Pre-Signature Scheme for Trustworthy Offline V2V Communication

Abstract. Vehicle-to-Vehicle (V2V) communication systems hold great potential for enhancing road safety and traffic efficiency. The authentication of such communication is crucial, particularly in scenarios where infrastructure is absent, while also ensuring the privacy of the participating vehicles. The Security Credential Management System (SCMS) offers a solution using pseudonym certificates. The pseudonymous nature of the V2V communication poses a challenge to integrating reputation of vehicles. We propose a novel solution that allows reputation to be used even when vehicles are pseudonymous and without access to a reputation server. By extending SCMS with a reputation system, vehicles can securely retrieve and update their reputation from a dedicated server, resulting in improved effectiveness of offline V2V communication. To achieve this, we propose a two-step signature scheme variant called *Pre-Signature*. This scheme enables an appropriate balance between reputation and pseudonymity in offline V2V communication. It increases message size by approximately 0.5 kilobytes while ensuring efficient offline operation and secure communication, with minimal computational overhead for signing and verification operations.

Keywords: V2V · SCMS · Reputation· Trust · Cryptographic Signatures · Certificates · Vehicular Communication

1 Introduction

Vehicular Ad-hoc Networks (VANETs) enable two important types of communication: Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V). V2V communication enables the exchange of emergency messages, even in offline settings, The authenticity and security of these messages essential for informed decision-making and enhanced road safety.

In offline scenarios, vehicles solely rely on neighbouring vehicles for communication, necessitating trust and reliability among them [2]. Certificates can be used to authenticate V2V communication. However, the reuse of certificates can break the privacy of the user, as the recipient can then recognise users. Mechanisms like SCMS (security credential management system) use *Pseudonym Certificates* (PCs) to verify message authenticity in an offline setting.

In SCMS, a Certificate Revocation List (CRL) is maintained to identify and block misbehaving vehicles from the communication network. The CRL must be synchronised when vehicles have access to the infrastructure, e.g. via Roadside Units (RSUs) [21, 27]. The CRL scales linearly with the number of misbehaving vehicles, and these lists must be communicated to and maintained by every vehicle. The property of misbehaving must be a black-or-white proposition. We propose a mechanism that is more scalable than a CRL, and uses a more granular notion of reputation.

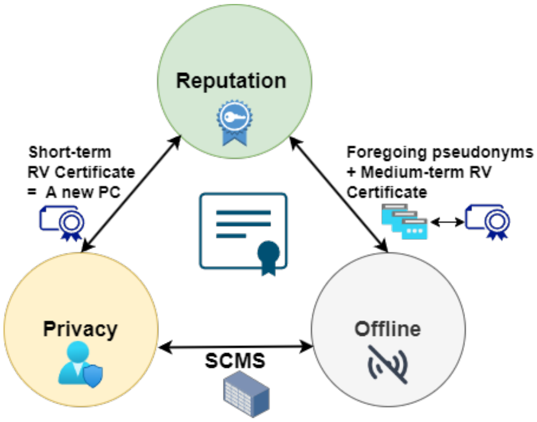


Fig. 1. An Integrated Approach for Reputation, Offline, and Privacy in V2V

A reputation system leverages the historical behaviour of vehicles, to assess their reliability and trustworthiness. By using the vehicle's reputation, decision-making can be made more accurate, reducing the risk posed by misleading information. How past information is collected, stored and used to compute or update a *reputation value* (RV) has been studied widely in [21]. However, in this paper, we are only interested in the question on how to disseminate the reputation value held at the *Reputation Server* (RS), such that it can be used in offline settings without breaking privacy.

The motivation for our work is to extend existing systems to enhance trust and reliability in V2V communication. The goal is to develop a system to authenticate messages which maintains *privacy*, works *offline*, and allows *reputation* to be used. See Figure 1.

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 the properties in a scalable way, with minimal changes to the standards.

The key ingredient for our solution is a new cryptographic primitive that we call a *pre-signature*. The pre-signature scheme is a two step process, where party A pre-signs a particular message and party B can complete the signature, linking it to a certificate. Party B cannot change the message without party A (unforgeability). Another party C cannot use the pre-signature to complete the signature (non-transferability). An observer cannot tell whether a pair of completed signatures are based on the same pre-signature or not (indistinguishability).

Our system works as follows: Every day vehicles should request a fresh pre-signature of their most recent reputation value. Using this pre-signature, the vehicle computes a new completed signature, every time they switch pseudonyms. Vehicles can verify the reputation value in an offline setting (due to unforgeability and non-transferability), without breaking the privacy of the sender (due to indistinguishability). Unlike CRLs, the overhead does not depend on the number of malicious vehicles identified. Moreover, the reputation value allows a more granular notion of misbehaviour than CRLs.

The next section summarizes the background and analyses the issues in the existing standards, leading to the introduction of the reputation-based system model in Section 3. Next, section 4 outlines the proposed *Pre-Signature* scheme. Section 5 then introduces the scheme operation. Section 6 discusses the scheme's operational considerations and some challenges. Section 7 reviews the state-of-the-art and related work, contextualizing the proposed scheme. Finally, section 8 concludes the paper and identifies directions for future work.

