Reconfigurable Intelligent Surface-Assisted Cross-Layer Authentication for Secure and Efficient Vehicular Communications

Mahmoud A. Shawky, Syed Tariq Shah, *Member, IEEE*, Ahmed G. Abdellatif, Muhammad A. Imran, *Fellow Member, IEEE*, Qammer H. Abbasi, Shuja Ansari, *Senior Member, IEEE*, and Ahmad Taha, *Member, IEEE*

***Abstract*—Intelligent transportation systems increasingly depend on wireless communication for broadcasting traffic messages and facilitating real-time vehicular communication. In this context, message authentication is crucial for establishing secure and reliable communication. However, security solutions must consider the dynamic nature of vehicular communication links, which fluctuate between line-of-sight (LoS) and non-line-of-sight (NLoS) due to obstructions. This paper proposes a lightweight cross-layer authentication scheme that employs public-key infrastructure (PKI)-based authentication for initial legitimacy detection/handshaking while using key-based physical-layer re-authentication for message verification. This approach reduces signature generation and signaling overheads associated with each transmission, thereby enhancing network scalability. However, the receiver operating characteristic (ROC; P_d: detection vs. P_{FA}: false alarm probabilities) of the latter decreases with lower signal-to-noise ratio (SNR). To address this, we investigate the use of reconfigurable intelligent surfaces (RISs) to strengthen the SNR directed toward the designated vehicle in shadowed areas (i.e., NLoS scenarios), thereby improving the ROC. Theoretical analysis and practical implementation are conducted using a 1-bit RIS consisting of 64×64 reflective metasurfaces. Experimental results show a significant improvement in P_d, increasing from 0.82 to 0.96 at SNR = -6 dB for an orthogonal frequency-division multiplexing (OFDM) system with 128 subcarriers. We also conducted informal and formal security analyses using Burrows-Abadi-Needham (BAN) logic to prove the scheme's ability to resist passive and active attacks. Furthermore, the proposed scheme reduces computational and communication overheads by 43% and 13%, respectively, compared to traditional cryptographic methods, demonstrating its superiority for real-time, challenging communication scenarios.**

***Index Terms*—AVISPA simulation, BAN-Logic analysis, Cross-layer authentication, Public key infrastructure, Reconfigurable intelligent surface, Random oracle modelling.**

I. Introduction

Road traffic accidents cause 1.35 million fatalities annually, resulting in about 3,700 deaths per day, and it is expected to rank fifth among the causes of death by 2030 [1]. To address this issue, the World Health Organization has recognised the importance of developing intelligent transportation systems that enable real-time communication from vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) [2]. Vehicular ad-hoc networks (VANETs) generally consist of three primary components: a trusted authority (TA), roadside units (RSUs), and wireless communication devices located on vehicles, also known as onboard units (OBUs) [3]. Each vehicle transmits a safety-related message containing information on location, speed, and heading at a transmission rate of $100 - 300$ $msec$ [4]. This significantly enhances the performance of many traffic-related applications, including safety, mobility, and autonomy. Moreover, it reduces the carbon footprint and facilitates green transportation. However, the open-access nature of wireless communication makes it vulnerable to typical attacks, such as impersonation and modification. Hence, message authentication is crucial in preventing such attacks [5].

Generally, there are three common types of authentication in VANETs: public key infrastructure (PKI)-based, identity (ID)-based, and group signature (GS)-based [3]. In PKI-based authentication, each vehicle has a pair of private and public keys [6]. The private key is used to generate digital signatures on messages. For verification, the public key is attached to the transmitted message as a digital certificate signed by the TA. In ID-based authentication, the vehicle's identifier, such as the vehicle identification number, is used as its public key, which can verify signatures generated by the vehicle's private key. This approach eliminates the need for a separate public key infrastructure, as the identifier serves as the public key [7]. In GS-based authentication, group members generate the signature (σ) on behalf of the group using their secret keys, while the recipient verifies σ using the group's public key [8]. The signature is generated so that it cannot be traced back to the specific member who generated it, offering anonymity and privacy preservation. However, these methods require complex cryptographic operations, leading to high computation and communication costs for transmitting and verifying messages.

To overcome this limitation, physical (PHY)-layer authentication techniques have emerged as a promising solution to reduce the overheads associated with upper-layer cryptographic approaches [9]. These techniques employ the unique features of wireless channels, such as channel amplitude and phase responses [10], and the hardware impairments, such as analogue front-end imperfections and carrier frequency offset [11], to discriminate between terminals. Interested readers in this topic are referred to [12]–[15], where Chen et al. [12], [13]

M.A. Shawky, M.A. Imran, Q.H. Abbasi, S. Ansari, and A. Taha {mahmoud.shawky, Muhammad.Imran, Qammer.Abbasi, Shuja.Ansari, Ahmad.Taha}@glasgow.ac.uk are with the James Watt School of Engineering, University of Glasgow, UK. A.G. Abdellatif {ag.abdellatef@zu.edu.eg} is with the Department of Communications and Electronics Engineering, Air Defense College, EMA, Cairo, Egypt. S.T. Shah {syed.shah@essex.ac.uk} is with the School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK.

introduce a secure PHY-layer message authentication mechanism, regardless of the computation availability of adversaries. The work presented in reference [14] introduces an innovative message authentication scheme that integrates a secure channel coding mechanism. This mechanism leverages random coding techniques to effectively identify potential man-in-the-middle (MITM) attacks. Reference [15] presents a keyless authentication methodology characterised by a high authentication rate, thereby enhancing network scalability. However, PHY-layer methods cannot be alternative to crypto-based methods due to challenges in extracting distinguishing features or channel attributes in hardware impairments-based and feature-based approaches. Additionally, observing all communicating terminals' secret features within a limited coherence period and dealing with minor differences between hardware impairments remain significant challenges. For more details, refer to [32].

In this context, integrating the PHY-layer into the upper-layer authentication approaches enhances the network's security and scalability, introducing what is referred to as "cross-layer authentication" [16]. In VANETs, the concept of cross-layer authentication is inspired by human interaction dynamics, wherein individuals are initially identified and subsequently remembered based on distinct physical traits like facial attributes, body structure, vocal characteristics, and other distinguishing qualities. Similarly, dependable and secure communication within vehicular networks can be established through an initial handshake procedure that integrates cryptographic authentication. This pivotal step assumes a critical role in verifying the authenticity of participating vehicles and capturing distinctive features of wireless devices, which can subsequently serve for ongoing re-authentication during forthcoming transmissions [17]. By combining PHY-layer features with upper-layer cryptographic techniques, this cross-layer authentication approach significantly reduces both computational and communication overheads. Unlike traditional methods that require generating and transmitting digital signatures with every message, an often costly process in terms of processing time and bandwidth, this methodology limits complex cryptographic operations to the initial handshake phase. Subsequent message verifications rely on lightweight PHY-layer re-authentication, which exploits unique wireless channel characteristics inherent to each vehicle. This reduces the frequency and complexity of cryptographic computations and decreases the amount of additional signaling data exchanged across the network [32]. As a result, the approach enhances network scalability and responsiveness, which are critical for real-time vehicular communication systems operating under stringent resource constraints. However, the performance of PHY-layer-based techniques in terms of detection and false alarm probabilities depends on the signal-to-noise ratio (SNR). The higher the SNR, the higher the detection probability, and vice versa. Considering the significant wireless channel variations and the instability of vehicular communication links caused by unpredictable obstructions, the re-authentication performance can be adversely affected, posing a challenge.

Reconfigurable intelligent surfaces (RISs) has emerged as a novel class of planar meta-material structures that can manipulate and reflect incident electromagnetic waves through dynamic surface property adjustments [18]. By controlling the electromagnetic waves' reflection and scattering, RISs can enhance wireless communication systems' SNR values and improve PHY-layer re-authentication performance. Following is a summary of this paper's contributions:

1) This paper proposes a novel pseudo-identity-based PHY-layer re-authentication scheme that complements the initial PKI-based legitimacy detection. This approach significantly reduces the need for computationally expensive cryptographic signature generation and transmission for every message, thereby reducing communication and computation overheads without compromising the security and privacy requirements of VANETs.
2) To overcome the challenges posed by dynamic and obstructed vehicular communication channels, we introduce the use of RIS to actively strengthen the signal quality in NLoS scenarios. We rigorously verify this enhancement via both theoretical analysis and real-world experimentation using a 1-bit RIS with 64×64 reflective units, demonstrating a significant improvement in detection probability from 0.82 to 0.96 at an SNR of -6 dB.
3) We conduct comprehensive security analyses, including informal discussion and formal verification using Burrows-Abadi-Needham (BAN) logic, proving the scheme's resilience against passive and active attacks. Furthermore, performance evaluations quantitatively show that our scheme reduces computational and communication overheads by 43% and 13%, respectively, compared to traditional cryptographic methods, underscoring its suitability for real-time VANET applications, particularly in challenging channel conditions.

The structure of the remainder of this paper is as follows. Section II reviews relevant prior works. Section III presents the proposed scheme. Section IV analyses the scheme's security and privacy. Section V evaluates the scheme's performance. Finally, in Section VI, we provide concluding remarks.

II. Related works

This section reviews existing work on traditional authentication approaches and cross-layer authentication.

A. Traditional cryptographic signatures-based authentication

This part reviews current authentication designs that seek to alleviate the significant overheads inherent in traditional authentication methods in VANETs. Liu et al. [19] propose a proxy vehicle-based authentication scheme to mitigate the computational overhead on RSUs. This scheme adopts an ID-based approach, leveraging the computational resources of proxy vehicles to verify signatures on behalf of RSUs. However, Asaar et al. [20] demonstrated that the scheme in [19] is vulnerable to impersonation attacks. Unfortunately, in scenarios where proxy vehicles are unavailable, all signatures must be verified directly by RSUs, leading to increased computational and communication overheads. In [21], Jiang et al. propose using region trust authorities to deliver efficient vehicle authentication services while reducing the computational load of TA and RSUs. In [22], Lim et al.

propose a GS-based solution that addresses the overheads of the TA by introducing a hierarchical structure of RSUs comprising leader and member RSUs. The leader RSUs are empowered to generate group keys as group managers, thereby reducing the overheads on the TA. However, a compromised leader RSU can compromise the security and privacy of group members within the region. In [23], Shao et al. propose a batch verification-based authentication scheme that enables recipients to verify multiple received signatures simultaneously. However, the high computation complexity of bilinear pairing (BP) operations poses a significant challenge. Moreover, this method is susceptible to failure in the presence of a single invalid signature, which can lead to time-consuming singular verification.

Mohammed et al. [24] introduce a fog computing-based pseudonym authentication scheme utilising elliptic curve cryptosystem (ECC) and general hash functions to enhance privacy and security in fifth-generation (5G)-enabled vehicular networks. In [25], Cui et al. developed an ECC-based content-sharing scheme tailored for 5G-enabled vehicular networks. The authors' approach enables vehicles with content downloading requests to efficiently filter their nearby vehicles to select competent and suitable proxy vehicles. These selected proxy vehicles are then requested to provide content services. Wang et al. [26], Li et al. [27], and Almazroi et al. [28] proposed conditional privacy-preserving authentication schemes to reduce authentication overheads and promote privacy. By adopting these schemes, vehicles are not required to store any certificates for authentication, and the TA is also relieved of the need to retrieve the real identity of malicious vehicles from certificates. While the previously mentioned methods aim to achieve a higher authentication rate, many suffer from limited network scalability, highlighting the need for more effective solutions to meet the growing demands of vehicular communication systems.

B. An overview of cross-layer authentication

Wen et al. [16] patented a cross-layer authentication method that uses PKI-based authentication for handshaking and generates a radio frequency fingerprint for re-authentication. In [29]–[31], PKI-based authentication is integrated with the PHY-layer re-authentication using the feature tracking mechanism. This mechanism depends on the spatial and temporal correlation of the wireless channel responses within the coherence period T_c. Mughal et al. [17] propose an approach for incorporating the integrated circuits (ICs) physically unclonable function (PUF). Based on the IC's physical variation (P), the PUF method effectively generates an unpredictable response $R = P(C)$, where C is the input challenge. However, the scalability of hardware imperfections-based techniques is limited, as the false alarm probabilities increase with the number of terminals. This is due to the slight dissimilarities in the hardware impairments extracted features from different devices. For feature tracking-based techniques, the recipient must extensively observe all the communicating terminals' secret features within T_c, constituting a significant challenge. In this context, it is crucial to consider some parameters when selecting the PHY-layer re-authentication method. These include channel variations, broadcasting rates, computation availability, and communication ranges. In [32], we presented two re-authentication mechanisms: the PHY-layer signature-based identity authentication mechanism (PHY-SIAM) and the PHY-layer feature-tracking mechanism (PHY-FTM). PHY-SIAM is a keyed-based PHY-layer authentication mechanism where the message content is hashed and encapsulated into two orthogonal frequency-division multiplexing (OFDM) symbols. This forms the PHY-layer signature that can only be equalised at the intended receiver's side. PHY-FTM is a feature-tracking mechanism that utilises the high correlation between the channel estimates of subsequent OFDM symbols to verify message integrity. However, the previous study presented in [32] focused on the re-authentication performance for subsequent transmissions, assuming that the initial authentication was conducted during the first time slot.

C. An overview of RIS-assisted PHY-layer authentication

Recent studies have increasingly explored the integration of RISs into PHY-layer authentication (PLA), aiming to enhance security and robustness against adversarial attacks. These works demonstrate how RISs can be leveraged not only to improve wireless communication performance but also to provide new mechanisms for identity verification and attack resilience. For instance, Zhang et al. [33] propose a lightweight PLA framework for IoT devices in smart cities based on tag embedding and verification, demonstrating strong resistance to active attacks and highlighting the scalability of RIS-assisted security solutions. Crosara et al. [34] analyse divergence-minimizing attacks against challenge-response PLA (CR-PLA) in RIS-enabled environments. By modeling the adversary's optimal strategy through Kullback–Leibler divergence, they expose vulnerabilities that emerge under different channel knowledge and SNR conditions, revealing the limits of CR-PLA. Similarly, Tomasin et al. [35] introduce an environment-based CR-PLA paradigm where the verifier manipulates the electromagnetic environment, including RIS-assisted channels, to authenticate devices without explicit challenges, an approach that illustrates both opportunities and emerging threats.

