportion of reputable

communications. We then investigated how adoption of RSU units affects how useful our approach is, which showed that, in rural environments, increasing RSUs typically has a positive effect. We finally quantified the impact of drivers obtaining a Pre-Signature before entering the road, showing that this is an extremely powerful way to boost the effectiveness of our approach.

A noteworthy aspect of the Pre-Signature scheme is its ability to uphold the integrity and trustworthiness of communications, regardless of RSU density. It ensures a consistent level of reputable communications, both online and offline. This is particularly vital in situations where vehicles operate outside the RSU range or in locations completely devoid of RSU presence. The study's findings highlight the Pre-Signature scheme as a key enabler for robust and dependable communication in rural vehicular networks, successfully addressing the challenges posed by limited infrastructure.

8. Conclusions

This research has delved into applying an innovative Pre-Signature scheme for V2V communications. We provide recommendations for changing standards, formats, and specifications to ensure that our approach is usable in the real-world.

The approach is particularly suitable for rural landscapes where RSU availability is often limited or irregular. Through detailed simulations that closely emulate real-world rural scenarios, our study has provided an in-depth evaluation of this scheme efficiency under the typical infrastructural constraints of rural settings. The findings underscore the scheme's adaptability in varying RSU conditions, demonstrating its efficacy in maintaining communication integrity even in sparse RSU networks. This contributes significantly to our understanding of strategic RSU deployment, highlighting its vital role in enhancing rural V2V communication systems.

Future research should focus on integrating emerging technologies like 5G and satellite communications to strengthen connectivity in remote areas. Additionally, exploring the synergy between this scheme and connected vehicle technologies could offer significant advancements in rural smart transportation systems. Further studies could also involve real-world trials to validate and fine-tune the applicability of our findings.

Author Contributions: conceptualisation, D.A., T.M. and S.F.; Methodology, D.A. T.M., S.F and X.C.; Validation, D.A., T.M. and S.F.; Formal analysis, D.A.; Investigation, D.A.; Data curation, D.A.; writing—original draft preparation, D.A.; Writing—review and editing, D.A., T.M., S.F., X.C. and T.Y.; Visualization, D.A., T.M., S.F., X.C. and T.Y.; Supervision, T.M. and S.F.; Project administration, D.A. All authors have read and agreed to the published version of the manuscript.

Funding: The work of Takahito Yoshizawa was partially supported by CyberSecurity Research Flanders with reference number VR20192203.

Data Availability Statement: The data can be shared up on request.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CPV	Vehicles with Pre-Signature
CRL	Certification Revocation List
CV	Vehicle Count
DENM	Decentralized Environmental Notification Message
DSRC	Dedicated Short-Range Communication
ECDSA	Elliptic Curve Digital Signature Algorithm
ITS	Intelligent Transport Systems

MA	Misbehavior Authority
ONRC	Online Reputable Communications
ORC	Offline Reputable Communications
PCA	Pseudonym Certificate Authority
PCs	Pseudonym Certificates
RA	Registration Authority
RC	Reputable Communications
RS	Reputation Server
RSUs	Roadside Units
RV	Reputation Value
SCMS	Security Credential Management System
SUMO	Simulation of Urban Mobility
TC	Total Number of Communications
V-PKI	Vehicular Public Key Infrastructure
V2I	Vehicle-to-Infrastructure
V2R	Vehicle-to-Roadside units
V2V	Vehicle-to-Vehicle
VANETs	Vehicular Ad hoc Networks
WAVE	Wireless Access in Vehicular Environments