2 Background

Outside residential and urban areas, vehicles can move into locations where no RSUs are deployed (e.g. tunnels, mountains, and remote areas). In such conditions, Dedicated Short Range Communication (DSRC) serves as the communication method for V2V interaction, allowing vehicles to exchange messages and send alert within a 300-900-meter range regardless of the presence of nearby RSUs [23]. The receiving vehicles would normally verify these messages with RSUs but cannot do so in offline conditions. Similarly, reference to a CRL is not possible in such a context. In this scenario, the sending vehicle needs to transmit a message that is linked to both its reputation and pseudonym certificate. A receiving vehicle then makes a decision based on the sender's reputation. As background for the work, it is relevant to begin by explaining some key elements that provide context for the problem, namely the current use of certificates and the challenge presented by the offline V2V communication scenario. In terms of certificates, two types are of interest in this discussion:

SCMS Certificates: Vehicular Public-Key Infrastructure (VPKI) networks are being deployed globally to ensure the security of vehicle communication. Key initiatives such as ETSI and C2C-CC in Europe [31], SCMS [34] in the US, SCME in China [32], and others are dedicated to establishing robust communication frameworks and efficient credential management systems for both vehicles and infrastructure. These endeavors significantly enhance the effectiveness and security of transportation systems. SCMS serves as a standardised solution for securing V2V communications, making it the focal point of our work. As shown in Figure 2, SCMS ensures trust between vehicles by facilitating and verifying V2V security certificates [19] and exchanges anonymised data without sharing personally identifiable information with other entities [38]. SCMS is therefore considered a central system in enabling trust amongst authorised vehicles. SCMS is an implementation of PKI based system that uses certificate management to enhance trust in V2V communication. In this system, the Pseudonym Certificate Authority (PCA) collaborates with the Misbehaviour Authority (MA), Linkage Authorities (LA1, LA2), and Registration Authority (RA) to identify linkage values to add a vehicle information in the CRL if misbehaviour detected on that vehicle [34]. In this system, authorised vehicles rely on PC to validate and au-

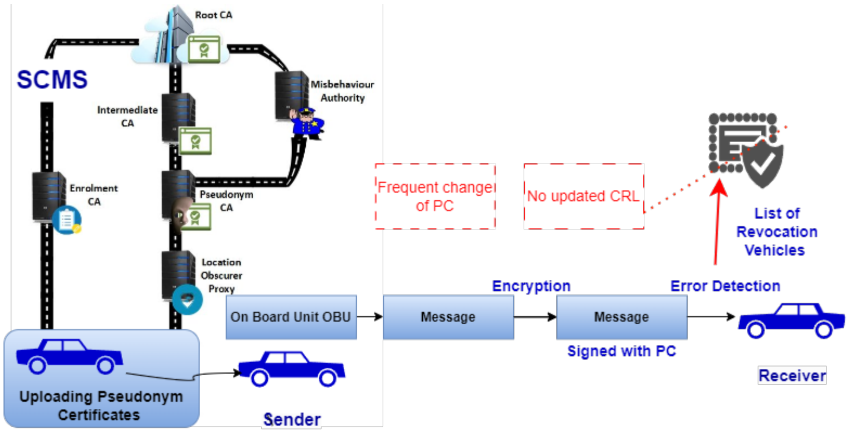


Fig. 2. Challenges of SCMS in Offline V2V Communication

thenticate the trustworthiness of messages. The SCMS provides the vehicle with multiple PCs and requires vehicles to change them periodically.

Pseudonym Certificates: To ensure message integrity, authentication, and vehicle privacy, PCs are utilized, typically issued by the PCA in the SCMS. PCs are employed for short durations to safeguard privacy, and they are changed periodically, such as every 5 minutes, to prevent message linkability. To facilitate the pseudonym-changing process, the SCMS system provides the vehicle with necessary PCs. These PCs can be preloaded with varying periods for an extended time (e.g., one year) or obtained on-demand (e.g., daily). Vehicles have the capability to refill PCs either online or offline. While in online mode, vehicles can directly download PCs on-demand using RSUs [34]. In offline mode, the PCA supplies all PCs to the vehicle regularly, necessitating ample storage capacity.

3 System Model

This section describes the proposed model and the roles and assumptions. Figure 3 illustrates our proposed addition to the SCMS architecture (see previous section). 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.