Other works have focused on channel sparsity and cascaded features. Bendaimi et al. [36] exploit the double-structured sparsity of RIS-assisted MIMO channels to design robust channel-based PLA, achieving significant improvements in detection and false alarm rates compared to conventional methods. Zhang et al. [37] extend the tag-based approach by embedding cover tags constructed from intrinsic channel features, random signals, and cryptographic keys, validating their scheme's resilience against impersonation and tampering. He et al. [38] propose a generalised PLA scheme for RIS-assisted IoT that jointly exploits direct and cascaded channel features. Their analytical and numerical analysis shows enhanced detection performance across a wide range of system parameters. Beyond PLA, RIS has also been investigated for its role in key generation. Shawky et al. [39] propose an RIS-enabled secret key generation framework for secure vehicular communications under denial-of-service attacks, showing that

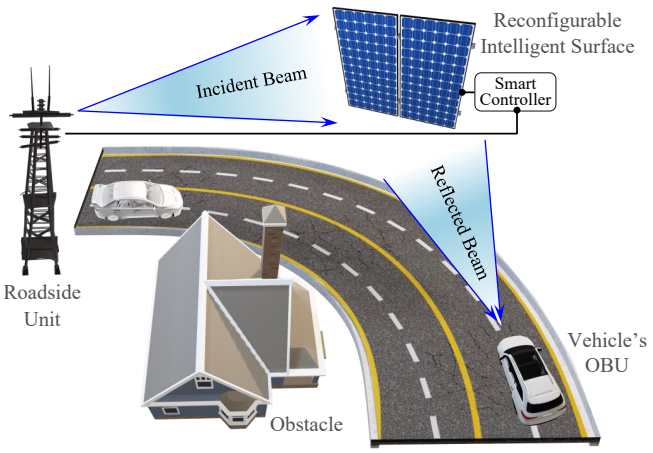


Fig. 1: System modelling.

RIS can simultaneously support authentication and robust key extraction in adversarial environments. Despite these advances, most existing studies remain simulation-based and rely on idealised assumptions, such as requiring network nodes to be separated by at least $\lambda/2$ to ensure feature uniqueness. However, this assumption can be undermined if an attacker is able to closely shadow a legitimate device and capture highly correlated channel features, thereby compromising the security strength of PLA. Furthermore, challenge-response mechanisms must typically operate within a short coherence interval T_c, which becomes particularly challenging in highly dynamic vehicular scenarios. To address these gaps, the present study proposes a comprehensive cross-layer authentication scheme that integrates PKI-based authentication for initial handshaking with a lightweight two-factor PHY-layer re-authentication process combining PHY-SIAM and PHY-FTM. Importantly, we also investigate how RIS can be utilised to further enhance re-authentication reliability, enhancing the detection probability of the PHY-layer re-authentication performance.

III. RIS-ASSISTED AUTHENTICATION: THE PROPOSED SCHEME

This section describes the system model, discusses the proposed scheme in detail, and explains how the RIS enhances the scheme's performance at low SNR values.

A. System modelling

The system model of the proposed RIS-assisted vehicular communication scheme is depicted in Fig. 1. The considered system model consists of the following entities.

- *TA*: The TA is a trusted entity for all network terminals, possessing sufficient computational resources to register and revoke any network terminal. It is also responsible for generating and distributing the system's public parameters. In addition, it is the only terminal capable of revealing vehicles' real identities in case of misbehaving (such as constructing an attack or violating traffic laws).
- *RSU*: The RSU authenticates vehicles within range by verifying their broadcasted messages. It is also assumed to have a reliable communication link with the RIS's smart controller, where it can control the phase shift of the RIS elements. The RSU aims to optimise the RIS's configuration to form a directed beam toward the communicating vehicle in the shadowed areas. Additionally, it functions as a relay between communicating vehicles, extending the V2V communication range.
- *Vehicle's OBU*: The OBU is a vehicle-mounted wireless communication device with limited computing capabilities. It can authenticate with nearby RSUs to send and receive real-time traffic conditions. We assume that both RSU and OBU are equipped with a single antenna.
- *RIS*: The RIS comprises L reconfigurable passive reflectors and is deployed to provide reliable communication links between the RSU and vehicles' OBUs (see Fig. 1). By doing so, the reflected signal towards the designated vehicle/RSU can be deliberately strengthened or impaired. Each RIS has a smart controller that allows the RSU to adjust the phase shift of the RIS reflecting units by choosing between different configuration patterns.

The notations used in this paper are summarised in Table I for ease of understanding.

B. The proposed authentication scheme

This section provides a detailed discussion of the proposed scheme. In this work, each terminal has a long-term digital certificate for initial verification and handshaking between two legitimate parties. For re-authentication and secure message verification between vehicles and RSUs, we use PHY-SIAM and PHY-FTM [32] as a two-factor re-authentication method for the OFDM system of N subcarriers. The handshaking process draws inspiration from conventional PKI-based mutual authentication, it significantly extends its capabilities through RIS-aware integration while satisfying the security and privacy requirement. These enhancements enable lightweight, low-latency, and physically resilient authentication tailored for dynamic vehicular environments. Generally, the proposed scheme comprises four phases, i.e., initialisation, registration, initial authentication, and message signing and verification.

1) System initialisation phase: The TA follows the following steps to initialise the system's public parameters.

- The scheme is designed based on the 80-bit security level of the elliptic curve $E : y^2 = x^3 + ax + b \bmod p$. In this context, we adopted the 160-bit elliptic curve, which is parameterised using the recommended domain settings of "$secp160k1$" [40], as listed in Table II.
- Based on the generator P, the TA generates a cyclic group $\mathbb{G}$ of order q, which consists of all E's points as well as the infinity point $\mathcal{O}$.
- The TA chooses the system master key $\beta \in Z_q^*$, then computes its related public parameter $PK_{TA} = \beta.P$.
- The TA selects two hash functions $H_1 : \{0,1\}^* \rightarrow \{0,1\}^{N_1}$ and $H_2 : \{0,1\}^* \rightarrow \{0,1\}^{2N_2}$ for $N_2 = 3N/4$. It also selects the 2-bit Gray code mapping function

TABLE I: List of notations and their equivalent AVISPA symbols

Symbol	Definition	AVISPA symbol
PPs	The system's public parameters	–
β, PK_{TA}	The system's master key and TA's public key	_inv{PKTA}, PKTA
PK_{V_i}, SK_{V_i}	V_i's certificate public and private keys	PKV1, _inv{PKV1}
$Cert_{V_i}$	V_i's long-term digital certificate	PKV1.TR.{PKV1.TR}_inv(PKTA)
T_R	The certificate validation time	TR
SPK_{V_i}, SSK_{V_i}	V_i's session public and private keys	SPKV1, _inv{SPKV1}
TID_{V_i}, PID_{V_i}	V_i's temporary and pseudo identities	TIDV1, PIDV1
PK_{R_k}, SK_{R_k}	R_k's certificate public and private keys	PKRSU, _inv{PKRSU}
$Cert_{R_k}$	R_k's long-term digital certificate	PKRSU.TR.{PKRSU.TR}_inv(PKTA)
SPK_{R_k}, SSK_{R_k}	R_k's session public and private keys	SPKRSU, _inv{SPKRSU}
TID_{R_k}	R_k's temporary identities	TIDRK
Sk_{i-k}	The shared key between V_i and R_k	SK12
σ_{V_i}, σ_{R_k}	V_i's and R_k's signatures	{–}_inv{PKV1}, {–}_inv{PKRSU}
$\sigma_{V_i}^{PHY}$	V_i's PHY-layer signature	{–}_SK12
ϕ_a, ϕ_b	The PHY-layer signature's phase shifts	–
T_i, T_r	signatures' creating and receiving timestamps	Ti $\forall$i $= \{1, 2, 3\}$
T_Δ	Timestamps' expiration period, e.g., [00:00:59]	–
P_d, P_{fa}	The detection and false alarm probabilities	–

TABLE II: The 160-bit EC's recommended parameters of "$secp160k1$" in the Hexadecimal form [40]

Par.	Value
a	00000000 00000000 00000000 00000000 00000000
b	00000000 00000000 00000000 00000000 00000007
p	FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFAC73
q	01 00000000 00000000 0001B8FA 16DFAB9A CA16B6B3
P	04 3B4C382C E37AA192 A4019E76 3036F4F5 DD4D7EBB 938CF935 318FDCED 6BC28286 531733C3 F03C4FEE

$\mathcal{M}(x_i) \rightarrow \phi_i$ that maps x_i to ϕ_i as follows.

$$\phi_i = \mathcal{M}(x_i) = \begin{cases} 0 & x_i = [00] \\ \frac{\pi}{2} & x_i = [01] \\ \pi & x_i = [11] \\ \frac{3\pi}{2} & x_i = [10] \end{cases}, \forall i \in [1, N_2] \quad (1)$$

- Finally, the system's public parameters PPs can be represented by the tuple $\langle a, b, p, q, P, Pk_{TA},\ H_1, H_2, \mathcal{M}\rangle$.

2) Registration phase: The TA registers all terminals before being part of the network by performing the following steps.

- For vehicle registration, the TA checks the vehicle V_i's real identity RID_{V_i}, selects at random V_i's secret key $SK_{V_i} \in Z_q^*$, and calculates its related public parameter $PK_{V_i} = SK_{V_i}.P$. Finally, the TA preloads the tuple $\langle PPs, SK_{V_i}, Cert_{V_i}\rangle$ onto V_i's OBU, where V_i's long-term digital certificate $Cert_{V_i} = \langle PK_{V_i}, T_R, \sigma_{TA}\rangle$, $\sigma_{TA} = Sign_\beta(PK_{V_i} \| T_R)$ and T_R is the certificate validation time.
- Each RSU R_k undergoes the same registration process.
- The TA creates a list of revoked vehicles' and RSUs' digital certificates known as the certificate revocation list $CRL = \{Cert_1, ..., Cert_z\}$, where z is the total number of revoked vehicles and RSUs. At last, the TA distributes the CRL among vehicles via RSUs in different regions. The proposed scheme uses the traditional revocation mechanism of PKI-based authentication. However, the proposed method is designed to be compatible with contemporary contributions in revocation mechanisms, as outlined in [41].

3) Initial authentication phase: Consider a scenario where V_i is within the communication range of R_k and wants to initiate a secure connection. In this case, both terminals, V_i and R_k, exchange certificate-based initial authentication packets for mutual legitimacy detection and extracting a symmetric shared key SK_{i-k}. The following steps constitute this phase.

- V_i randomly selects the session secret key $SSK_{V_i} \in Z_q^*$ and computes its corresponding public parameter $SPK_{V_i} = SSK_{V_i}.P$.
- V_i selects at random a temporary identity $TID_{V_i} \in \{0, 1\}^{N_1}$ and sends R_k a request to communicate in the form of $\langle TID_{V_i}, SPK_{V_i}, T_1, Cert_{V_i}, \sigma_{V_i}\rangle$, where the signature $\sigma_{V_i} = \text{Sign}_{SK_{V_i}}(TID_{V_i} \| SPK_{V_i} \| T_1 \| Cert_{V_i})$ and T_1 is the attached timestamp.
- Avoiding replay attacks, R_k checks T_1's freshness by testing whether if $T_r - T_1 \leq T_\Delta$ holds or not. Then, R_k checks V_i's legitimacy by determining if $Cert_{V_i} \in CRL$ holds or not. After that, R_k authenticates the received tuple by verifying σ_{V_i} as Verify $(\sigma_{V_i})_{PK_{V_i}}$.
- In response to V_i's request, R_k selects at random $SSK_{R_k} \in Z_q^*$ and computes its corresponding public parameter $SPK_{R_k} = SSK_{R_k}.P$, computes $SK_{i-k} = SPK_{V_i}.SSK_{R_k}$ using the Diffie-Hellman key exchanging protocol, and sends the tuple $\langle TID_{R_k}, SPK_{R_k}, T_2, Cert_{R_k},\ \sigma_{R_k}\rangle$ to V_i, where TID_{R_k} is the R_k's temporary identity and $\sigma_{R_k} = \text{Sign}_{SK_{R_k}}(TID_{R_k} \| \ SPK_{R_k} \| T_2 \| Cert_{R_k})$.
- At last, V_i checks if $T_r - T_2 \leq T_\Delta$ and $Cert_{R_k} \in CRL$ hold or not, verifies σ_{R_k} as Verify $(\sigma_{R_k})_{PK_{R_k}}$, and computes its own symmetric key $SK_{i-k} = SSK_{V_i}.SPK_{R_k}$.
- Each R_k in a coverage area stores a list of communicating vehicles' temporary identities and their associated shared key so that $list_{R_k} = \{Tuple_1, ..., Tuple_n\}$, where $Tuple_i = \langle Cert_{V_i}, TID_{V_i}, SK_{i-k}\rangle\ \forall i \in [1, n]$.

Fig. 2 shows the top-level description flowchart of the initial authentication phase. Note that the same procedures can be reapplied for communication between two involved vehicles, V_i and V_k, thereby facilitating V2V communication.

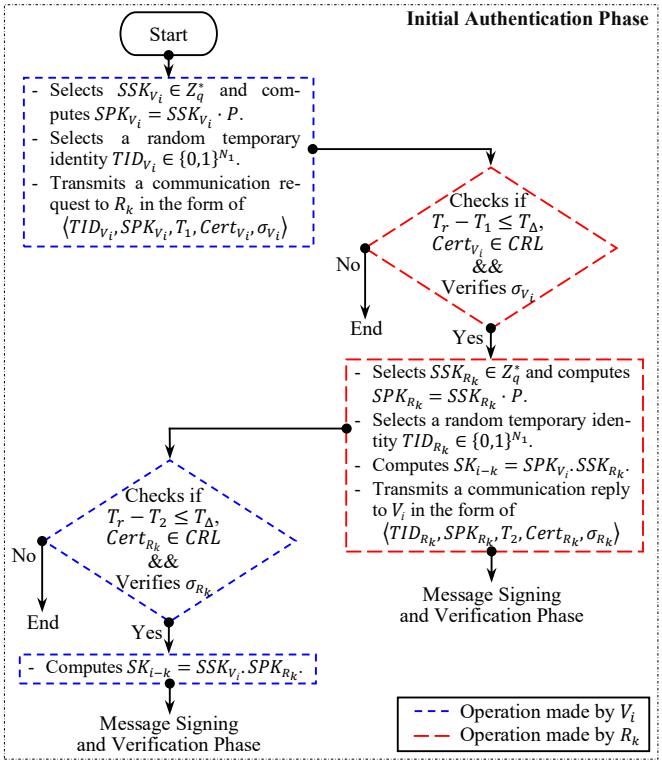


Fig. 2: The top-level description of the initial authentication.

4) Message signing and verification phase: In this phase, we adopt PHY-SIAM and PHY-FTM proposed in [32] as a two-factor re-authentication process performed at the physical layer. We create a PHY-layer signature used as a lightweight re-authentication technique based on the symmetric shared key SK_{i-k} and the message payload. Throughout this part, $\mathbb{C}^{N_x \times N_y}$, $\odot$, $()^*$, and $[]^T$ refer to a $N_x \times N_y$ matrix of complex elements, element-wise multiplication, conjugate, and transpose, respectively. While variables in uppercase and Bold represent matrices. The following steps constitute this phase.

- For each specific number Q of message (m) transmissions, V_i selects a random $a_1 \in Z_q^*$ and calculates its related public parameter $A_1 = a_1.P$. Next, V_i computes its pseudo-identity $PID_{V_i} = TID_{V_i} \oplus H_1(a_1.PK_{R_k})$.
- Then, V_i sends R_k the message in the form of $\langle m, PID_{V_i}, A_1, T_3, \sigma_{V_i}^{PHY} \rangle$, where $\sigma_{V_i}^{PHY}$ is the PHY-layer signature computed in a 2-step process as follows.