References

1. Anwar, W.; Franchi, N.; Fettweis, G. Physical Layer Evaluation of V2X Communications Technologies: 5G NR-V2X, LTE-V2X, IEEE 802.11 BD, and IEEE 802.11 P. In Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22–25 September 2019.
2. Shurrab, M.; Singh, S.; Otrok, H.; Mizouni, R.; Khadkikar, V.; Zeineldin, H. An Efficient Vehicle-to-Vehicle (V2V) Energy Sharing Framework. *IEEE Internet Things J.* **2021**, *9*, 5315–5328. [CrossRef]
3. Li, Q.; Malip, A.; Martin, K.M.; Ng, S.L.; Zhang, J. A Reputation-Based Announcement Scheme for VANETs. *IEEE Trans. Veh. Technol.* **2012**, *61*, 4095–4108.
4. Xie, Q.; Ding, Z.; Zheng, P. Provably Secure and Anonymous V2I and V2V Authentication Protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 7318–7327. [CrossRef]
5. Cui, J.; Wei, L.; Zhang, J.; Xu, Y.; Zhong, H. An Efficient Message-Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 1621–1632. [CrossRef]
6. Papadimitratos, P. Secure Vehicular Communication Systems. In *Encyclopedia of Cryptography, Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 1–6.
7. Simplicio, M.A.; Cominetti, E.L.; Patil, H.K.; Ricardini, J.E.; Silva, M.V.M. The Unified Butterfly Effect: Efficient Security Credential Management System for Vehicular Communications. In Proceedings of the 2018 IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, 5–7 December 2018.
8. Verheul, E.; Hicks, C.; Garcia, F.D. IFAL: Issue First Activate Later Certificates for V2X. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroSP), Stockholm, Sweden, 17–19 June 2019.
9. Liu, Z.-C.; Xiong, L.; Peng, T.; Peng, D.-Y.; Liang, H.-B. A Realistic Distributed Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Access* **2018**, *6*, 26307–26317. [CrossRef]
10. Asghar, M.; Doss, R.R.M.; Pan, L. A Scalable and Efficient PKI Based Authentication Protocol for VANETs. In Proceedings of the 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, Australia, 21–23 November 2018.
11. Qi, J.; Gao, T. A Privacy-Preserving Authentication and Pseudonym Revocation Scheme for VANETs. *IEEE Access* **2020**, *8*, 177693–177707. [CrossRef]