The RS has the capability to associate a vehicle's identity with its corresponding RV, ensuring privacy while facilitating efficient reputation management. This approach allows the vehicle to maintain its anonymity while still benefiting from reputation-based services. However, the detailed feedback mechanism, which en-

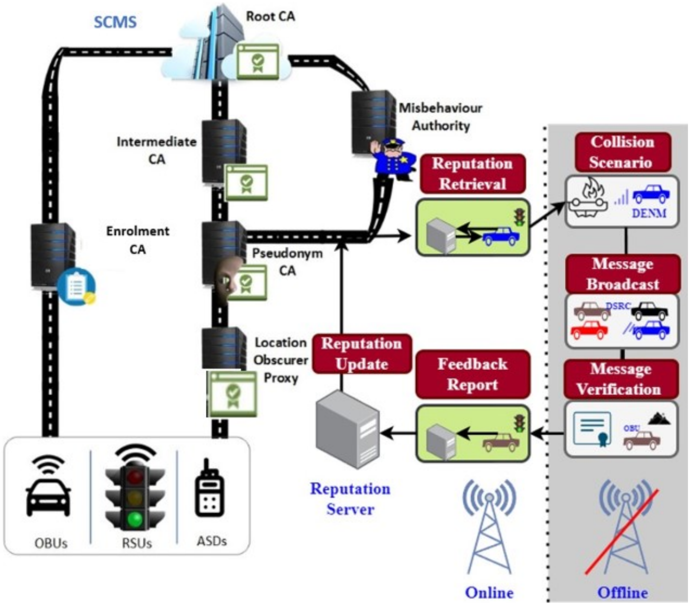


Fig. 3. Proposed System Model

compasses the historical information used to determine a specific RV, falls outside the scope of our current discussion [21]. The proposed scheme provides a secure way of attaching a reputation score to PCs without compromising the privacy of the vehicles. Furthermore, it ensures that the RV is tamper-proof and can only be used by the vehicle. This approach also enables efficient reputation management, allowing fast retrieval of RVs from the RS. The roles and operations of the key entities in the proposed architecture are as follows:

Vehicles: In an offline setting, vehicles act as end users and communicate with neighbouring vehicles. Trust between vehicles is not assumed. Upon receiving a message, a vehicle assesses its reliability before proceeding. Vehicles are equipped with On Board Units (OBUs) that facilitate wireless communication with neighbouring OBUs. Trusted hardware within the OBUs securely stores keys and handles cryptographic operations [22].

Reputation Server: We propose a centralised RS considered a trusted authority. The RS's primary role is to manage the vehicle's reputation. This role comprises, gathering, and aggregating multiple reputation-related reports from vehicles to form an RV, then distributing a new RV to vehicles.

Vehicles can set up a secure channel with the RS using TLS [25]. The vehicle and the RS can exchange authentication credentials to establish a secure connection. Once the secure session is established, the vehicle can send its reputation requests to the server and receive responses securely. In addition, the secure channel ensures that the data exchanged between the vehicle and the server is not tampered with or accessed by malicious actors.

4 Novel Signature Scheme

In SCMS, a vehicle's PCs allow other vehicles to be confident that the messages originate from that vehicle, and has 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 reputation certificate itself breaks privacy if it is reused. An alternative 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 [37].

In this section, we introduce a special two-step signature scheme that addresses this privacy/scalability compromise. Many variations of regular signature schemes exist, to name a few: ring signatures [10], group signatures [15], delegatable signatures [35], blind signatures [1], or proxy signatures [16]. 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.

4.1 *Pre-Signature* Scheme

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.

Due to space constraints, we assume familiarity with certain concepts such as cryptographic hardness. These are taken with the usual definitions, see e.g. [17].

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

- $(pk, sk) = \mathrm{keygen}(\ell)$*: I generates a public/private key pair with a security parameter ℓ, then keeps sk secret and distributes pk.*
- $(k, \{(b_i, v_i)\}_{i=1}^{n}) = \mathrm{register}(P, n)$*: 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, sends $S_P \coloneqq \{(b_i, v_i)\}_{i=1}^{n}$ to P, and $\{v_i\}_{i=1}^{n}$ to V.*
- $\sigma = \mathrm{presign}(m, P)$*: I pre-signs a message m and sends it to P.*
- $\bar{\sigma} = \mathrm{complete}(\sigma, b)$*: P chooses a blinding key b and completes a pre-signature σ, then sends it to V. In practice, the completed signature is also accompanied with an indicator for the corresponding verification code v.*
- $\mathrm{verify}(\bar{\sigma}, m, v)$*: V verifies completed signature $\bar{\sigma}$ of message m using the associated verification code v.*

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* $(k, S_P) = \text{register}(P, n)$*,*

$$\text{verify}(\text{complete}(\text{presign}(m, P), b), v) = \mathit{True} \iff \exists (b, v) \in S_P.$$

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

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

Indistinguishability *Let* $\sigma_0 = \text{presign}(m_0, P_0)$*,* $\bar{\sigma}_0 = \text{complete}(\sigma_0, b_0)$*,* 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*.*

4.2 RSA-based Instantiation

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 $v_i = (kb_i)^e \pmod N$.
- presign: $\sigma = h(m)^d k \pmod N$, with k the hidden key associated with P, and h a secure hash function.
- complete: $\bar{\sigma} = \sigma b \pmod N$.
- verify: $\bar{\sigma}^e \overset{?}{\equiv} h(m)v \pmod N$.

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

Proof (sketch). 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.