  - *Signature preparation step*: V_i computes two OFDM symbols' phase shifts, $\mathbf{\Phi}_a = [e^{j\phi_{a,1}}, ..., e^{j\phi_{a,N_2}}]^T \in \mathbb{C}^{N_2 \times 1}$ and $\mathbf{\Phi}_b = [e^{j\phi_{b,1}}, ..., e^{j\phi_{b,N_2}}]^T \in \mathbb{C}^{N_2 \times 1}$, where $\phi_a = \mathcal{M}(H_2(\{SK_{i-k}\}_x \| T_3 \| A_1 \| PID_{V_i} \| m))$, $\phi_b = \mathcal{M}(H_2(\{SK_{i-k}\}_y \| T_3 \| A_1 \| PID_{V_i} \| m))$, and $\{.\}_x$ and $\{.\}_y$ represent the x and y coordinates of the elliptic curve point $SK_{i-k} \in \mathbb{G}$, respectively.

  - *Signature generation step*: In this step, V_i encapsulates ϕ_a and ϕ_b onto two subsequent OFDM symbols of N subcarriers and sends it to R_k at times t and $t + \Delta t$ so that the transmitted symbols can be represented as

$$\begin{aligned} \mathbf{S}_1 &= [s_{1,1}, ..., s_{1,N_2}]^T = \mathbf{\Phi}_a \odot \mathbf{X}, \\ \mathbf{S}_2 &= [s_{2,1}, ..., s_{2,N_2}]^T = \mathbf{\Phi}_b \odot \mathbf{X} \end{aligned} \tag{2}$$

where $\mathbf{X} = [e^{j\psi_1}, ..., e^{j\psi_{N_2}}]^T \in \mathbb{C}^{N_2 \times 1}$, ψ_i is a uniformly distributed random variable $\psi_i \sim U[0, 2\pi)$, and Δt is the transmission time interval. Note that the OFDM symbols in (2) are collectively referred to as $\sigma_{V_i}^{PHY}$. Also, we consider the OFDM system as a superposition of N independently operating narrow-band subsystems.

- R_k receives $\sigma_{V_i}^{PHY}$ in (2) at times t' and $t' + \Delta t$, which can be represented in the frequency-domain, following the removal of the cyclic-prefix and calculating the Fast Fourier Transform (FFT), as

$$\begin{aligned} \mathbf{R}_1 &= [r_{1,1}, ..., r_{1,N_2}]^T = (\mathbf{H}_{VR} \odot \mathbf{S}_1) + \mathbf{N}, \\ \mathbf{R}_2 &= [r_{2,1}, ..., r_{2,N_2}]^T = (\mathbf{H}'_{VR} \odot \mathbf{S}_2) + \mathbf{N}' \end{aligned} \tag{3}$$

where $\mathbf{H}_{VR} = [|h_{1,1}|e^{j\xi_{1,1}}, ..., |h_{1,N_2}|e^{j\xi_{1,N_2}}]^T \in \mathbb{C}^{N_2 \times 1}$, $\mathbf{H}'_{VR} = [|h'_{1,1}|e^{j\xi'_{1,1}}, ..., |h'_{1,N_2}|e^{j\xi'_{1,N_2}}]^T \in \mathbb{C}^{N_2 \times 1}$, $\{|h_{1,i}|, \xi_{1,i}\}$ and $\{|h'_{1,i}|, \xi'_{1,i}\}$ are the channel amplitude and phase responses of the i^{th} subcarrier at times t' and $t' + \Delta t$, respectively, and $\{\mathbf{N}, \mathbf{N}'\}$ are complex additive Gaussian noises $\mathbb{CN}(0, \sigma_n^2)^{N_2 \times 1}$ with means and variances equal zero and σ_n^2, respectively. Note that $\mathbf{H}_{VR}$ is highly correlated with $\mathbf{H}'_{VR}$ for $\Delta t \leq T_c$.
- R_k checks T_3's freshness, computes $TID_{V_i} = PID_{V_i} \oplus H_1(A_1.SK_{R_k})$ and finds out if $TID_{V_i} \in list_{R_k}$ holds or no. If yes, R_k uses SK_{i-k} associated with TID_{V_i} and the message payload $\langle m, PID_{V_i}, A_1, T_3 \rangle$ to compute $\phi'_a = \mathcal{M}(H_2(\{SK_{i-k}\}_x \| T_3 \| A_1 \| PID_{V_i} \| m))$ and $\phi'_b = \mathcal{M}(H_2(\{SK_{i-k}\}_y \| T_3 \| A_1 \| PID_{V_i} \| m))$.
- Then, R_k uses a two-factor authentication process, PHY-SIAM and PHY-FTM, in two binary hypothesis testing problems for identity and message verification. This process comprises the following steps.

  - *Message verification step using PHY-SIAM*: In this step, R_k uses the computed ϕ'_a and ϕ'_b to equalise the received PHY-layer signature in (3) by computing $\mathbf{R}'_1 = \mathbf{R}_1 \odot \mathbf{\Phi}'^*_a$ and $\mathbf{R}'_2 = \mathbf{R}_2 \odot \mathbf{\Phi}'^*_b$, where $\mathbf{\Phi}'_a = [e^{j\phi'_{a,1}}, ..., e^{j\phi'_{a,N_2}}]^T \in \mathbb{C}^{N_2 \times 1}$ and $\mathbf{\Phi}'_b = [e^{j\phi'_{b,1}}, ..., e^{j\phi'_{b,N_2}}]^T \in \mathbb{C}^{N_2 \times 1}$. Since $\xi_{1,i}$ and $\xi'_{1,i}$ are highly correlated within T_c, R_k verifies the received message by computing $\mathbf{C} = [c_1, ..., c_{N_2}]^T = \mathbf{R}'_1 \odot \mathbf{R}'^*_2$. Then, R_k calculates the circular variance $c.var(.)$ of $\angle(\mathbf{C}) = [\angle(c_1), ..., \angle(c_{N_2})]^T$ as

$$v = c.var\left(\sum_{i=1}^{N_2} \arctan\left(\frac{\mathrm{Im}\,(c_i(t))}{\mathrm{Re}\,(c_i(t))}\right)\right) \tag{4}$$

where $c.var$ is defined as

$$\begin{aligned} \alpha_i = \begin{pmatrix} \cos(\angle(c_i)) \\ \sin(\angle(c_i)) \end{pmatrix}, \bar{\alpha} = \frac{1}{N_2}\sum_{i=1}^{N_2} \alpha_i, \\ v = 1 - \|\bar{\alpha}\| \end{aligned} \tag{5}$$

where $\|.\|$ represents the norm function. Avoiding impersonation and modification attacks, R_k verifies $\sigma_{V_i}^{PHY}$ in a hypothesis-testing problem given by

$$\begin{matrix} H_0 \\ v \lessgtr \tau_1, \text{ for} \\ H_1 \end{matrix} \begin{cases} H_0: & \mathbf{\Phi}'_a = \mathbf{\Phi}_a \ \& \ \mathbf{\Phi}'_b = \mathbf{\Phi}_b \\ H_1: & \mathbf{\Phi}'_a \neq \mathbf{\Phi}_a \ \& \ \mathbf{\Phi}'_b \neq \mathbf{\Phi}_b \end{cases} \tag{6}$$

where τ_1 is the threshold value and H_0 and H_1 are the hypotheses that state whether the received message has been successfully authenticated or unauthenticated, respectively. For more information, see reference [32].

- *Message verification step using PHY-FTM*: Based on the OFDM symbols structure of order M symbols in Fig. 3, R_k measures the correlation coefficient between the channel observation vector $\bar{H}_j$ estimated from the reference symbols of the j^{th} OFDM symbol and that $\bar{H}_{j+1}$ of the $(j+1)^{th}$ OFDM symbol, starting from $\sigma_{V_i}^{PHY}$ at $j = \{1, 2\}$ to the M^{th} symbol. Hence, if $\bar{H}_j$ is highly correlated with $\bar{H}_{j+1}$, this means that these symbols are sent from the same transmitter. Otherwise, the received message is discarded. Hence, message verification can be described as a hypothesis-testing process based on the normalised likelihood ratio test (LRT), which is given by

$$\Lambda_{LRT} = \frac{n_{\tau_2} \left\| \bar{H}_j - \bar{H}_{j-1} \right\|^2}{\left\| \bar{H}_{j-1} \right\|^2} \quad \forall j \in [2, M], \qquad \Lambda_{LRT} \underset{H_0}{\overset{H_1}{\lessgtr}} \tau_2 \tag{7}$$

where $\tau_2 \in [0, 1]$ is the threshold value and n_{τ_2} is the normalisation coefficient. The decision rule can be made based on the sequential probability ratio test (SPRT) that sums the LRTs between the j^{th} and the $(j-1)^{th}$ OFDM symbols $\forall j \in [2, M]$. The SPRT-based hypothesis-testing problem can be expressed as

$$\Lambda_j = \frac{n_{\tau_2} \left\| \bar{H}_{M-j+1} - \bar{H}_{M-j} \right\|^2}{\left\| \bar{H}_{M-j} \right\|^2} \forall j \in [1, M-1], \qquad \Lambda_{SPRT} = n_{\tau_3} \sum_{j=2}^{M} \Lambda_j, \Lambda_{SPRT} \underset{H_0}{\overset{H_1}{\lessgtr}} \tau_3 \tag{8}$$

where $\tau_3 \in [0, 1]$ is the threshold value and n_{τ_3} is the normalisation coefficient. For more information, see reference [32].

- Finally, R_k accepts or discards the received message from V_i based on the decision rule of both PHY-SIAM and PHY-FTM hypothesis problems. Accepted messages are those that are identified by both problems as being H_0. Otherwise, the message will be discarded.

Fig. 4 shows the top-level description flowchart of the message authentication and integrity verification phase. Note that the pseudo-identity PID_{V_i} undergoes periodic updates for every re-authentication session to support traceability and anonymity. However, if we consider the system failure due to synchronization issues during the session time period denoted by $Q \times [100, 300]\ msec$, the scheme will be reset and return to the initial authentication phase.

C. RIS-assisted PHY-layer authentication

One of the challenging issues of PHY-layer authentication is that the detection probability P_d primarily depends on the received signal's SNR value, whereas P_d defines the probability of authenticating legitimate users as authorised terminals. A higher SNR value indicates a higher P_d for an acceptable false alarm probability P_{fa}, and vice versa, where P_{fa} defines the probability of authenticating legitimate users as unauthorised terminals. This makes the PHY-layer authentication impractical in long-range and non-line-of-sight (NLoS) vehicular communications. While traditional beamforming and repeaters improve signal strength, their performance degrades in highly dynamic, obstructed vehicular environments due to factors like noise amplification and limited spectral efficiency. RIS offers a power-efficient, environment-aware solution that enhances throughput and robustness, especially under mobility and blockage conditions common in urban settings, see Fig. 1. As a result, the proposed scheme can effectively authenticate the received messages from the vehicles in the shadowing areas. Thus, the received signals in (3) for the i^{th} subcarrier is the superposition of L multipath components coming from L RIS's reflective elements and can be reformulated as

$$\begin{aligned} r_{1,i} &= (\mathbf{H}_{VI} \odot \mathbf{H}_{IR})\, \boldsymbol{\omega}_\theta\, s_{1,i} + n_i, \\ r_{2,i} &= (\mathbf{H}'_{VI} \odot \mathbf{H}'_{IR})\, \boldsymbol{\omega}_\theta\, s_{2,i} + n'_i \end{aligned} \quad \forall i \in [1, N_2] \tag{9}$$

where $\mathbf{H}_{VI} = [|h_{2,1}|e^{j\xi_{2,1}}, ..., |h_{2,L}|e^{j\xi_{2,L}}] \in \mathbb{C}^{1\times L}$, $\mathbf{H}_{IR} = [|h_{3,1}|e^{j\xi_{3,1}}, ..., |h_{3,L}|e^{j\xi_{3,L}}] \in \mathbb{C}^{1\times L}$, and $\boldsymbol{\omega}_\theta = [e^{j\omega_1\theta_1}, ..., e^{j\omega_L\theta_L}]^T \in \mathbb{C}^{L\times 1}$. $\mathbf{H}_{VI}$ and $\mathbf{H}_{IR}$ represents the channel responses from V_i to RIS and from RIS to R_k, respectively. While $\boldsymbol{\omega}_\theta$ defines the phase shift matrix related to the L reflective elements of the RIS, where θ_l and ω_l defines the l^{th} reflective element phase shift value and state, respectively $\forall l \in [1, L]$, for example, $\theta_l = \pi$ and $\omega_l \in \{0, 1\}$ for a 1-bit RIS. Note that $\{\mathbf{H}_{VI}, \mathbf{H}_{IR}\}$ is highly correlated with $\{\mathbf{H}'_{VI}, \mathbf{H}'_{IR}\}$ within T_c. The RSU in each region optimises the RIS configuration $\boldsymbol{\omega}_\theta$ to maximise the power of the received signals at the side of the intended user. Hence, improving the receiver operating characteristics (ROCs; P_d versus P_{fa}) of the two-factor re-authentication process at poor SNRs.

In conclusion, the impact of the RIS on the performance of the PHY-SIAM and PHY-FTM mechanisms can be summarised as follows:

1) For PHY-SIAM: In the circular variance test defined in equations (4 : 6), the phase stability of the signal components $\phi'_{a,i}$ and $\phi'_{b,i}$ directly influences the dispersion of the resulting complex correlation vector $\mathbf{C}$. Specifically, when the RIS is configured to align signal phases constructively, it preserves the coherence of the received signals originating from legitimate users. This coherence reduces the circular variance v under hypothesis H_0, resulting in a lower variance distribution of phase angles around the mean value-i.e., stronger clustering on the unit circle.
2) **For PHY-FTM**: The RIS can be optimally configured to reinforce the dominant multipath component between a legitimate vehicle and the RSU. This reinforcement reduces the variability between successive channel estimates $\bar{H}_{j-1}$ and $\bar{H}_j$ in equations (7) and (8), thereby decreasing the term $\left\| \bar{H}_j - \bar{H}_{j-1} \right\|^2$ under hypothesis H_1 during normal (authentic) conditions.

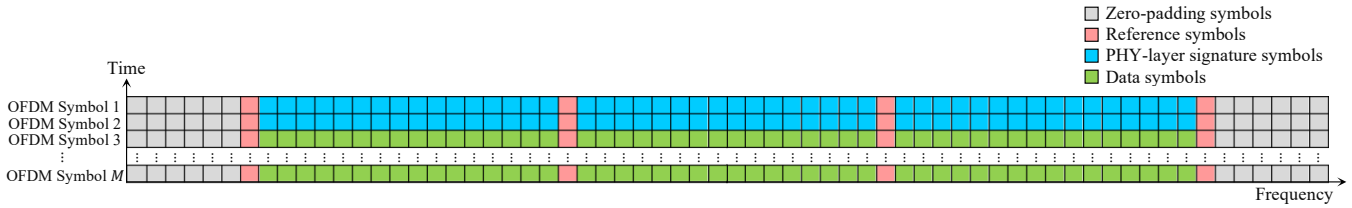


Fig. 3: OFDM symbols' structure for 64 subcarriers.