12. Joshi, A.; Gaonkar, P.; Bapat, J. A Reliable and Secure Approach for Efficient Car-to-Car Communication in Intelligent Transportation Systems. In Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2017.
13. Miorandi, D.; Altman, E. Connectivity in One-Dimensional Ad Hoc Networks: A Queueing Theoretical Approach. *Wirel. Netw.* **2006**, *12*, 573–587. [CrossRef]
14. Wisitpongphan, N.; Bai, F.; Mudalige, P.; Sadekar, V.; Tonguz, O. Routing in Sparse Vehicular Ad Hoc Wireless Networks. *IEEE J. Sel. Areas Commun.* **2007**, *25*, 1538–1556. [CrossRef]
15. Wu, J. Connectivity Analysis of a Mobile Vehicular Ad Hoc Network with Dynamic Node Population. In Proceedings of the 2008 IEEE Globecom Workshops, New Orleans, LA, USA, 30 November–4 December 2008.
16. Khabazian, M.; Ali, M.K.M. A Performance Modeling of Connectivity in Vehicular Ad Hoc Networks. *IEEE Trans. Veh. Technol.* **2008**, *57*, 2440–2450. [CrossRef]
17. Ng, S.C.; Zhang, W.; Yang, Y.; Mao, G. Analysis of Access and Connectivity Probabilities in Infrastructure-Based Vehicular Relay Networks. In Proceedings of the 2010 IEEE Wireless Communication and Networking Conference, Sydney, NSW, Australia, 18–21 April 2010.
18. Coifman, B.; Li, L. A Critical Evaluation of the Next Generation Simulation (NGSIM) Vehicle Trajectory Dataset. *Transp. Res. Part B Methodol.* **2017**, *105*, 362–377. [CrossRef]
19. Reis, A.B.; Sargento, S.; Tonguz, O.K. On the Performance of Sparse Vehicular Networks with Road Side Units. In Proceedings of the 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring), Budapest, Hungary, 15–18 May 2011.
20. Liu, C.; Huang, H.; Du, H. Optimal RSUs Deployment with Delay Bound along Highways in VANET. *J. Comb. Optim.* **2017**, *33*, 1168–1182. [CrossRef]
21. Wu, T.J.; Liao, W.; Chang, C.J. A Cost-Effective Strategy for Road-Side Unit Placement in Vehicular Networks. *IEEE Trans. Commun.* **2012**, *60*, 2295–2303. [CrossRef]
22. Cui, J.; Zhang, X.; Zhong, H.; Zhang, J.; Liu, L. Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in a Multi-Cloud Environment. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 1654–1667. [CrossRef]
23. Khan, S.; Zhu, L.; Yu, X.; Zhang, Z.; Rahim, M.A.; Khan, M.; Du, X.; Guizani, M. Accountable Credential Management System for Vehicular Communication. *Veh. Commun.* **2020**, *25*, 100279. [CrossRef]
24. El Sayed, H.; Zeadally, S.; Puthal, D. Design and Evaluation of a Novel Hierarchical Trust Assessment Approach for Vehicular Networks. *Veh. Commun.* **2020**, *24*, 100227. [CrossRef]
25. Kudva, S.; Badsha, S.; Sengupta, S.; Khalil, I.; Zomaya, A. Towards Secure and Practical Consensus for Blockchain Based VANET. *Inf. Sci.* **2021**, *545*, 170–187. [CrossRef]
26. Liu, C.; Huang, H.; Du, H.; Jia, X. Optimal RSUs Placement with Delay Bounded Message Dissemination in Vehicular Networks. *J. Comb. Optim.* **2017**, *33*, 1276–1299. [CrossRef]
27. Guerna, A.; Bitam, S. GICA: An Evolutionary Strategy for Roadside Units Deployment in Vehicular Networks. In Proceedings of the 2019 International Conference on Networking and Advanced Systems (ICNAS), Annaba, Algeria, 26–27 June 2019; pp. 1–6.
28. Aurenhammer, F. Voronoi Diagrams—A Survey of a Fundamental Geometric Data Structure. *ACM Comput. Surv. (CSUR)* **1991**, *23*, 345–405. [CrossRef]
29. Patil, P.; Gokhale, A. Voronoi-Based Placement of Road-Side Units to Improve Dynamic Resource Management in Vehicular Ad Hoc Networks. In Proceedings of the 2013 International Conference on Collaboration Technologies and Systems (CTS), San Diego, CA, USA, 20–24 May 2013; pp. 389–396.
30. Sukuvaara, T.; Nurmi, P. Wireless Traffic Service Platform for Combined Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communications. *IEEE Wirel. Commun.* **2009**, *16*, 54–61. [CrossRef]
31. Brecht, B.; Therriault, D.; Weimerskirch, A.; Whyte, W.; Kumar, V.; Hehn, T.; Goudy, R. A Security Credential Management System for V2X Communications. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3850–3871. [CrossRef]
32. Tao, R.; Wolleschensky, L.; Weimerskirch, A. Security Certificate Management System for V2V Communication in China. *SAE Int. J. Transp. Cyber. Privacy* **2019**, *2*, 169–183. [CrossRef]
33. Kenney, J.B. Dedicated Short-Range Communications (DSRC) Standards in the United States. *Proc. IEEE* **2011**, *99*, 1162–1182. [CrossRef]
34. Automated Vehicle Research. [Online]. 2021. Available online: https://www.its.dot.gov/automatedvehicle/ (accessed on 23 September 2023).
35. Yu, H.; Liu, R.; Li, Z.; Ren, Y.; Jiang, H. An RSU Deployment Strategy Based on Traffic Demand in Vehicular Ad Hoc Networks (VANETs). *IEEE Internet Things J.* **2022**, *9*, 6496–6505. [CrossRef]
36. *IEEE Std 1609.2-2016*; IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages. IEEE Vehicular Technology Society: Piscataway, NJ, USA, 2016.
37. *TS 102 940*; Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management, Ver.2.1.1. European Telecommunication Standard Institute (ETSI): Sophia Antipolis, France, 2021.
38. *TS 102 941*; Intelligent Transport Systems (ITS); Security; Trust and Privacy Management, Ver.2.1.1. European Telecommunication Standard Institute (ETSI): Sophia Antipolis, France, 2021.
39. *TS 103 097*; Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats, Ver.2.1.1. European Telecommunication Standard Institute (ETSI): Sophia Antipolis, France, 2021.