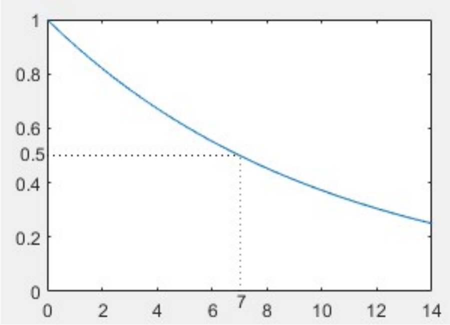


Fig. 4. Decay of Reputation Over Time

5 Reputation System in an Offline Context

This section presents a reputation system for offline vehicular networks based on the *Pre-Signature* scheme. It includes reputation calculation, initialization and synchronization of reputation, offline demonstration of fresh reputation, and vehicle privacy considerations.

5.1 Reputation Value

Reputation in V2V enhances communication reliability and effectiveness by identifying reliable messages and detecting vehicle misbehavior [26]. It does this in a more finegrained way than CRLs can. In addition, CRLs are not designed for offline settings. This work follows some established reputation assumptions in V2V [5, 11, 21, 36], for estimating reliability based on feedback from communications.

We assume that there is a reputation server (RS) that has a precise trust opinion. This trust opinion may simply be a single value, but may be more complex, e.g. like in Subjective Logic [4]. Vehicles can request a reputation value (RV), which is a numerical value between 0 and 1, derived from the RS's trust opinion. The message with the RV can be used in an offline setting to evidence its trustworthiness.

There is no mechanism to force vehicles to request an updated RV. A vehicle could request an RV when it is high, then misbehave, and simply not update the RV after it drops. This is a reputation lag attack [30]. To mitigate reputation lag, reputation values should decay. We propose a geometric decay rate with a half-life of a week, or about -9.43% per day. Taking the time units in days, after d days, an initial reputation of r_0 is decayed to $r = r_0 \cdot 2^{-d/7}$. This exponential decay pattern as explained in [8] ensures that reputation gradually diminishes over time. The decay is depicted in Figure 4.

To compute the current reputation using the formula above, one would need to have the initial reputation and the timestamp of the message. However, as the decay is geometric, there exists an offset o, such that $r_0 \cdot 2^{-d/7} = 2^{-\frac{d+o}{7}}$, for all d. In fact, this occurs when $r_0 = 2^{-o/7}$ or $o = -7\log_2(r_0)$. Using this technique,

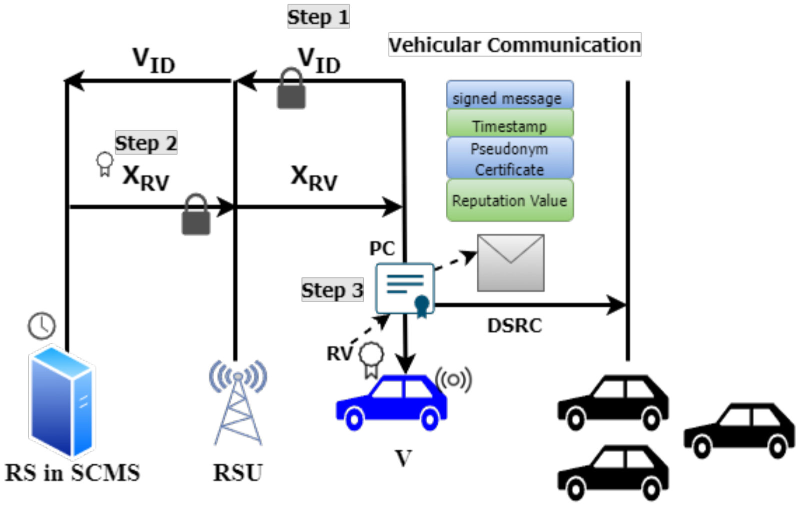


Fig. 5. Reputation Scheme Steps in SCMS

we can send the reputation value using only a timestamp – which is $7\log_2(r_0)$ days in the past – and implicitly have $r_0 = 1$. Hence, the value that will be sent is a timestamp TS.

We want the entropy of the timestamp to be low. After all, if someone notices that two timestamps are equal to the millisecond, then this may hint that its the same vehicle under a different pseudonym. Therefore, we round TS to the nearest day. So, if today is T, then $TS = T - \text{round}(7\log_2(r_0))$. The vast majority of vehicles will be using a 'date corresponding to the last couple of days.

The reputation value RV can be computed as $RV = 2^{-\frac{T-TS}{7}}$. And RV will approximately equal the corresponding reputation value r_0 in the RS. As intended, the derived RV will decrease by about 10% per day, as T increases by 1 every day, giving us the desired half-life of 7 days. Of course, the scheme can be adjusted to decay faster or slower, or have more or less granular timestamps.

In the employed decay system, the RV follows an exponential decay pattern, approaching zero without ever becoming negative. However, having a low reputation, say $RS < 1/4$, is not particularly impactful. Therefore, we specify that honest vehicles should not be using timestamps longer than 14 days ago, as $-7\log_2(1/4) = 14$.