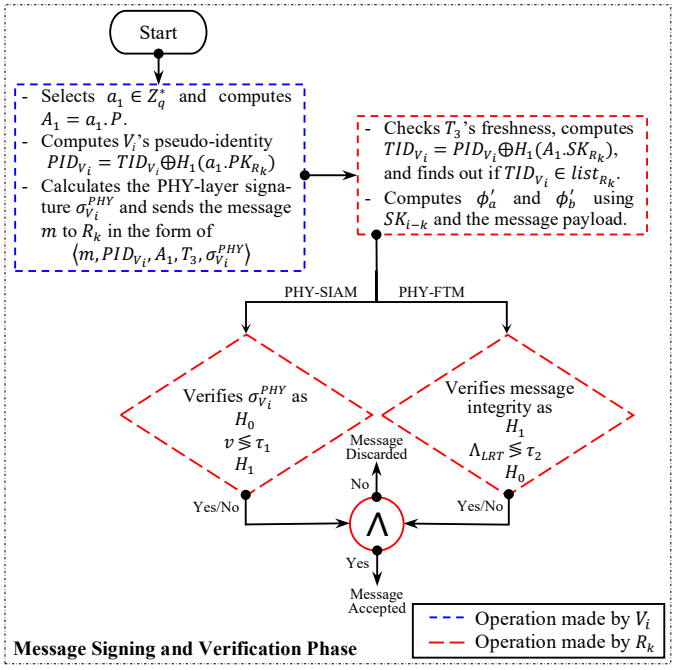


Fig. 4: The top-level description of the message authentication and integrity verification phase.

IV. Security and Privacy Analyses

This section investigates how the proposed scheme satisfies the security and privacy requirements of VANETs.

A. Attack model

In this work, the attack model is designed to thoroughly assess the security of the proposed re-authentication method within VANET communications. The adversaries in this model are strategically positioned within the network to exploit various vulnerabilities: Eavesdroppers are located where they can intercept and potentially exploit sensitive communications between vehicles and RSUs. Replay attackers capture authentication messages and retransmit them to deceive the system into accepting outdated credentials. Impersonators forge credentials to appear as legitimate entities, gaining unauthorised access to the network. MitM attackers position themselves to intercept and alter communications between vehicles and RSUs, compromising the integrity of authentication messages. This attack model helps evaluate how well the proposed system withstands various types of security threats and maintains robustness under different adversarial conditions.

B. Security proof using Random Oracle Modelling

In cryptography, the random oracle model (ROM) is a theoretical framework often used to analyse the security of cryptographic constructions [42]. It involves using a random oracle, a mathematical function that produces random output for each unique input and maintains no internal state. In this part, we prove the security robustness of the proposed scheme using the ROM analysis. Specifically, we analyse the resistance of the signature generation process against potential threats posed by an adversarial entity $\mathcal{A}$. $\mathcal{A}$ is trying to impersonate an authorised vehicle V_i by generating valid signatures σ_{V_i} and $\sigma_{V_i}^{PHY}$ within the initial authentication and message signing and verification phases. The computational complexity associated with signature generation in both phases depends on the infeasibility of forging two distinct cryptographic problems, formally defined as follows.

- **Definition 1.** The elliptic curve discrete logarithm problem (ECDLP). Given PPs and $Q = \gamma \cdot P$ on an elliptic curve, find $\gamma \in \mathbb{Z}_q^*$.
- **Definition 2.** Hashing problem. Given the value s', where $s' = H_2(x)$, determine the corresponding input value $x \in \{0,1\}^{2N_2}$.

The signature generation stage, denoted as $(q_s, q_k, \epsilon_{\text{Sig.Gen}})$, exhibits existential unforgeability against identity and adaptive chosen message attacks in the ROM, given that:

$$\epsilon_{\text{Sig.Gen}} = \epsilon \left(1 - \frac{q_s^2 q_k^2}{q}\right) \tag{10}$$

where, q_s and q_k represent the number of queries made to the oracles $\sigma_{V_i}(.)$ and $SK_{i-k}(.)$ respectively. Furthermore, $\epsilon_{\text{Sig.Gen}}$ denotes the probability of $\mathcal{A}$ to successfully generate a non-trivial forgery. The proof of (10) is given in Appendix A.

C. Security proof using automated validation of internet security protocols and applications (AVISPA) simulation

Similar to the work introduced in [43], [44], this subsection proves the resilience of the proposed scheme against common attacks using the AVISPA simulation toolkit.

1) *Preliminaries*: Armando et al. [45] introduced the automated validation of internet security protocols and applications (AVISPA) framework, a prominent toolkit for assessing security protocols and internet applications. AVISPA employs high-level protocol specification language (HLPSL) to specify network terminal roles for agents, evaluating authentication and message confidentiality against potential intrusions. Security properties are formalized in "goals," enabling protocol classification as "SAFE" or "UNSAFE." The HLPSL2IF translator

converts HLPSL code to the intermediate format (IF), feeding various back-ends: TA4SP, SATMC, OFMC, and CL-AtSe. In this study, CL-AtSe assesses the proposed scheme, evaluating resistance to MITM and replay attacks. A comprehensive explanation of these roles is offered within Appendix B through the utilisation of HLPSL codes. These codes are written using the notations and their corresponding AVISPA symbols listed in Table I. It is important to note that the symbol "/\" signifies a conjunction between two operations.

2) *Simulation specifications*: The initial stage involves the definition of security objectives for the proposed scheme. These objectives encompass the authentication of broadcasted messages by the designated agent, as specified by auth_1, auth_2, and auth_3. In the simulation context, two agent roles, namely role_V1 and role_RSU, are assumed, each representing the functions of V1 and RSU, respectively. The declarations pertinent to all agents are established within the role session, while the role environment identifies variables and functions associated with distinct agents. Fig. 5 shows the protocol simulation, visualizing the transitional interactions among agents.
3) *Simulation results*: Using the AVISPA security analysis, simulation results of the specified goals are presented in Fig. 6, employing the Cl-AtSe back-end checker. Notably, the CL-AtSe model exhibits minimal time consumption (~ 0.00 seconds) for the IF translation process. Based on the summary, it can be inferred that the proposed scheme is secure against potential MITM and replay attacks.

D. Security and privacy informal analysis

1) Message authentication: The proposed scheme offers legitimacy detection and ensures message integrity for the following reasons:

- For legitimacy detection, the recipient V_i/R_k verifies the sender's legitimacy R_k/V_i by checking if $Cert_{V_i/R_k} \in CRL$, where $\sigma_{TA} \in Cert_{V_i/R_k}$ is signed using $\beta \in Z_q^*$ and verified by the recipient using $PK_{TA} \in PPs$, which is infeasible to be forged under the difficulty of solving the ECDLP. In addition, the transmitted tuple $\langle TID_{V_i/R_k}, SPK_{V_i/R_k}, T_1, Cert_{V_i/R_k}, \sigma_{V_i/R_k} \rangle$ is verified for its integrity using the signature σ_{V_i/R_k} that is signed using V_i/R_k's secret key Sk_{V_i/R_k} and verified by the recipient using $Pk_{V_i/R_k} \in Cert_{V_i/R_k}$.
- For message authentication at subsequent transmission slots, the tuple $\langle m, PID_{V_i}, A_1, T_3, \sigma_{V_i}^{PHY} \rangle$ is verified by R_k for its integrity in a two-factor authentication process, PHY-SIAM and PHY-FTM, that's infeasible to be forged for the following reasons: A) The phase shifts, $\mathbf{\Phi}_a$ and $\mathbf{\Phi}_b$, in (2) are computed based on the shared key $SK_{i-k} \in \mathbb{G}$ and masked by $\mathbf{X} = \{e^{j\psi_1}, ..., e^{j\psi_{N_2}}\}$, where ψ_i is a uniformly distributed random variable $\sim U[0, 2\pi)$, which makes it infeasible for an adversary to differentiate between $\mathbf{\Phi}_a$ and $\mathbf{\Phi}_b$ and $\mathbf{X}$. B) The high correlation coefficient between subsequent channel observation vectors $\{\bar{H}_{j-1}, \bar{H}_j\}$ in (7) $\forall j \in [2, M]$ or $\{\bar{H}_j, \bar{H}_{j+1}\}$ in (8) $\forall j \in [1, M-1]$ helps in detecting modification attempts in the message payload.

2) Privacy preservation: In the proposed scheme, vehicles communicate using their temporary identities TID_{V_i} at the first transmission slot, while pseudo identities PID_{V_i} are used at subsequent transmissions. This preserves users' real identities RID_{V_i} from exposure as no network terminals possess RID_{V_i} or even the link between RID_{V_i} and its associated long-term digital certificates $Cert_{V_i}$ except for the TA. Only the TA is authorised to expose RID_{V_i} in cases of misbehaviour (for example, when the vehicle constructs an attack or when a driver drives an unregistered vehicle).

3) Unlinkability: For each Q number of message transmissions per session, V_i uses a different pseudo-identity $PID_{V_i} = TID_{V_i} \oplus H_1(a_1.PK_{R_k})$, where $a_1 \in Z_q^*$ is dynamically updated for each session. Hence, no parameter is used twice per session, thereby avoiding location-tracking attacks.

4) Traceability and revocation: Each RSU in a specific area can report misbehaving vehicles to the TA by sending its associated digital certificate $Cert_{V_i}$. The TA, in turn, reveals its associated real identity, appends $Cert_{V_i}$ to the CRL, and distributes the updated CRL among vehicles via RSUs.

5) Perfect forward secrecy (PFS): PFS is a cryptographic property where the compromise of a long-term symmetric key does not compromise the confidentiality of past or future communications. It ensures that even if an attacker gains access to a session key, they cannot compromise previously recorded messages or intercept future messages (m). In this context, considering an adversary (Eve) capable of deducing the symmetric key SK_{i-k} by hypothesising acquisition of the private key SSK_{R_k} associated with RSU, the compromise of previous sessions becomes infeasible due to each session being established using a distinct randomly selected $SSK_{R_k} \in Z_q^*$. Consequently, no traceability exists among the established shared keys from different sessions.

6) Resistance to passive and active attacks: This part discusses the scheme's resistance against typical adversarial attacks. By considering an adversary, Eve acts as a passive attacker and listens to the communicating terminals' broadcasted messages to deduce any useful information about the symmetric key Sk_{i-k}. In this scenario, Eve attempts to deduce the shared key either during the initial authentication phase (case 1) or during the message signing and verification phase (case 2). In case 1, Sk_{i-k} is calculated using the Diffie-Hellman key exchanging protocol. This makes it difficult for Eve to compute Sk_{i-k} due to the difficulty of solving the ECDLP. In case 2, Eve has difficulty deducing the value of Sk_{i-k} from the PHY-layer signature $\sigma_{V_i}^{PHY}$ due to the following: 1) The signature generation step is dependent on the dynamically updated parameters $\langle T_i, A_i, PID_{V_i}, m \rangle$, which results in different outputs, $\mathbf{\Phi}_a$ and $\mathbf{\Phi}_b$, under the same shared key Sk_{i-k}. In addition, The received $\sigma_{V_i}^{PHY}$ in (3) is dependent on the spatially and temporally varying channel phase responses ξ_i and ξ_i' that masks $\phi_{a,i}$ and $\phi_{b,i}$, respectively. 2) For $y = H_2(x)$, it is difficult for Eve to determine the input variable x from the hashed variable $y : \{0,1\}^{N_2}$. In this scenario, we consider Eve to be an active attacker who is capable of constructing the following types of attacks:

- *Modification resistance*: In this attack, Eve tries to modify the message payload either during the initial authentica-

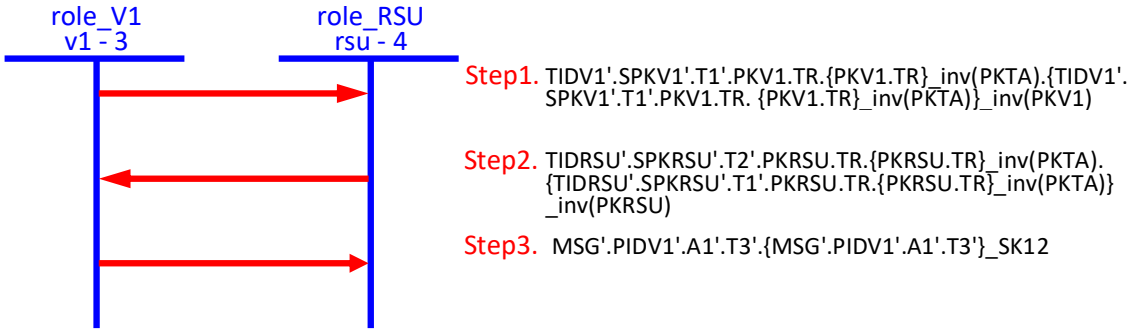


Fig. 5: Protocol simulation using AVISPA.

Fig. 6: AVISPA simulation results using CL-AtSe.

tion phase (case 1) or during the message signing and verification phase (case 2). In case 1, the recipient R_k/V_i verifies the received tuple $\langle TID_{V_i/R_k}, SPK_{V_i/R_k}, T_i, Cert_{V_i/R_k}, \sigma_{V_i/R_k}\rangle$ for its integrity based on the attached signature σ_{V_i/R_k}. For this attack to be successful, Eve must modify the message contents and forge a valid signature, which is computationally intractable due to the difficulty of solving the ECDLP. In case 2, Eve must modify the message contents $\langle m, PID_{V_i}, A_i, T_i\rangle$ and forge a valid signature $\sigma_{V_i}^{PHY}$. Without any knowledge of the shared key Sk_{i-k}, Eve is unable to correctly estimate the values of $\mathbf{\Phi}_a$ and $\mathbf{\Phi}_b$ needed to generate a valid signature. Accordingly, this type of attack can be easily detected.

- *Impersonation resistance*: In this attack, Eve tries to impersonate the communicating vehicle V_i during the initial authentication phase. For this attack to be successful, Eve must generate a valid signature σ_{V_i} using the V_i's secret key Sk_{V_i}, which cannot be forged due to the difficulty of solving the ECDLP. Accordingly, it is hard to compute a valid shared key Sk_{i-k} used for generating $\sigma_{V_i}^{PHY}$ during the message signing and verification phase. Hence, the proposed scheme is resistant to this type of attack.
- *Replay resistance*: In this attack, Eve repeats the transmission of a previously captured message either during the initial authentication phase (case 1) or during the message signing and verification phase (case 2). In both cases, each transmission is accompanied by a fresh timestamp T_i that helps the recipient detect this type of attack by testing whether $T_r - T_i \leq T_\Delta$ holds. Hence, the proposed scheme is resistant to replay attacks.