40. *EN 302 637-2*; Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service, Ver.1.3.1. European Telecommunication Standard Institute (ETSI): Sophia Antipolis, France, 2019.
41. Almani, D.; Muller, T.; Furnell, S.; Carpent, X.; Yoshizawa, T. A Pre-Signature Scheme for Trustworthy Offline V2V Communication. In Proceedings of the 14th IFIP International Conference on Trust Management (IFIPTM 2023), Amsterdam, The Netherlands, 19–20 October 2023.
42. Zeddini, B.; Maachaoui, M.; Inedjaren, Y. Security Threats in Intelligent Transportation Systems and Their Risk Levels. *Risks* **2022**, *10*, 91. [CrossRef]
43. Fujisaki, E.; Suzuki, K. Traceable Ring Signature. In *International Workshop on Public Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 181–200.
44. Jiang, Y.; Ge, S.; Shen, X. AAAS: An Anonymous Authentication Scheme Based on Group Signature in VANETs. *IEEE Access* **2020**, *8*, 98986–98998. [CrossRef]
45. Backes, M.; Meiser, S.; Schröder, D. Delegatable Functional Signatures. In *Public-Key Cryptography—PKC 2016: 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, 6–9 March 2016*; Proceedings, Part I; Springer: Berlin/Heidelberg, Germany, 2016; pp. 357–386.
46. Pointcheval, D.; Stern, J. Security Arguments for Digital Signatures and Blind Signatures. *J. Cryptol.* **2000**, *13*, 361–396. [CrossRef]
47. Ateniese, G.; Hohenberger, S. Proxy Re-Signatures: New Definitions, Algorithms, and Applications. In Proceedings of the 12th ACM Conference on Computer and Communications Security, ACM, Alexandria, VA, USA, 7–11 November 2005; pp. 310–319.
48. Katz, J.; Katz, J. Cryptographic Hardness Assumptions. In *Digital Signatures*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 35–66.
49. SUMO Home Page. [Online]. 2021. Available online: https://eclipse.dev/sumo/ (accessed on 10 February 2023).
50. Lopez, P.A.; Behrisch, M.; Bieker-Walz, L.; Erdmann, J.; Flötteröd, Y.-P.; Hilbrich, R.; Lücken, L.; Rummel, J.; Wagner, P.; Wießner, E. Microscopic Traffic Simulation Using SUMO. In Proceedings of the 21st IEEE International Conference on Intelligent Transportation Systems, IEEE Intelligent Transportation Systems Conference (ITSC), Maui, HI, USA, 4–7 November 2018. Available online: https://elib.dlr.de/124092/ (accessed on 19 October 2023).
51. Sommer, C.; German, R.; Dressler, F. Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. *IEEE Trans. Mob. Comput.* **2011**, *10*, 3–15. [CrossRef]
52. Di Felice, M.; Ghandour, A.J.; Artail, H.; Bononi, L. On the Impact of Multi-Channel Technology on Safety-Message Delivery in IEEE 802.11p/1609.4 Vehicular Networks. In Proceedings of the 2012 21st International Conference on Computer Communications and Networks (ICCCN), Munich, Germany, 30 July–2 August 2012; pp. 1–8.