Cross-Layer Authentication based on Physical-Layer Signatures for Secure Vehicular Communication

Mahmoud A. Shawky†, Qammer H. Abbasi†, Muhammad Ali Imran‡, Shuja Ansari†, and Ahmad Taha†

Abstract—**In recent years, research has focused on exploiting the inherent physical (PHY) characteristics of wireless channels to discriminate between different spatially separated network terminals, mitigating the significant costs of signature-based techniques. In this paper, the legitimacy of the corresponding terminal is firstly verified at the protocol stack's upper layers, and then the re-authentication process is performed at the PHY-layer. In the latter, a unique PHY-layer signature is created for each transmission based on the spatially and temporally correlated channel attributes. Extensive simulation has shown the capability of the proposed scheme to support high detection probability at small signal-to-noise ratios. In addition, security evaluation is conducted against passive and active attacks. Moreover, computation and communication comparisons are performed to demonstrate that the proposed scheme provides superior performance compared to conventional cryptographic approaches.**

Keywords—Cross-Layer Authentication, Physical-Layer Signatures, Public Key Infrastructure, Wireless Security.

I. Introduction

Intelligent Transportation Systems are employed to facilitate direct connectivity between vehicles, pedestrians, and roadside infrastructures referred to as vehicular communication. By using wireless channels for communication between terminals, vehicular networks are susceptible to a wide range of attacks, such as impersonation, modification, and replay attacks [1]. Therefore, message authentication and integrity are crucial security services that must be assured to avoid these attacks. Most of the existing authentication schemes have been developed based on the difficulty of solving complex cryptographic problems, e.g., discrete logarithm and factorization problems [2]. However, the significant computational cost of the mathematical crypto operations limits the number of the communicating terminals in the network [3]. In response, researchers have come up with several solutions to this problem, including singular and bilinear batch verifications and using proxy vehicles to verify signatures on behalf of endpoint terminals [4-6]. Generally, the vehicular network structure consists of the trusted authority (TA), roadside units (RSUs), and vehicles' onboard units (OBUs).

Recently, many physical (PHY) layer discrimination techniques have been introduced to the research community as a promising solution to the significant costs of traditional signature-based schemes. Some of these techniques exploit the wireless channel reciprocity and randomness to ensure that the receiver is still in communication with the same transmitter [7-8]. These techniques are referred to as "feature tracking". Hardware imperfections attributes are also utilized to construct a radio frequency fingerprint for each terminal in the network [9-10]. However, these approaches demonstrated low reliability due to the signal quality fluctuation caused by the limited range of communication devices as well as the significant variations of channel attributes over time. Therefore, key-based PHY-layer authentication has been proposed as an alternative solution that requires a pre-agreed key for successful detection [11-12]. Nowadays, cross-layer authentication has emerged by integrating PHY-layer techniques with upper layers cryptographic signatures. However, choosing the proper PHY-layer technique must be compatible with the application's requirements in terms of computational resources availability, communication range, and number of network terminals.

In [13], a cross-layer scheme has been patented by integrating the Public Key Infrastructure (PKI) based authentication with RF fingerprinting for re-authentication. In fact, the small dissimilarities between the extracted features from different devices can mislead the decision rule, which cannot support high scalability. In [14-15], the integration is performed with feature tracking techniques. However, an extensive observation is essential to extract terminals' distinctive features for successful detection, in addition to the low detection probability at small signal-to-noise ratios. Reference [16] integrated the physically unclonable functions of the integrated circuits with a pseudo-identity signature-based algorithm. Unfortunately, the instability of these features due to voltage supply variations and electromagnetic interference constitutes a complex challenge. In summary, some of the mentioned works are applicable in resource-constrained applications. However, it is not applicable in long-range and high-speed dynamic terminals, e.g., vehicular communication. To address this gap, the proposed scheme in this paper uses PKI-based algorithm for initial identity verification followed by creating a PHY-layer orthogonal frequency division multiplexing (OFDM) signature for each subsequent transmission. This signature is considered as a PHY-layer message authentication code for the attached data packet that can only be equalized at the intended endpoint terminal.