E. Security proof using BAN-logic formal analysis

The Burrows-Abadi-Needham (BAN) security proof is a formal methodology that offers a rigorous approach to evaluate the security of authentication protocols. The BAN approach is grounded in a formal model of authentication protocols and employs inference rules to analyse the knowledge and beliefs of principals involved in the protocol. Due to its effectiveness, the BAN methodology has been extensively adopted for analysing and verifying the security of authentication protocols in diverse settings such as computer networks, web communications, smart cards, and mobile devices. This study employs the BAN logic analysis to scrutinise the security of the proposed method against various types of attacks, such as replay, man-in-the-middle, and impersonation attacks.

1) Notations: In BAN-logic, security properties are expressed and argued using the following symbols.

- $A \mid\equiv X$: A believes that the proposition of X is true.
- $A \triangleleft X$: A sees X denotes that principal A has received a message that includes the value X.
- $A \mid\sim X$: X has been transmitted to A at some point, and A has subsequently believed the proposition X.
- $A \mid\Longrightarrow X$: A has control over the value X and has the authority or jurisdiction to manipulate or modify it.
- $A \overset{k}{\longleftrightarrow} B$: A and B share a secret key k, which they use to securely communicate with each other.
- $A \overset{k}{\longrightarrow} B$: k denotes the public key attributed to A.
- $\{X\}_k$: The shared key k is used to encrypt X.
- $\#(X)$: It represents a fresh message X.

2) Rules: A set of deductive rules are used to analyse initial beliefs and protocol messages exchanged between participants and make inferences about the security properties of the protocol. These rules are listed and defined in Table III.

3) Goals: The primary objective of BAN-logic is to demonstrate the validity of the proposed scheme by accomplishing the following set of goals.

- *Goal* 1: $R_k \mid\equiv (R_k \overset{Sk_{i-k}}{\longleftrightarrow} V_i)$.
- *Goal* 2: $R_k \mid\equiv (V_i \mid\equiv M_1)$.
- *Goal* 3: $V_i \mid\equiv (V_i \overset{Sk_{i-k}}{\longleftrightarrow} R_k)$.

TABLE III: The rules involved in the BAN-logic analysis

No.	Rule	BAN-logic representation	Definition
R_1	Message rule for a shared key	$\frac{A\mid\equiv(A\overset{K}{\longleftrightarrow}B),A\triangleleft\{X\}_K}{A\mid\equiv(B\mid\sim X)}$	If A believes in K and A received X encrypted by K, then A believes B said X
R_2	Message rule for a public key	$\frac{A\mid\equiv(B\overset{K}{\longrightarrow}A),A\triangleleft\{X\}_{k-1}}{A\mid\equiv(B\mid\sim X)}$	If A believes K is B's public key and receives X encrypted with B's private key, then A believes B said X
R_3	Nonce verification rule (NVR)	$\frac{A\mid\equiv\#(X),A\mid\equiv(B\mid\sim X)}{A\mid\equiv(B\mid\equiv X)}$	If A believes X is fresh and that B said X, then A believes B believes X
R_4	Jurisdiction rule (JR)	$\frac{A\mid\equiv(B\Longrightarrow X),A\mid\equiv(B\mid\equiv X)}{A\mid\equiv X}$	If A believes B has jurisdiction over X and that B believes X, then A believes X
R_5	Freshness rule (FR)	$\frac{A\mid\equiv\#(X)}{A\mid\equiv\#(X,Y)}$	Freshness of one part ensures the freshness of the entire formula

- *Goal* 4: $V_i \mid\equiv (R_k \mid\equiv M_2)$.
- *Goal* 5: $R_k \mid\equiv (M_3)$.

4) Idealised forms: The following points formulate the idealised messages for the proposed method.

- M_1: $V_i \rightarrow R_k$: $\{TID_{V_i}, SPK_{V_i}, T_1, Cert_{V_i}\}_{SK_{V_i}}$, where $Cert_{V_i} = \{PK_{V_i}, T_R\}_\beta$.
- M_2: $R_k \rightarrow V_i$: $\{TID_{R_k}, SPK_{R_k}, T_2, Cert_{R_k}\}_{SK_{R_k}}$, where $Cert_{R_k} = \{PK_{R_k}, T_R\}_\beta$.
- M_3: $V_i \rightarrow R_k$: $\{m, PID_{V_i}, A_1, T_3, \sigma_{V_i}^{PHY}\}$, where $\sigma_{V_i}^{PHY} = \{m, PID_{V_i}, A_1, T_3\}_{Sk_{i-k}}$.

5) Assumptions: The fundamental assumptions underlying the BAN-logic security proof are as follows.

- A_1: $R_k \mid\equiv \#(T_1)$.
- A_2: $V_i \mid\equiv \#(T_2)$.
- A_3: $R_k \mid\equiv \#(T_3)$.
- A_4: $R_k \mid\equiv (TA \overset{K_{TA}}{\longrightarrow} R_k)$.
- A_5: $V_i \mid\equiv (TA \overset{K_{TA}}{\longrightarrow} V_i)$.
- A_6: $\frac{R_k\mid\equiv(TA\overset{PK_{T_A}}{\longrightarrow}R_k),R_k\triangleleft\{Pk_{V_i},T_R\}_\beta}{R_k\mid\equiv(V_i\overset{Pk_{V_i}}{\longrightarrow}R_k)}$.
- A_7: $\frac{V_i\mid\equiv(TA\overset{PK_{T_A}}{\longrightarrow}V_i),V_i\triangleleft\{Pk_{R_k},T_R\}_\beta}{V_i\mid\equiv(R_k\overset{Pk_{R_k}}{\longrightarrow}V_i)}$.
- A_8: $R_k\mid\equiv (V_i \Longrightarrow M_3)$.

6) Implementation: The security proof of the proposed protocol is presented as follows.

- *Step* 1: Upon receipt of the message M_1 from V_i, R_k applies A_4 and $Cert_{V_i} \in M_1$ to A_6, resulting in the following outcome: $O_1 : R_k \mid\equiv (V_i \overset{Pk_{V_i}}{\longrightarrow} R_k)$.
- *Step* 2: By applying O_1 and M_1 to R_2 from Table III, the outcome is $O_2 : R_k \mid\equiv (V_i \mid\sim M_1)$. Accordingly, R_k computes $SK_{i-k} = SPK_{V_i}.SSK_{R_k}$ and have $O_3 : R_k \mid\equiv (R_k \overset{SK_{i-k}}{\longleftrightarrow} V_i)$, achieving *Goal* 1. Next, by applying A_1 and M_2 to R_5 from Table III, we have $O_4 : R_k \mid\equiv \#(M_1)$. Accordingly, by applying O_4 and O_2 to R_3 from Table III, we have $R_k \mid\equiv (V_i \mid\equiv M_1)$, achieving *Goal* 2.
- *Step* 3: Upon receipt of the message M_2 from R_k, V_i applies A_5 and $Cert_{R_k} \in M_2$ to A_7, resulting in the following outcome: $O_5 : V_i \mid\equiv (R_k \overset{Pk_{R_k}}{\longrightarrow} V_i)$. By applying O_5 and M_2 to R_2 from Table III, the outcome is $O_6 : V_i \mid\equiv (R_k \mid\sim M_2)$. Accordingly, V_i computes $SK_{i-k} = SSK_{V_i}.SPK_{R_k}$ and have $O_7 : V_i \mid\equiv (V_i \overset{SK_{i-k}}{\longleftrightarrow} R_k)$, achieving *Goal* 3.
- *Step* 4: By applying A_2 and M_2 to R_5 from Table III, we have $O_8 : V_i \mid\equiv \#(M_2)$. Accordingly, by applying O_8 and O_6 to R_3 from Table III, we have $V_i \mid\equiv (R_k \mid\equiv M_2)$, achieving *Goal* 4.
- *Step* 5: Upon receipt of the message M_3 from V_i, R_k applies O_2 and $\sigma_{V_i}^{PHY} \in M_3$ to R_1 from Table III, then we have $O_9 : R_k \mid\equiv (V_i \mid\sim M_3)$. Next, by applying A_3 and M_3 to R_5 from Table III, we have $O_{10} : R_k \mid\equiv \#(M_3)$. Then, by applying O_{10} and O_9 to R_3 from Table III, we have $O_{11} : R_k \mid\equiv (V_i \mid\equiv M_3)$. Finally, by applying A_8 and O_{11} to R_4 from Table III, we have $O_{12} : R_k \mid\equiv (M_3)$, achieving *Goal* 5.

V. Performance evaluation

This section analyses the theoretical and practical aspects of RIS-assisted PHY-layer authentication performance, followed by detailed computation and communication comparisons.

A. Theoretical analysis of the PHY-layer authentication

In order to evaluate the ROCs of the proposed method, it is crucial to evaluate the probability density function (PDF) for the phase estimate (Θ) of $\mathrm{C} = \mathbf{R}_1' \odot \mathbf{R}_2'^*$, where $\mathbf{R}_1'$ and $\mathbf{R}_2'$ denote the equalised received PHY-layer signature, given by the element-wise multiplication of $\mathbf{R}_1$ in (3) and $\mathbf{\Phi}_a'^*$, and $\mathbf{R}_2$ in (3) and $\mathbf{\Phi}_b'^*$, respectively. In the case of $\{\mathbf{\Phi}_a, \mathbf{\Phi}_b\}$ at the transmitting side V_i are equivalent to $\{\mathbf{\Phi}_a', \mathbf{\Phi}_b'\}$ at the receiving side R_k, the phase distribution of C for varying SNR values can be formulated according to [32] as follows.

$$P(\Theta \mid \Gamma) = \frac{1}{2\pi}e^{-\Gamma} + \frac{1}{\sqrt{\pi}}(\sqrt{\Gamma}\cos\Theta)\cdot e^{-\Gamma\sin^2\Theta}[1 - \mathbb{Q}(\sqrt{2\Gamma}\cos\Theta)] \tag{11}$$

where

$$\Gamma = \frac{|h_i|^2 \cdot {E_S}^2}{\sigma_n^2}, \qquad \mathbb{Q}(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-t^2/2}dt \tag{12}$$

where E_S is the symbol energy. Fig. 7 presents $P(\Theta \mid \Gamma)$ for different SNR values (i.e., $\Gamma \in [0, 25]$ dB). As indicated in (4), the circular variance of $\angle(\mathbf{C})$ with a specific order of N_2 is denoted as v, and this quantity satisfies the central limit theorem (CLT). Therefore, v's distribution $\mathcal{F}(x)$ follows a normal distribution with a mean (μ_{H_0}) equal to the variance of $P(\Theta)$ for a given Γ value and a variance equal to $\sigma_{H_0}^2$.

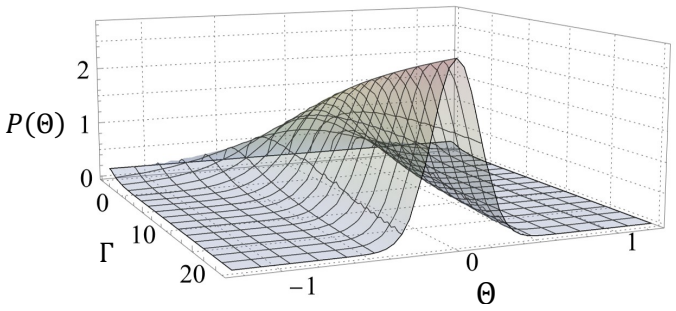


Fig. 7: $P(\Theta \mid \Gamma)$ in (11) at different given $\Gamma \in [0, 25]$dB.

Thus, the following formulation can express v's cumulative distribution function (CDF) for both hypotheses.

$$\phi\left(x \mid \mu_{H_i}, \sigma^2_{H_i}\right) = \frac{1}{2}\left[1 + \text{erf}\left(\frac{x - \mu_{H_i}}{\sqrt{2\sigma^2_{H_i}}}\right)\right], \forall i \in \{0, 1\} \tag{13}$$

In this context, we define $P_d = \phi(x \mid \mu_{H_0}, \sigma^2_{H_0})\big|_{x=\tau_1}$ and $P_{fa} = \phi(x \mid \mu_{H_1}, \sigma^2_{H_1})\big|_{x=\tau_1}$ for a threshold value τ_1 of the hypothesis testing problem in (6). As illustrated in (12), the channel fading coefficient, represented by $|h_i|$, is a critical factor in determining the value of Γ while maintaining a constant value of E_s and noise variance σ^2_n. Generally, the received signal at the recipient side comprises various multipath components originating from distinct scatterers. Nonetheless, in this study, our focus is solely on the RIS path connecting the communicating terminals, as the impact of the remaining scatterers is consistent regardless of whether the RIS is being switched ON or OFF. The channel components of the i^{th} subcarrier in both scenarios, considering the RIS turned ON and OFF, have been expressed in (3) and (9), respectively. Accordingly, the presence of the RIS can improve the SNR towards the communicating vehicle by configuring the reflective elements in a way that constructively interferes in a specific direction. This can be achieved by controlling the RIS electromagnetic behaviour by optimising $\boldsymbol{\omega}_\theta$ in (9) to maximise the Γ value in (12). By doing so, the system's performance at a certain SNR value, denoted as $\Gamma = X$ dB, without the RIS can be equal to its performance at a lower SNR value, $\Gamma = X - \Delta X$ dB, with the RIS. A higher Γ value signifies a decrease in the overlapping between the distributions of both hypotheses, $\mathcal{F}(x)|_{H_0}$ and $\mathcal{F}(x)|_{H_1}$, due to a lower value of μ_{H_0} for $\mathcal{F}(x)|_{H_0}$ relative to μ_{H_1} for $\mathcal{F}(x)|_{H_1}$. This improvement enhances the detection performance while maintaining an acceptable false alarm probability (a_1). Hence, the optimisation of the system's threshold value (τ_1 in (6)) can be computed by utilising the following formula [32].

$$\tau_1 = \arg\max_{\tau_1'} \text{erf}\left(\frac{\tau_1' - \mu_{H_1}}{\sqrt{2\sigma^2_{H_1}}}\right) \leq 2a_1 - 1 \tag{14}$$

B. Practical experimentation of the RIS-assisted method

In order to demonstrate the practicality of the proposed RIS-assisted PHY-layer authentication method, we conducted a hardware implementation using a 1-bit RIS consisting of 4096 reflective elements arranged in a two-dimensional 64×64 grid, along with a universal serial radio peripheral (USRP) equipped with two channels (denoted as Ch_0 and Ch_1) that functioned as the transmitter (T_x) and receiver (R_x), representing R_k and V_i, respectively. The antennas used for T_x and R_x are of the two-horn type, with the T_x antenna beam adjusted perpendicular to the RIS reflecting surface and located 3 meters away from the centre. On the other hand, the R_x antenna was situated 9 meters away from the RIS, with an NLoS path between it and the T_x antenna, and its beam set at a 45-degree angle from the line connecting the T_x antenna to the RIS. The experiment is conducted on an Intel Core $i7$ 2.7 GHz processor with 16.0 GB RAM with the NI LabVIEW platform to control the USRPs. Different views of the experimental setup are presented in Fig. 8. Table IV shows the experimental settings.