5.2 Reputation Initialisation and Synchronisation

Each vehicle is assigned a unique identifier called the Vehicle ID V_{ID} and a pair of public/secret key V_{PK}/V_{SK}. These keys are essential for the reputation retrieval process:

In this process: the RS creates and stores a *hidden key* V_K, and generates the verification codes PC_{VC} and blinding keys PC_B for the each of the certificates

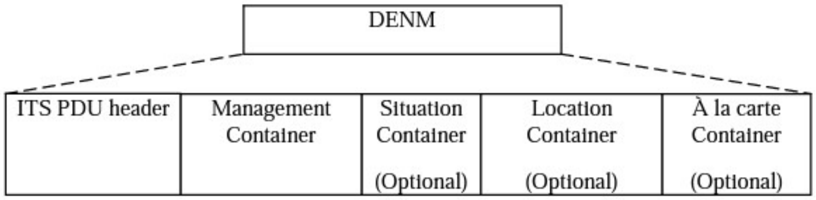

DENM
ITS PDU header
Management Container
Situation Container (Optional)
Location Container (Optional)
À la carte Container (Optional)

Fig. 6. The Structure of a DENM message

PC. The RS does not need to store the blinding keys, but only needs to store an association between V_{ID} and V_K.

Figure 5 describes the main steps in the reputation scheme as follows:

Step 1: When vehicle V contacts an RSU, it can request a reputation synchronisation. The vehicle will send its V_{ID} securely to the RSU. The RSU will then send the vehicle's request to RS.

Step 2: The RS calculates the value $TS = CT - \text{round}(7 \log_2(RV))$, where CT is the current time and RV the reputation of V found in its database. The RS then pre-signs the value TS, as $\sigma_{RS,V}(TS)$.

Step 3: The vehicle sets $V_{PS} = \sigma_{RS,V}(TS)$, so it can use the pre-signature later.

5.3 Vehicular Communication

The vehicle V_{send} wants to send the message M to vehicle V_{rcv}, using a specific PC. The message M follows the standards Decentralized Environmental Notification Message ($DENM$) and contains information such as location, time, type of message, and message contents [12]. The DENM structure is depicted in Figure 6. The message needs to be signed with the private key PC_{SK}, so that the public key PC_{PK} on the certificate can verify it.

We further introduce an additional signature to be included, based on the pre-signature scheme: V_{send} creates the completed signature $\bar{\sigma}_{RS,PC}(TS)$, using the blinding key PC_B and the stored pre-signature. For a message M, with pseudonym PC, and reputation RV, V_{send} needs to send:

$$(\sigma_{PC_{SK}}(M), PC, \bar{\sigma}_{RS,PC}(TS)) \tag{1}$$

As with normal DENM operation, the receiving vehicle V_{rcv} can verify that the certificate PC was issued by a trusted PCA. Additionally, it can verify that the owner of PC has correctly signed the message M, guaranteeing integrity and authentication w.r.t. the pseudonymous identity. In our proposed approach, vehicle V_{rcv} can furthermore verify (using the completed signature and the verification code on PC) that RS has provided evidence of a certain timestame TS for vehicle V_{send}, and thus of reputation $RV = 2^{-\frac{T-TS}{7}}$ on day T.

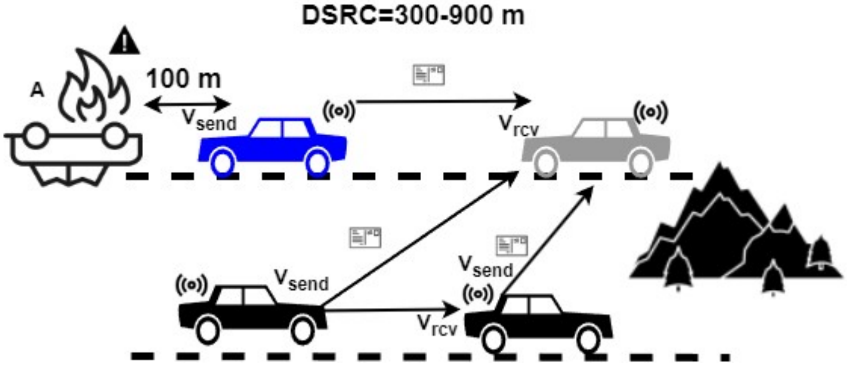


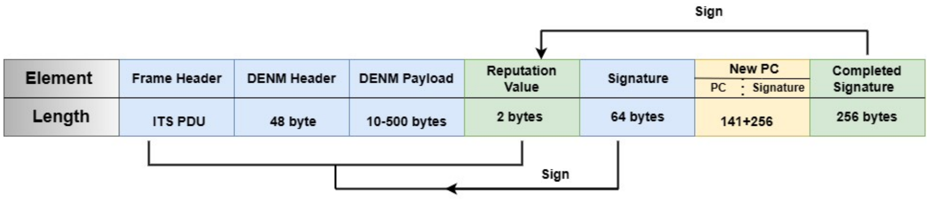
Fig. 7. Emergency Communication Scenario

In the context of the DENM system, Vehicle V_{send} generates the message M in DENM format. The DENM system is event-driven, and is meant to be used to identify safety issues (e.g., collision, obstacles, etc.). V_{send} sends M in hop-by-hop transmission format through the DSRC to neighbour vehicles in the same area. After receiving message M, the receiving vehicle V_{rcv} submits M to its OBU and verifies the message's reliability. Figure 7 shows the emergency communication in an offline scenario.