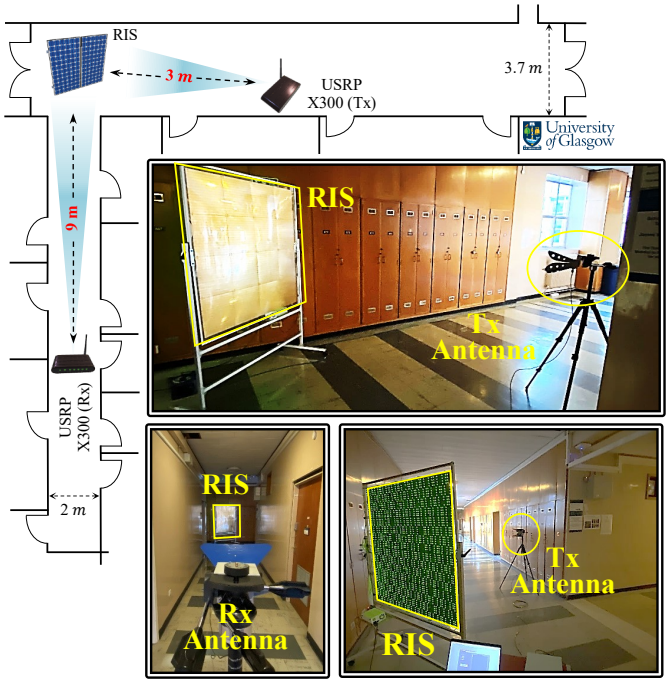


Fig. 8: Experiment setup of the RIS-assisted method.

We set the carrier frequency F_c to 3.75 GHz for 5G-V2I communication, the T_x and R_x gains to 20 dB and 5 dB, respectively, and the sampling rates for both channels to 200 KHz. We implemented a range of OFDM systems with varying numbers of subcarriers including 64, 128, and 256, and cyclic prefix (CP) lengths of 16, 32, and 64. To determine the optimal configuration associated with the location of the receiving antenna, we utilised the Hadamard codebook. The Hadamard codebook comprises a number of Hadamard matrices that provide a set of binary and orthogonal phase shift states ($\omega_l, \forall l \in [1, L]$) that can be used to modify the reflection of incoming electromagnetic waves in a desired direction or with a preferred phase shift by applying these values to the reflective elements, maximizing the SNR towards the Rx side. Algorithm (1) outlines the optimization process for selecting

Algorithm 1 Optimizing the Best RIS Configuration Towards Bob (H_{opt})

Initialization
Construct the Hadamard codebook $HD = \{H_1, H_2, \ldots, H_L\}$ of L matrices for the $(N_x \times N_y)$ RIS reflecting units
Initialize an empty list SNR^{Bob} to store the SNRs measured at Bob
SNR Measurement at the Legitimate Receiver (Bob)
for $i = 1$ to L **do**
    Apply the Hadamard matrix configuration H_i to the RIS
    Measure the average SNR $\overline{\text{SNR}}_i^{Bob}$ at Bob
    Append $\overline{\text{SNR}}_i^{Bob}$ to SNR^{Bob}
end for
Optimal Configuration Selection
Find the index $i^* = \arg\max_i \left(\overline{\text{SNR}}_i^{Bob}\right)$
Set the best RIS configuration: $H_{opt} = H_{i^*}$

TABLE IV: Experimental settings

Par.	Value	Description
F_c	3.75 GHz	Carrier frequency
T_x $(Gain)$	20 dB	The transmitter gain
R_x $(Gain)$	5 dB	The receiver gain
N	64, 128, 256	Number of subcarriers
CP $length$	16, 32, 64	The cyclic prefix length
SR	200 KHz	The sampling rate for the T_x and R_x
$Antennas$ $types$	Horn	T_x and R_x antennas types
$T_x \leftrightarrow RIS$	3 meters	The distance between the T_x and RIS
$RIS \leftrightarrow R_x$	9 meters	The distance between the RIS and R_x

the optimal RIS configuration to maximize signal strength at the designated receiver. Accordingly, we implemented the proposed re-authentication method by transmitting two consecutive OFDM symbols with the same structure presented in Fig. 3, representing the PHY-layer signature $\sigma_{V_i}^{PHY}$.

Fig. 9 shows the received OFDM symbol in the frequency domain after removing the CP and applying the FFT. This figure presents the received power in dB for each subcarrier when the RIS is ON and OFF. Note that, the scenario of the deactivated RIS corresponds to the case described in reference [30]. It can be seen that the power of the subcarriers carrying data has increased by approximately 2 dB with the activation of the RIS. This improvement is significant, especially for NLoS scenarios. Fig. 10 shows the PDF for hypothesis H_0 when the RIS is ON and OFF and for hypothesis H_1 for $N = 64$ subcarriers and SNR = 5 dB. The figure demonstrates that the activation of the RIS reduces the mean value for PDF$|_{H_0}$ compared to when the RIS is off. This reduction leads to a decrease in the overlap between PDF$|_{H_0}$ and PDF$|_{H_1}$, providing superior ROC curves under low SNR conditions.

Fig. 11 illustrates the ROC curve for varying SNR values SNR $\in \{0, -3, -6\}$ dB, $N = 64$ subcarriers, and with and without the use of the RIS. The figure demonstrates that decreasing the SNR value reduces P_d for a given P_{fa}. This result arises from the increasing overlap between both hypotheses as the SNR decreases. Furthermore, the figure indicates that activating the RIS improves ROC curves. For example, when the RIS is off, the P_d is approximately 0.92; see Fig. 11(b). However, with the RIS enabled, the P_d increases to approximately 0.99 for $P_{fa} \sim 0.2$, thereby demonstrating the ability of the RIS to enhance the authentication performance.

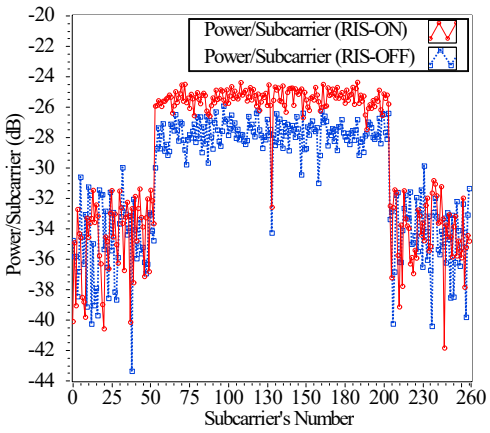


Fig. 9: The received symbol's power for each subcarrier at $N = 256$ subcarriers.

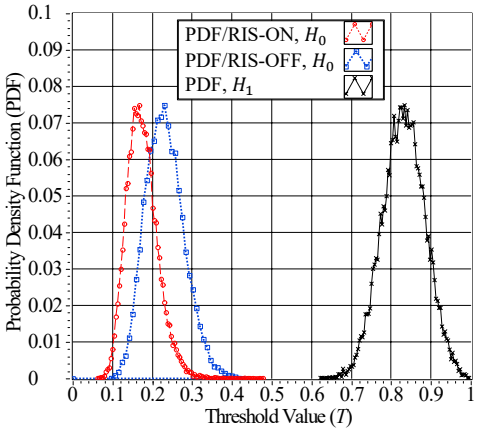
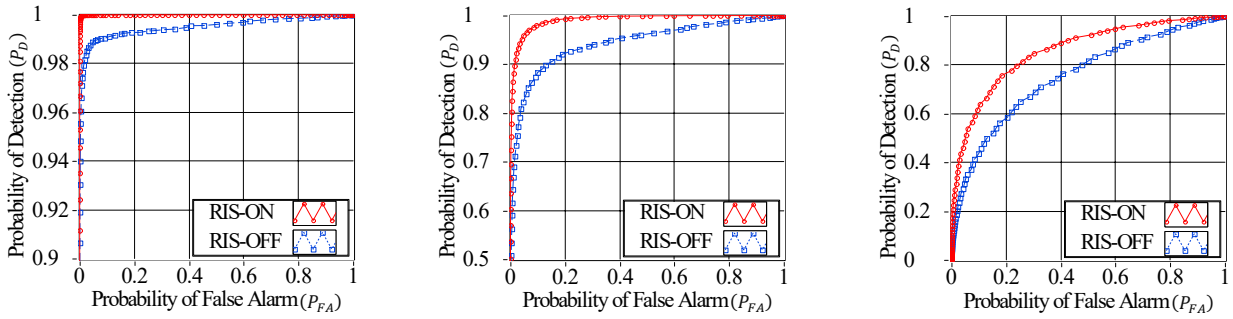


Fig. 10: Distributions of both hypotheses $H_{0,1}$ with and without the RIS for $N = 64$ subcarriers and SNR = 5 dB.

Additionally, we evaluate the ROC for different numbers of subcarriers $N = \{64, 128, 256\}$ and fixed SNR value of -6 dB, as presented in Fig. 12. Since v in (4) represents the circular variance of a specific number of $N_2 = 3N/4$ values, it follows the CLT. Hence, increasing the number of subcarriers results in an increase in N_2, which reduces the variance of $\mathcal{F}(x)|_{H_0}$ and minimises the overlap with $\mathcal{F}(x)|_{H_1}$, thereby improving the authentication performance. The enhanced ROC curves obtained in Fig. 12 affirm the effectiveness of increasing the number of subcarriers. Moreover, activating the RIS increases the P_d for a given P_{fa}. As shown in Fig. 12(b), when the RIS is off, the P_d is roughly 0.82. However, with the RIS enabled, the P_d increases to approximately 0.96 for $P_{fa} \sim 0.2$, thus demonstrating the beneficial impact of the RIS in enhancing authentication performance.

To further clarify the impact of mobility, it is important to note that the ROC of the proposed authentication scheme are influenced by two key factors: the Tx-Rx separation distance, which determines the SNR, and the velocity of the moving Rx, which introduces Doppler components. In our prior work [32], we systematically investigated this relationship using a Doppler emulator at fixed SNR values in a realistic vehicular environment, demonstrating that mobility (i.e., varying speed) significantly shifts the ROC performance.



(a) ROC with/without RIS at SNR = 0 dB (b) ROC with/without RIS at SNR = -3 dB (c) ROC with/without RIS at SNR = -6 dB

Fig. 11: The ROCs with and without the RIS at different SNRs and $N = 64$ subcarriers.

TABLE V: The time required for various crypto operations in $msec$

Symbol	The operation definition	Run time
T_{sm}^{BP}	BP-based scale multiplication in $\mathbb{G}_1$	0.6940
T_{pa}^{BP}	BP-based point addition in $\mathbb{G}_1$	0.0018
T_{sm}^{ECC}	ECC-based scale multiplication in $\mathbb{G}$	0.3218
T_{pa}^{ECC}	ECC-based point addition in $\mathbb{G}$	0.0024
T_h	One way hashing operation	0.0010

However, the main objective of this study is to evaluate the role of RIS in reinforcing signal quality and improving re-authentication performance under challenging NLoS and low-SNR conditions. A full-scale evaluation of RIS reconfiguration under realistic mobility, while essential, requires adaptive optimization for each instantaneous Tx/Rx position and is therefore considered for future work.

C. Comparison of computation and communication costs

This subsection presents the computation and communication analyses of the proposed method and shows that it outperforms traditional approaches.

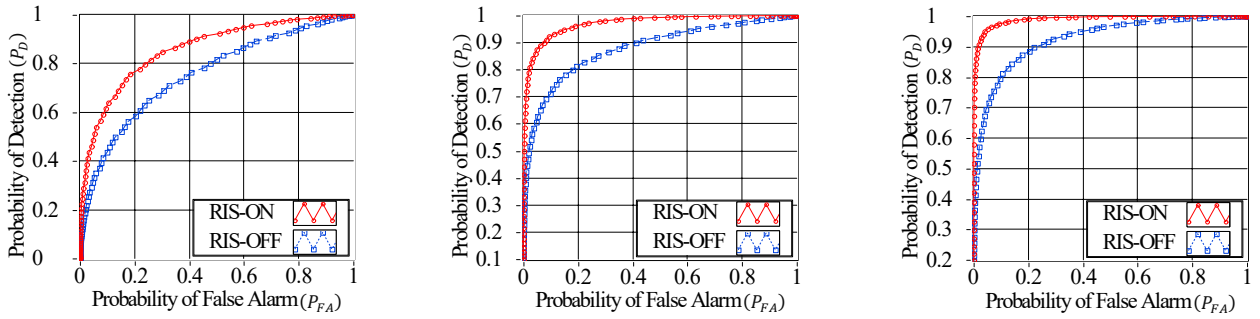
1) Comparison of computation cost: This part provides a detailed analysis of the computation comparison. Table V provides a summary of the running time for various crypto-based operations measured in [46] using the MIRACL cryptographic library [47] and a device equipped with an Intel Core $I7-6700$ processor. In Table V, the notations $\{T_{sm}^{BP}, T_{pa}^{BP}\}$ and $\{T_{sm}^{ECC}, T_{pa}^{ECC}\}$ denote the computational time for the BP-based and ECC-based scale multiplication and point addition, respectively. Furthermore, we evaluated the computational time for the mapping operation $T_{\mathcal{M}}$, and the circular variance operation in (5) denoted as $T_{c.var}$. The latter was insignificant compared to the values presented in Table V. Consequently, we have incorporated these results to accurately quantify the total computation cost of the proposed method and ensure a fair comparison, as listed in Table VI.

In our proposed scheme, the EC signature generation process incurs a cost of approximately $1T_{sm}^{ECC}$, while the verification process costs $2T_{sm}^{ECC}$. Based on this, the computation cost of transmitting n messages from a single vehicle using our method can be expressed as $[3T_{sm}^{ECC} + \lceil \frac{n}{Q} \rceil (2T_{sm}^{ECC} + T_h) + n(T_h + T_{\mathcal{M}})]$. The first term accounts for the signature generation and the secret key agreement, the second term accounts for the dynamically updating pseudo-identity after every Q transmitted messages, and the third term accounts for generating $\sigma_{V_i}^{PHY}$. On the other hand, the verification time can be expressed as $[2T_{sm}^{ECC} + \lceil \frac{n}{Q} \rceil (T_{sm}^{ECC} + T_h) + n(T_h + T_{\mathcal{M}} + T_{c.var})]$. The first term corresponds to the initial signature verification, and the second and third terms verify the pseudo-identity for every Q transmitted messages and $\sigma_{V_i}^{PHY}$, respectively. Thus, the total computation cost can be expressed as $(0.9654 + 0.3228\lceil \frac{n}{q} \rceil + 0.001n)\ msec$.

In Mohammed et al. [24], the computation cost for verifying n received messages is $[T_{sm}^{ECC} + (n)T_{pa}^{ECC}] = (0.3218 + 0.0024n)\ msec$, while for Cui et al. [25], Wang et al. [26], Li et al. [27], and Almazroi et al. [28], this value is $[(n+2)T_{sm}^{ECC} + (n-1)T_{pa}^{ECC} + (2n)T_h] = (0.6412 + 0.3262n)\ msec$, $[(3n+2)T_{sm}^{BP} + (2n)T_{pa}^{BP} + (n)T_h] = (1.388 + 2.0866n)\ msec$, $[(3n+2)T_{sm}^{BP} + (3n)T_{pa}^{BP} + (n)T_h] = (1.388 + 2.0884n)\ msec$, and $[(n+1)T_{sm}^{ECC} + (3n-1)T_{pa}^{ECC} + (n)T_h] = (0.3194 + 0.33n)\ msec$, respectively. To illustrate the comparison, Fig. 13 displays the computation cost required to verify 10000 received messages from a single user. Table VI and Fig. 13 indicate that the proposed scheme has a computational cost of approximately 13.87 ms, which is nearly half that of its closest competitors reported in [24].

2) Comparison of communication cost : This part provides a detailed comparison of communication costs. For the 80-bit security level of the proposed scheme, the elliptic curve group is denoted as $\mathbb{G}$, where $|\mathbb{G}| = 40$ bytes and $Z_q^* = 20$ bytes. For the same security level, the bilinear pairing is denoted as $\bar{E} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$, where $\bar{P}$ is the generator of the elliptic curve $\bar{E} : y^2 = x^3 + x \bmod \bar{p}$, with $|\mathbb{G}_1| = 128$ bytes and $Z_{\bar{q}}^* = 20$ bytes. Moreover, the size of hashed values using the SHA-1 hashing operation is 20 bytes, and the timestamp has a size of 4 bytes.

In the proposed scheme, the communication cost of transmitting n messages is determined by the size of the tuple $\langle TID_{V_i}, SPK_{V_i}, T_1, (PK_{V_i}, T_R, \sigma_{TA}), \sigma_{V_i} \rangle$ during the first transmission slot, as well as the size of the tuple $\langle PID_{V_i}, A_1, T_3, \sigma_{V_i}^{PHY} \rangle$ for n subsequent transmissions. Specifically, $\{SPK_{V_i}, PK_{V_i}, A_1\} \in \mathbb{G}$, and the length of TID_{V_i} and PID_{V_i} is 20 bytes each. The sizes of σ_{TA} and σ_{V_i} are 40 bytes each, while the lengths of T_R, T_1, and T_3 are 4 bytes each. The size of $\sigma_{V_i}^{PHY}$ is 48 bytes. Therefore, the total communication cost for transmitting n messages is $[(20 + 2 \times 4 + 4 \times 40) + (20 + 40 + 4 + 48)n] = (188 + 112n)$ bytes. In Mohammed et al. [24], the signature is represented



(a) ROC with/without RIS at $N = 64$ (b) ROC with/without RIS at $N = 128$ (c) ROC with/without RIS at $N = 256$

Fig. 12: The ROCs with and without the RIS at different numbers of subcarriers and SNR $= -6$ dB.

TABLE VI: Computation and communication comparisons

Scheme	Computation cost (*msec*)			Communication cost (*bytes*)
	Signature generation	Signature verification of n messages	Verifying 10000 messages	
[24]	$T_{sm}^{ECC} + T_{pa}^{ECC}$	$T_{sm}^{ECC} + (n)T_{pa}^{ECC}$	24.3218	$128n$
[25]	$3T_{sm}^{ECC} + 3T_h$	$(n+2)T_{sm}^{ECC} + (n-1)T_{pa}^{ECC} + (2n)T_h$	3262.64	$124n$
[26]	$2T_{sm}^{BP} + 2T_{pa}^{BP} + T_h$	$(3n+2)T_{sm}^{BP} + (2n)T_{pa}^{BP} + (n)T_h$	20867.4	$300n$
[27]	$3T_{sm}^{BP} + 2T_{pa}^{BP} + T_h$	$(3n+2)T_{sm}^{BP} + (3n)T_{pa}^{BP} + (n)T_h$	20885.4	$408n$
[28]	$2T_{sm}^{ECC} + 2T_{pa}^{ECC} + T_h$	$(n+1)T_{sm}^{ECC} + (3n-1)T_{pa}^{ECC} + (n)T_h$	3300.32	$124n$
Ours	$3T_{sm}^{ECC} + \lceil \frac{n}{Q} \rceil (2T_{sm}^{ECC} + T_h) + n(T_h + T_{\mathcal{M}})$	$2T_{sm}^{ECC} + \lceil \frac{n}{Q} \rceil (T_{sm}^{ECC} + T_h) + n(T_h + T_{\mathcal{M}} + T_{c.var})$	13.8716	$188 + 112n$

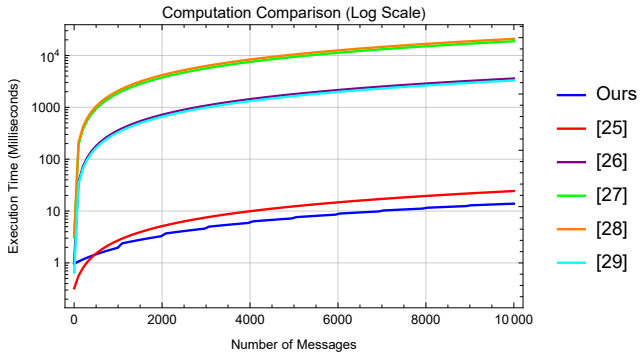


Fig. 13: The computation cost of verifying 10000 messages at $Q = 1000$.

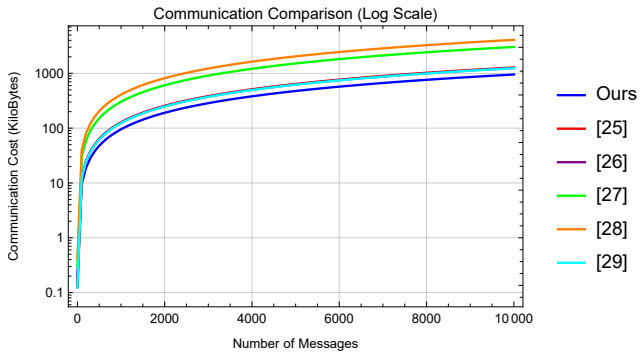


Fig. 14: The communication cost of sending 10000 messages.

by the tuple $\langle PID_i^1, PID_i^2, U_i, R_i, T_i \rangle$, where $|PID_i^1| = 64$ bytes, $\{PID_i^2, U_i, R_i\} \in Z_q^*$ and T_i is timestamp. Thus, the total size of the signature is $(64 + 3 \times 20 + 4) = 128$ bytes. In Cui et al. [25], the signature is represented by the tuple $\langle PID_j^1, PID_j^2, \delta_j, D_j, T_j \rangle$, where $\{PID_j^1, D_j\} \in \mathbb{G}$, $\{PID_j^2, \delta_j\} \in Z_q^*$, and T_j denotes the timestamp. Thus, the total size of the signature is $(2 \times 40 + 2 \times 20 + 4) = 124$ bytes. In Wang et al. [26], the signature is represented by the tuple $\langle R_{u_i}, T'_{u_i}, \varrho_{u_i}, PK_{TA}, t_i \rangle$, where $\{R_{u_i}, T'_{u_i}\} \in \mathbb{G}_1$, $\{\varrho_{u_i}, PK_{TA}\} \in Z_{\bar{q}}^*$, and t_i represents the timestamp. Thus, the total size of the signature is $(2 \times 128 + 2 \times 20 + 4) = 300$ bytes. Similarly, Li et al. [27] represent a signature as $\langle R_{u_i}, K'_{u_i}, KG'_{u_i}, \varrho_{u_i}, t_i \rangle$, where $\{R_{u_i}, K'_{u_i}, KG'_{u_i}\} \in \mathbb{G}_1$, $\varrho_{u_i} \in Z_{\bar{q}}^*$, and t_i denotes the timestamp. The total size of this signature is $(3 \times 128 + 20 + 4) = 408$ bytes. In Almazroi et al. [28], the signature is represented by the tuple $\langle AID_v, R_{pub}, D_{v,i}, T_{V,i}, \sigma_{v,i} \rangle$, where $\{R_{pub}, D_{v,i}\} \in \mathbb{G}$, $\{AID_v, \sigma_{v,i}\} \in Z_q^*$, and timestamp $T_{V,i} = 4$ bytes. Thus, the total size of this signature is $(2 \times 20 + 2 \times 40 + 4) = 124$ bytes. Fig. 14 shows the communication cost required for transmitting 10000 messages received from a single user. Our proposed scheme exhibits the lowest communication cost of at least ≈ 120 Kb less than that of its best competitors in [25].

VI. Conclusions

This paper proposes an authentication scheme that utilises the RIS to enhance the detection probability of the PHY-layer authentication in NLoS conditions while still adhering to the security and privacy requirements of VANETs. The theoretical and experimental results demonstrate the effectiveness of the RIS in improving authentication performance. We have performed informal and formal (BAN-logic) analyses to verify the scheme's security resistance against typical attacks. Additionally, we have conducted a computation and communication comparison to demonstrate that the proposed method reduces overheads, resulting in a computation cost savings of over 98% compared to existing methods in [25]–[27], and communication cost savings of approximately 10%, 62%, and 72% compared to [25], [26], and [27], respectively. Our future work will explore the possibility of incorporating the PHY-layer secret key extraction as an alternative key agreement

technique and implementing it in outdoor scenarios. Furthermore, we aim to extend the proposed scheme to dynamic vehicular environments by employing a mobile USRP testbed mounted on a railkit and integrating adaptive RIS configuration using machine learning to evaluate performance under realistic mobility conditions.

APPENDIX

A. ROM security prove

Proof. Considering an adversary $\mathcal{A}$ who is trying to impersonate the vehicle V_i during the initial authentication and message signing and verification phases. In this case, $\mathcal{A}$ must forge a valid signature σ_{V_i} and $\sigma_{V_i}^{PHY}$ by the construction of an algorithm C to solve the defined problems with a probability of success $\epsilon_{\text{Sig.Gen.}}$. Algorithm C initially holds two empty tables $T_{\sigma_{V_i}}[.]$ and $T_{SK_{i-k}}[.]$ to simulate random oracles $\sigma_{V_i}(.)$ and $SK_{i-k}(.)$, then answers $\mathcal{A}$'s oracle queries as follows:

- $\sigma_{V_i}(.)$ *queries*: For a query σ'_{V_i}, C holds $\{TID_{V_i}, Cert_{V_i}\}$, selects $\{SSK_{V_i}, SK_{V_i}\} \xleftarrow{\$} Z_q^*$ at T_1 timestamp, and calculates $SPK_{V_i} = SSK_{V_i} \cdot P$. Then, C generates its associated EC-signature using $T_{\sigma_{V_i}}[.]$, so that $T_{\sigma_{V_i}}[SK_{V_i}, TID_{V_i}, T_1, SPK_{V_i}, Cert_{V_i}] \leftarrow \sigma'_{V_i} \in \mathbb{G}$. of order q. If $T_{\sigma_{V_i}}[SK_{V_i}, \{TID_{V_i}, T_1, SPK_{V_i}, Cert_{V_i}\}]$ is defined, C halts, returns $\perp$, and sets $false \leftarrow true$. Otherwise, it returns σ'_{V_i} to $\mathcal{A}$ under SK_{V_i}.
- $SK_{i-k}(.)$ *queries*: For a query SK'_{i-k}, C holds m, randomly selects $a_1 \xleftarrow{\$} Z_q^*$, and computes $A_1 = a_1 \cdot P$ and $PID_{V_i} = TID_{V_j} \oplus H_1(a_1 \cdot PK_{R_k})$. Then, C generates the shared key SK_{i-k} using $T_{SK_{i-k}}[.]$, so that $T_{SK_{i-k}}[SSK_{V_i}] \leftarrow SK'_{i-k} \in \mathbb{G}$ of order q. If $T_{SK_{i-k}}[SSK_{V_i}]$ is defined, C halts, returns $\perp$, and sets $false \leftarrow true$. Otherwise, it returns SK'_{i-k} to $\mathcal{A}$ under SSK_{V_i}.

Finally, it is assumed that $\mathcal{A}$ successfully generated a forged signature $\langle TID_{V_i}, SPK_{V_i}, T_1, Cert_{V_i}, \sigma'_{V_i}\rangle$ under SK_{V_i} and $\langle m, PID_{V_i}, A_1, T_3, \sigma_{V_i}^{PHY}\rangle$ under SSK'_{V_i} based on q_s and q_k queries for $\sigma_{V_i}(.)$ and $SK_{i-k}(.)$ oracles with probability $\epsilon_{\text{Sig.Gen}} = \Pr[E_1]\Pr[E_2 \mid E_1]$, in which E_1 and E_2 are defined as:

- *Event* E_1 : The execution of Algorithm C did not halt as a result of $\{\sigma'_{V_i}, SK'_{i-k}\}$ generation.
- *Event* E_2 : Adversary $\mathcal{A}$ successfully generates a non-trivial forgery.

The probability $\Pr[\neg\text{false}]$ is to be calculated, where $\neg$false signifies that algorithm C does not abort due to the $\sigma_{V_i}(.)$ and $SK_{i-k}(.)$ queries. This probability is assessed based on the claims outlined below. Claim 1. $\Pr[E_1] = \Pr[\neg false] \geq 1 - \frac{q_s^2 q_k^2}{q^2}$

Proof. The probability $\Pr[\text{false}]$ can be determined by approximating the product of the following probabilities.

- *Scenario 1*. The event $false \leftarrow true$ is realised during the $\sigma_{V_i}(.)$ queries when σ'_{V_i} previously recorded in $\sigma_{V_i}(.)$ oracle under SK_{V_i}. With a maximum of q_s queries recorded in the $T_{\sigma_{V_i}}[.]$ table, the probability for an individual $\sigma_{V_i}(.)$ query remains at most $\frac{q_s}{q}$, and the cumulative probability for q_s queries stands at $\frac{q_s^2}{q}$.
- *Scenario 2*. The event $false \leftarrow true$ is realised during the $SK_{i-k}(.)$ queries when SK'_{i-k} previously recorded in $SK_{i-k}(.)$ oracle under SSK_{V_i}. With a maximum of q_k queries recorded in the $T_{SK_{i-k}}[.]$ table, the probability for an individual $SK_{i-k}(.)$ query remains at most $\frac{q_k}{q}$, and the cumulative probability for q_k queries stands at $\frac{q_k^2}{q}$.

Claim 2. $\Pr[E_2 \mid E_1] \geq \epsilon$

Proof. The term $\Pr[E_2 \mid E_1]$ denotes the probability that adversary $\mathcal{A}$ generates an authentic forgery, and algorithm C continues without termination due to the $\mathcal{A}$'s interactions involving $\sigma_{V_i}(.)$ and $SK_{i-k}(.)$ queries. This indicates that all responses to these queries are valid. As a result, adversary $\mathcal{A}$ is able to fabricate a valid forgery with a probability denoted by ϵ. Consequently, the probability that adversary $\mathcal{A}$ effectively impersonate V_i through the production of a significant forgery under the context of $\{SK_{V_i}, SSK_{V_i}\}$ is at least:

$$\epsilon_{\text{Sig.Gen}} = \epsilon\left(1 - \frac{q_s^2 q_k^2}{q}\right)$$

B. AVISPA simulation

This subsection presents the AVISPA simulation codes.