The OBUs authenticate the message and the TS by verifying the source of the message and its integrity. Vehicle V_{rcv} receive many messages regarding the collision. In case of conflicting information, V_{rcv} has to decide which message is correct. To support V_{rcv} in making the right decision, each sources reputation value can be used and compared. The RV provides additional information to help V_{rcv} make a more informed decision about the accurate message. By comparing the RV of the vehicles, V_{rcv} can determine which message is more likely to be accurate. If verified, V_{rcv} forwards M to its neighbour vehicles in the same area. The also interpret the message content and take appropriate safety measures. What (if any) actions to undertake may depend on the RV of the source.

5.4 Vehicle Privacy

The adoption of our system introduces three potential avenues of reducing privacy: discernible patterns in verification codes, recognising that two completed signatures are based on the same pre-signature, and recognition of identical messages. However, verification codes are chosen at random, and we proved indistinguishability of completed signatures (Section 4). Therefore, the only avenue in which privacy may be reduced, is by recognising the messages are identical. The message is a date TS within the last two weeks. This means we have 15 possible message values. While matching TS values may hint that two PCs are from the same vehicle, there will be many vehicles using the same TS. Our scheme trades off reputation accuracy and privacy, but both the reputation accuracy is sufficiently high and the privacy is safeguarded, with the values we use. Overall, our



Element	Frame Header	DENM Header	DENM Payload	Reputation Value	Signature	New PC PC : Signature	Completed Signature
Length	ITS PDU	48 byte	10-500 bytes	2 bytes	64 bytes	141+256	256 bytes

Fig. 8. DENM message signed by*Pre-Signature*

scheme combines uses robust RSA encryption to enhance trustworthiness and resilience in V2V communication.

6 Operational Considerations

In this section, a detailed analysis is conducted to assess the cost and overhead of the proposed scheme. This evaluation focuses on the additional communication and signing/verification processes introduced by the scheme in comparison to existing systems. The following technical aspects are examined:

6.1 RS to Vehicle

Efficient retrieval of RVs from the RS in offline areas requires evaluating communication overhead. V2I scenarios use a specific message exchange protocol [6]. and employ DSRC with parameters like a 256-byte reputation response, 300-meter transmission range, 6 Mbps data rate, and one daily handshake. This ensures minimal overhead in bandwidth and latency, resulting in exceptionally efficient communication between vehicles and the RS.

6.2 V2V Communication

Within the context of DENM messages, which adhere to the ETSI standard for Intelligent Transport Systems [9], size considerations play a crucial role. These messages are subject to a maximum size limit of 3,072 bytes, encompassing various components such as frame size, header size, payload size, and total message size. Figure 8 visually illustrates the integration of additional components introduced by the *Pre-Signature* scheme into the DENM. These components include updating the *PC* with a pre-signature, resulting in a size increase of 256 bytes, and signing the 2-byte *RV* with the completed signature, adding another 256 bytes. Therefore, the total size is increased by 514 bytes. The cumulative size increase amounts to approximately 0.50 kilobytes. While this is a substantial relative increase in size, it is important to consider the bandwidth capabilities of DSRC, which operates in the licensed 5.9 GHz band and is based on IEEE 802.11p [13], where half a kilobyte is not substantial.

The *Pre-Signature* scheme incurs minimal communication overhead compared to alternative signature schemes [3, 24, 29], making it an effective solution for generating digital signatures in offline setting.

6.3 Computation Overhead

The *Pre-Signature* scheme demonstrates minimal communication overhead in terms of signing and verification operations. Verification operations are not significantly impacted due to the faster nature of RSA verification compared to ECDSA verification [14]. This is attributed to the inherent computational efficiency of RSA, resulting in minimal overhead during the verification process.

Similarly, the signing operations in the *Pre-Signature* scheme exhibit favourable performance characteristics. The additional signature, referred to as the *completed* signature, involves a simple multiplication modulo N, which can be performed efficiently. As a consequence, the inclusion of the completion signature does not introduce substantial overhead during the signing process. Considering both signing and verification, the *Pre-Signature* scheme maintains an efficient computation overhead. This characteristic makes it well-suited for secure communication in offline environments, offering an optimal balance between cryptographic robustness and computational efficiency.

7 Related Work

Existing literature can be classified into reputation in V2V communications and SCMS for V2V communications. Here, we provide a brief overview of these areas:

V2V Reputation Systems: The reputation system in V2V is classified as centralized and decentralized. The centralized system was first introduced by Li et al [21]; this work is based on the centralized reputation scheme that centrally disseminates, update, and store vehicles' reputation scores. In their work, a reputation announcement scheme for VANETs based on Time Threshold was designed to evaluate message reliability. A recent centralized reputation system for highways and urban roads was proposed by Cui et al. [5]. They assumed that the central Trusted Authority is the solution to calculate the feedback scores from different vehicles and then update the target's reputation value. Meanwhile, Khalid et al [18] suggest a method of incentive provisioning built on the idea that the RSU updates the sender's reputation score based on the observed action validated by vehicles.