Code 1: HLPSL code for the role of the vehicle V_1, played by V_1

```
role role_V1 (V1,RSU:agent,PKTA,PKV1,PKRSU:public_key,
              SK12:symmetric_key,SND,RCV:channel(dy))
played_by V1
def=
        local
                State:nat,TR,T1,T2,T3,TIDV1,SPKV1,TIDRSU,
                SPKRSU,MSG,PIDV1,A1:text
        init
                State:=0
        transition
                1. State=0 /\ RCV(start) = | > State' := 1 /\ T1' :=
                   new() /\ TIDV1' := new() /\ SPKV1' := new() /\
                   SND(TIDV1'.SPKV1'.T1'.PKV1.TR.{PKV1.TR}
                   _inv(PKTA).{TIDV1'.SPKV1'.T1'.PKV1.TR.{PKV1.
                   TR}_inv(PKTA)}_inv(PKV1))
                   %% V1 hopes that SPKV1' will be verified by RSU
                   /\ witness(V1,RSU,auth_1,SPKV1')

                2. State=1 /\ RCV(TIDRSU'.SPKRSU'.T2'.PKRSU.
                   TR.{PKRSU.TR}_inv(PKTA). {TIDRSU'.
                   SPKRSU'.T1'.PKRSU.TR.{PKRSU.TR}
                   _inv(PKTA)}_inv(PKRSU)} = | > State' := 2 /\
                   T3' := new() /\ PIDV1' := new() /\ A1' := new()
                   /\ MSG' := new() /\ SND(MSG'.PIDV1'.A1'.T3'.
                   {MSG'.PIDV1'.A1'.T3'}_SK12)
                   %% V1 verifies the received SPKRSU' from RSU
                   /\ request(V1,RSU,auth_2,SPKRSU')
                   %% V1 hopes that MSG' will be verified by RSU
                   /\ witness(V1,RSU,auth_3,MSG')
end role
```

Code 2: HLPSL code for the role of the RSU R_k, played by R_k

```
role role_RSU (RSU,V1:agent,PKTA,PKV1,PKRSU:public_key,
               SK12:symmetric_key,SND,RCV:channel(dy))
played_by RSU
def=
        local
                State:nat,TR,T1,T2,T3,TIDV1,SPKV1,TIDRSU,
                SPKRSU,MSG,PIDV1,A1:text
        init
                State:=0
        transition
                1. State=0 /\ RCV(TIDV1'.SPKV1'.T1'.PKV1.TR.
                   {PKV1.TR}_inv(PKTA).{TIDV1'.SPKV1'.T1'.PKV1.
                   TR.{PKV1.TR}_inv(PKTA)}_inv(PKV1)) = | > State'
                   := 1 /\ T2' := new() /\ TIDRSU' := new() /\
                   SPKRSU' := new() /\ SND(TIDRSU'.SPKRSU'.T2'.
                   PKRSU.TR.{PKRSU.TR}_inv(PKTA)}_inv(PKRSU))
                   %% RSU verifies the received SPKV1' from V1
                   /\ request(RSU,V1,auth_1,SPKV1')
                   %% RSU hopes that SPKRSU' will be verified by V1
                   /\ witness(RSU,V1,auth_2,SPKRSU')

                2. State=1 /\ RCV(MSG'.PIDV1'.A1'.T3'.{MSG'.
                   PIDV1'.A1'.T3'}_SK12) = | > State' :=2
                   %% RSU verifies the received MSG' from V1
                   /\ request(RSU,V1,auth_3,MSG')
end role
```

Code 3: HLPSL code for the roles of session and environment

```
role session (V1,RSU:agent,PKTA,PKV1,PKRSU:public_key,
              SK12:symmetric_key)
def=
        local
                SND1,RCV1,SND2,RCV2:channel(dy)
        composition
                role_V1 (V1,RSU,PKTA,PKV1,PKRSU,SK12,
                         SND1,RCV1) /\
                role_RSU (RSU,V1,PKTA,PKV1,PKRSU,SK12,
                          SND2,RCV2)
end role
role environment ()
def=
        const
                pkta,pkv1,pkrsu:public_key,
                sk12:symmetric_key,
                v1,rsu:agent,
                auth_1,auth_2,auth_3:protocol_id
                intruder_knowledge={v1,rsu,pkta,pkv1,pkrsu}
        composition
                session(v1,rsu,pkta,pkv1,pkrsu,sk12)
end role
goal
                authentication_on auth_1,auth_2,auth_3
end goal
environment()
```

REFERENCES

[1] World Health Organization, "Road Traffic Injuries", 2021, available at: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

[2] World Health Organization (WHO), "Intelligent Transport Systems (ITS) for in-Vehicle and Infrastructure Safety: an Evidence-based Analysis", Geneva, Switzerland, 2016.

[3] M. A. Al-Shareeda, M. Anbar, I. Hasbullah, and S. Manickam, "Survey of Authentication and Privacy Schemes in Vehicular ad hoc Networks", *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2422-2433, Jan. 2015.

[4] S. Grafling, P. Mahonen, and J. Riihijarvi, "Performance Evaluation of IEEE 1609 WAVE and IEEE 802.11p for Vehicular Communications", ICUFN Conference, pp. 344-348, 2010.

[5] F. Qu, Z. Wu, F. -Y. Wang and W. Cho, "A Security and Privacy Review of VANETs", IEEE Trans. on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985-2996, Dec. 2015.

[6] M. Raya, and J. P. Hubaux, "The Security of Vehicular Ad Hoc Networks", in Proc. 3^{rd} ACM Workshop Security Ad Hoc Sensor Networks, pp. 11–21, Nov. 2005.

[7] A. Shamir, "Identity-based Cryptosystems and Signature Schemes", in Proc. Workshop Theory Applications Crypto. Technology, vol. 196, pp. 47–53, 1984.

[8] D. Chaum, and E. V. Heyst, "Group Signatures", Workshop on the Theory and Application of Crypto. Tech., vol. 547, pp. 257-265, 1991.

[9] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the Physical Layer for Wireless Authentication in Time-Variant Channels", *IEEE Trans. on Wireless Communications*, vol. 7, no. 7, Jul. 2008.

[10] J. Liu, and X. Wang, "Physical Layer Authentication Enhancement Using Two-Dimensional Channel Quantization", *IEEE Trans. on Wireless Communications*, vol. 15, no. 6, Jun. 2016.

[11] H. Fang, X. Wang, and L. Hanzo, "Learning-Aided Physical Layer Authentication as an Intelligent Process", *IEEE Trans. on Communications*, vol. 67, Nov. 2018.

[12] D. Chen, N. Zhang, R. Lu, X. Fang, K. Zhang, Z. Qin, and X Shen, "An LDPC Code Based Physical Layer Message Authentication Scheme With Prefect Security", *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 748-761, Apr. 2018.

[13] D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, and X. Shen, "Physical Layer based Message Authentication with Secure Channel Codes", *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1079-1093, Oct. 2020.

[14] D. Chen, S. Jiang, N. Zhang, L. Liu and K. -K. R. Choo, "On Message Authentication Channel Capacity Over a Wiretap Channel", *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3107-3122, Aug. 2022.

[15] S. Jiang, "Keyless Authentication in a Noisy Model", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 6, pp. 1024-1033, Jun. 2014.

[16] H. Wen, J. Zhang, R. Liao, J. Tang, and F. Pan, "Cross-Layer Authentication Method based on Radio Frequency Fingerprint", US 10251058 B2, United States Patent, Apr. 2019.

[17] M. A. Mughal, X. Luo, Z. Mahmood, and A. Ullah, "Physical unclonable function based authentication scheme for smart devices in internet of things", in Proc. 2018 IEEE Int. Conf. Smart Internet Things (SmartIoT), Xi'an, China, Aug. 2018, pp. 160–165.

[18] M.A. Shawky, S.T. Shah, Q.H. Abbasi, M. Hussein, M.A. Imran, S.F. Hasan, S. Ansari, A. Taha, "RIS-Enabled Secret Key Generation for Secured Vehicular Communication in the Presence of Denial-of-Service Attacks", *Sensors*, vol. 23, no. 8, Apr. 2023.

[19] Y. Liu, L. Wang and H. -H. Chen, "Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks", *IEEE Trans. on Vehicular Technology*, vol. 64, no. 8, pp. 3697-3710, Aug. 2015.

[20] M. R. Asaar et al., "A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks", *IEEE Trans. on Vehicular Technology*, vol. 67, no. 6, pp. 5409-5423, Jun. 2018.

[21] Y. Jiang, S. Ge, and X. Shen, "AAAS: An Anonymous Authentication Scheme Based on Group Signature in VANETs", *IEEE Access*, vol. 8, pp. 98986-98998, 2020.

[22] K. Lim, W. Liu, X. Wang, and J. Joung, "SSKM: Scalable and Secure Key Management Scheme for Group Signature Based Authentication and CRL in VANET", *Electronics*, vol. 8, no. 11, 2019.

[23] J. Shao, X. Lin, R. Lu, and C. Zuo, "A Threshold Anonymous Authentication Protocol for VANETs", *IEEE Trans. on Vehicular Technology*, vol. 65, no. 3, pp. 1711-1720, Mar. 2016.

[24] B. A. Mohammed et al., "FC-PA: Fog Computing-Based Pseudonym Authentication Scheme in 5G-Enabled Vehicular Networks", *IEEE Access*, vol. 11, pp. 18571-18581, 2023.

[25] J. Cui, J. Chen, H. Zhong et al., "Reliable and Efficient Content Sharing for 5G-Enabled Vehicular Networks", *IEEE Trans. on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1247-1259, Feb. 2022.

[26] Y. Wang, Y. Liu, and Y. Tian, "ISC-CPPA: Improverd-Security Certificateless Conditional Privacy-Preserving Authentication Scheme With Revocation", *IEEE Trans. on Vehicular Technology*, vol. 71, no. 11, pp. 12304-12314, Nov. 2022.

[27] J. Li, Y. Ji et al., "CL-CPPA: Certificate-Less Conditional Privacy-Preserving Authentication Protocol for the Internet of Vehicles", *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10332–10343, Dec. 2019.

[28] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: An Efficient Certificateless Authentication Scheme for 5G-Assisted Vehicular Fog Computing", *PLoS ONE*, vol. 18, no. 6, 2023.

[29] J. Wang, Y. Shao, Y. Ge, and R. Yu, "Physical-Layer Authentication based on Adaptive Kalman Filter for V2X Communication", *Vehicular Communications*, vol. 26, Jul. 2020.

[30] S. Althunibat, V. Sucasas, G. Mantas, and J. Rodriguez, "Physical-Layer Entity Authentication Scheme for Mobile MIMO Systems", *IET Communications*, vol. 12, pp. 712-718, Mar. 2018.

[31] H. Wen, and P.-H. Ho, "Physical Layer Technique to Assist Authentication Based on PKI for Vehicular Communication Networks", *KSII Trans. on Internet and Info. Sys.*, vol. 5, no. 2, Feb. 2011.

[32] M.A. Shawky, M. Usman, M.A. Imran et al., "Adaptive Chaotic Map-based Key Extraction for Efficient Cross-Layer Authentication in VANETs", *Vehicular Communications*, vol. 39, Feb. 2023.

[33] P. Zhang, J. Liu, Y. Shen, H. Li, and X. Jiang, "Lightweight Tag-Based PHY-Layer Authentication for IoT Devices in Smart Cities," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3977–3990, May 2020.

[34] L. Crosara, A.V. Guglielmi, N. Laurenti, and S. Tomasin, "Divergence-Minimizing Attack Against Challenge-Response Authentication with IRSs," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Denver, CO, USA, pp. 1986–1991, 2024.

[35] S. Tomasin, H. Zhang, A. Chorti, and H.V. Poor, "Challenge-Response Physical Layer Authentication over Partially Controllable Channels," *IEEE Communications Magazine*, vol. 60, no. 12, pp. 138–144, Dec. 2022.

[36] A. Bendaimi, A. Abdallah, A. Celik, A.M. Eltawil, and H. Arslan, "How to Leverage Double-Structured Sparsity of RIS Channels to Boost Physical-Layer Authentication," *IEEE Wireless Communications Letters*, vol. 13, no. 8, pp. 2260–2264, Aug. 2024.

[37] P. Zhang, Y. Teng, Y. Shen, X. Jiang, and F. Xiao, "Tag-Based PHY-Layer Authentication for RIS-Assisted Communication Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 6, pp. 4778–4792, Nov.–Dec. 2023.

[38] J. He, M. Niu, P. Zhang, and C. Qin, "Enhancing PHY-Layer Authentication in RIS-Assisted IoT Systems With Cascaded Channel Features," *IEEE Internet of Things Journal*, vol. 11, no. 14, pp. 24984–24997, Jul. 15, 2024.

[39] M.A. Shawky, S.T. Shah, Q.H. Abbasi, M. Hussein, M.A. Imran, S.F. Hasan, S. Ansari, and A. Taha, "RIS-Enabled Secret Key Generation for Secured Vehicular Communication in the Presence of Denial-of-Service Attacks," *Sensors*, vol. 23, no. 8, p. 4104, Apr. 2023.

[40] Certicom Research, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters 1.0, pp. 9–10, Sep. 2000.

[41] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A Privacy-Preserving Trust Model Based on Blockchain for VANETs", *IEEE Access*, vol. 6, pp. 45655-45664, Aug. 2018.

[42] M. Bellare, and P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols", 1 st ACM Conference on Computer and Communications Security, pp. 62–73, Nov. 1993.

[43] M.A. Shawky, M. Usman, D. Flynn, M.A. Imran, Q.H. Abbasi, S. Ansari, and A. Taha, "Blockchain-based Secret Key Extraction for Efficient and Secure Authentication in VANETs", *Journal of Information Security and Applications*, vol. 74, May 2023.

[44] H.E. Mohamadi, N. Kara, and M. Lagha, "Formal Verification of RGR-SEC, a Secured RGR Routing for UAANETs Using AVISPA," in *Scyther and Tamarin*. In: R. Doss, S. Piramuthu, W. Zhou (eds.), *Future Network Systems and Security*, FNSS 2018, *Communications in Computer and Information Science*, vol. 878, Springer, Cham, Jun. 2018.

[45] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, and S. Mödersheim, "The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications", International Conference on Computer Aided Verification, Springer, pp. 5-281, 2005.

[46] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "RSMA: Reputation System-Based Lightweight Message Authentication Framework and Protocol for 5G-Enabled Vehicular Networks", *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6417-6428, Aug. 2019.

[47] Shamus Software Ltd., Miracl library. Available: http://www.shamus.ie /index.php?page=home.