On the other hand, distributed reputation systems do not rely on infrastructure. Instead, vehicles collect, maintain, and update the reputation score in an ad hoc mode. El et al. [7] designed a node reputation system to evaluate the reliability of both vehicles and their messages: Vehicles that are close to each other and have the same mobility patterns are grouped into a platoon to reduce propagation overhead. Kudva et al [20] suggested a framework of self-organized vehicles to filter the malicious vehicles based on the standard score.

SCMS for V2V Communications: Prior studies have investigated a PKI-based security infrastructure system SCMS. While the system is designed to provide secure authentication, authorization, and data integrity for V2V communication, several related issues as indicated by [19], [28] , must be solved. For example, in SCMS, each vehicle receives 20 certificates each week to sign the messages with the PCs that rotating every 5 minutes [33]. As a result, every 100 minutes, a vehicle will utilise a fresh set of 20 PCs. In this case, SCMS may analyse all the PCs a vehicle uses in a single day and then utilise them to track for a week. Although the SCMS system assures who signed those PCs, proving how correct or reliable the messages provided from the vehicle is challenging. Moreover, the revocation process of certificates for malicious vehicles would need the distribution of CRLs to all enrolled vehicles, which would take time and bandwidth. In this case, each vehicle must receive an updated CRL copy in a timely and secure manner, making the transfer of CRL in offline areas challenging and not successfully guaranteed. Hence, more than relying on the SCMS to identify the misbehaving vehicles is required in some scenarios.

8 Conclusion

One of the main challenges in V2V communications is finding the right balance between security, privacy, and efficiency. Our proposed solution aims to enhance trust and reliability in V2V communication in offline settings. We address the need for authenticating messages while maintaining privacy by leveraging pseudonym certificates (SCMS style) and introducing a reputation system. We introduce the pre-signature cryptographic primitive. Vehicles can request fresh pre-signatures of their reputation values (via a timestamp) daily, ensuring offline verification without compromising privacy. Our approach offers scalability, reduced overhead compared to Certificate Revocation Lists, and a more granular assessment of misbehavior in V2V communication. Future work entails exploring alternative cryptographic primitives to reduce the size of the signatures and verification codes, to reduce V2V communication overhead. Further, we plan to use realistic, state-of-the-art simulation tools to test and validate our work for large-scale V2V communication networks.

References

1. Agustina, E.R., Hakim, A.R.: Secure vanet protocol using hierarchical pseudonyms with blind signature. In: 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). pp. 1–4. IEEE (2017)
2. 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: 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall). pp. 1–7. IEEE (2019)
3. Bindel, N., McCarthy, S., Twardokus, G., Rahbari, H.: Drive (quantum) safe!–towards post-quantum security for v2v communications. Cryptology ePrint Archive (2022)
4. Cheng, T., Liu, G., Yang, Q., Sun, J.: Trust assessment in vehicular social network based on three-valued subjective logic. IEEE Transactions on Multimedia **21**(3), 652–663 (2019)
5. 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 Transactions on Information Forensics and Security **15**, 1654–1667 (2019)

6. Dey, K.C., Rayamajhi, A., Chowdhury, M., Bhavsar, P., Martin, J.: Vehicle-to-vehicle (v2v) and vehicle-to-infrastructure (v2i) communication in a heterogeneous wireless network–performance evaluation. Transportation Research Part C: Emerging Technologies **68**, 168–184 (2016)
7. El Sayed, H., Zeadally, S., Puthal, D.: Design and evaluation of a novel hierarchical trust assessment approach for vehicular networks. Vehicular Communications **24**, 100227 (2020)
8. ElSalamouny, E., Krukow, K.T., Sassone, V.: An analysis of the exponential decay principle in probabilistic trust models. Theoretical computer science **410**(41), 4067–4084 (2009)
9. Festag, A.: Cooperative intelligent transport systems standards in europe. IEEE communications magazine **52**(12), 166–172 (2014)
10. Fujisaki, E., Suzuki, K.: Traceable ring signature. In: Public Key Cryptography–PKC 2007: 10th International Conference on Practice and Theory in Public-Key Cryptography Beijing, China, April 16-20, 2007. Proceedings 10. pp. 181–200. Springer (2007)
11. Gyawali, S., Qian, Y., Hu, R.Q.: Machine learning and reputation based misbehavior detection in vehicular communication networks. IEEE Transactions on Vehicular Technology **69**(8), 8871–8885 (2020)
12. Ha, S., Yoo, W., Kim, H., Chung, J.M.: C-v2x adaptive short-term sensing scheme for enhanced denm and cam communication. IEEE Wireless Communications Letters **11**(3), 593–597 (2021)
13. Hafeez, K.A., Zhao, L., Ma, B., Mark, J.W.: Performance analysis and enhancement of the dsrc for vanet's safety applications. IEEE Transactions on Vehicular Technology **62**(7), 3069–3083 (2013)
14. Jansma, N., Arrendondo, B.: Performance comparison of elliptic curve and rsa digital signatures. nicj. net/files (2004)
15. Jiang, Y., Ge, S., Shen, X.: Aaas: An anonymous authentication scheme based on group signature in vanets. IEEE Access **8**, 98986–98998 (2020)
16. Kanchan, S., Chaudhari, N.S.: Srcpr: Signrecrypting proxy re-signature in secure vanet groups. IEEE Access **6**, 59282–59295 (2018)
17. Katz, J.: Cryptographic Hardness Assumptions, pp. 35–66. Springer US, Boston, MA (2010)
18. Khalid, A., Iftikhar, M.S., Almogren, A., Khalid, R., Afzal, M.K., Javaid, N.: A blockchain based incentive provisioning scheme for traffic event validation and information storage in vanets. Information Processing & Management **58**(2), 102464 (2021)
19. Khan, S., Zhu, L., Yu, X., Zhang, Z., Rahim, M.A., Khan, M., Du, X., Guizani, M.: Accountable credential management system for vehicular communication. Vehicular Communications **25**, 100279 (2020)
20. Kudva, S., Badsha, S., Sengupta, S., Khalil, I., Zomaya, A.: Towards secure and practical consensus for blockchain based vanet. Information Sciences **545**, 170–187 (2021)
21. Li, Q., Malip, A., Martin, K.M., Ng, S.L., Zhang, J.: A reputation-based announcement scheme for vanets. IEEE Transactions on Vehicular Technology **61**(9), 4095–4108 (2012)
22. Naskath, J., Paramasivan, B., Aldabbas, H.: A study on modeling vehicles mobility with mlc for enhancing vehicle-to-vehicle connectivity in vanet. Journal of Ambient Intelligence and Humanized Computing **12**, 8255–8264 (2021)

23. Rahman, N.A., Jamlos, M.A., Jamlos, M.F., Soh, P.J., Bahari, N., Hossain, T.M.: Compact bidirectional circularly polarized dedicated short range communication antenna for on-board unit vehicle-to-everything applications. International Journal of RF and Microwave Computer-Aided Engineering **30**(5), e22174 (2020)
24. Ramakrishnan, M., et al.: Signature based v2x communication and authentications using resourceful signcryption and optimised ecc. IEEE Transactions on Intelligent Transportation Systems (2023)
25. Rescorla, E., Dierks, T.: The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Aug 2008). https://doi.org/10.17487/RFC5246, https://www.rfc-editor.org/info/rfc5246
26. Samara, G.: Intelligent reputation system for safety messages in vanet. arXiv preprint arXiv:2007.12717 (2020)
27. Shurrab, M., Singh, S., Otrok, H., Mizouni, R., Khadkikar, V., Zeineldin, H.: An efficient vehicle-to-vehicle (v2v) energy sharing framework. IEEE Internet of Things Journal **9**(7), 5315–5328 (2021)
28. 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: 2018 IEEE Vehicular Networking Conference (VNC). pp. 1–8. IEEE (2018)
29. Singh Sehrawat, V., Shah, Y., Choyi, V.K., Brusilovsky, A., Ferdi, S.: Certificate and signature free anonymity for v2v communications. arXiv e-prints pp. arXiv–2008 (2020)
30. Sirur, S., Muller, T.: The reputation lag attack. In: Trust Management XIII: 13th IFIP WG 11.11 International Conference, IFIPTM 2019, Copenhagen, Denmark, July 17-19, 2019, Proceedings 13. pp. 39–56. Springer (2019)
31. Sukuvaara, T., Nurmi, P.: Wireless traffic service platform for combined vehicle-to-vehicle and vehicle-to-infrastructure communications. IEEE Wireless Communications **16**(6), 54–61 (2009)
32. Tao, R., Wolleschensky, L., Weimerskirch, A.: Security certificate management system for v2v communication in china. SAE International Journal of Transportation Cybersecurity and Privacy **2**(11-02-02-0015), 169–183 (2019)
33. Verheul, E., Hicks, C., Garcia, F.D.: Ifal: Issue first activate later certificates for v2x. In: 2019 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 279–293. IEEE (2019)
34. Whyte, W., Weimerskirch, A., Kumar, V., Hehn, T.: A security credential management system for v2v communications. In: 2013 IEEE Vehicular Networking Conference. pp. 1–8. IEEE (2013)
35. Xu, S., Yang, G., Mu, Y.: A new revocable and re-delegable proxy signature and its application. Journal of Computer Science and Technology **33**, 380–399 (2018)
36. Xu, X., Wang, Y., Qin, H., Zhang, J., Yan, M., Ji, H.: Secured authentication method in v2x communication scenario. In: CICTP 2020, pp. 2916–2927. CICTP (2020)
37. Zeddini, B., Maachaoui, M., Inedjaren, Y.: Security threats in intelligent transportation systems and their risk levels. Risks **10**(5), 91 (2022)
38. Zhang, T., Tao, D., Qu, X., Zhang, X., Lin, R., Zhang, W.: The roles of initial trust and perceived risk in public's acceptance of automated vehicles. Transportation research part C: emerging technologies **98**, 207–220 (2019)