The remainder of this paper is organized as follows. Section II describes the proposed scheme's structure. In Section III, threat modelling is discussed, while Section IV presents simulation results and comparisons. Finally, Section V concludes the current study.

†, ‡ The authors are with the Department of Electronics and Electrical Engineering, James Watt School of Engineering, University of Glasgow, Glasgow, G12 8QQ, United Kingdom {m.shawky.1@research.gla.ac.uk}, {Qammer.Abbasi, Muhammad.Imran, Shuja.Ansari, Ahmad.Taha}@glasgow.ac.uk.

† The authors are members of the Communications Sensing and Imaging research group at University of Glasgow.

‡ The author is the Dean University of Glasgow UESTC, Head of the Communications Sensing and Imaging (CSI) research group, and the Director of Glasgow UESTC Centre of Educational Development and Innovation.

II. Cross-Layer Authentication Scheme

In this section, the proposed scheme is firstly modelled, and then, in the following subsections, the scheme is discussed in detail.

A. *Scheme modelling*

The proposed scheme aims to authenticate the sender's identity and verify the message's integrity with minimum computation and communication costs. For vehicle-to-vehicle (V2V) communication, if V_i is in the transmission range of V_j and wants to initiate a trust connection, the authentication is carried out in a two-step process, as illustrated in Fig. 1, and explained below:

S1. During the first transmission slot, the corresponding terminal's legitimacy is initially verified using a signature-based authentication algorithm executed at the upper layers of the protocol stack.

S2. If the mutual verification succeeds, the re-authentication process is performed by generating a PHY-layer signature to the attached data packet, which is used to identify the message integrity. Otherwise, the initial verification step (S1) is aborted.

The generated PHY-layer signature can only be equalized at the side of the intended receiver based on the spatial and temporal correlation of channel responses between two communicating terminals within the coherence time interval T_c. For longer V2V communication distances, intermediate cooperative relays can also be employed to amplify and forward (AF) the received data packets, including the attached PHY-layer signatures. Table I lists the notations used in this paper.

B. *Signature-based authentication algorithm*

In this algorithm, each terminal verifies the legitimacy of the corresponding vehicle and generates a symmetric session key. In fact, the mutual authentication process consists of three primary phases.

S1.1. *System initialisation phase:* TA computes the algorithm's public parameters PPs as follows.

- Selecting at random two prime numbers p and q are used to generate the cyclic additive group $\mathbb{G}$ of the elliptic curve E: $x^3 + ax + b \ mod \ q$ based on the base-point P so that $a, b \in Finite\ Field(p)$ and $\Delta = 4a^3 + 27b^2 \neq 0$.
- Choosing the hash function $H_1: \{0,1\}^* \rightarrow \{0,1\}^{N_1}$.
- Randomly selecting TA's secret key $\beta \in Z_q^*$.

S1.2. *System registration phase:* For each registered vehicle V_i, TA has to do the following steps.

- TA creates a list of vehicle's anonymous certificates $[Cert_1, \ldots, Cert_z]$ by randomly selecting an array of secret keys $[sk_1, ..., sk_z] \in Z_q^*$ used to compute their corresponding public keys $[pk_1, ..., pk_z]$ for $pk_i = sk_i.P$ and $i = 1, ..., z$. For privacy preservation, all V_i's certificates are generated with different pseudo-identities $PIDv_i \in \{0,1\}^*$ to preserve V_i's real identity from exposure. Next, TA computes certificate signatures $[\sigma_{TA_1}, ..., \sigma_{TA_Z}]$ for $\sigma_{TA_i} = sign(H_1(pk_i \parallel PIDv_i \parallel T_R))_\beta$ where T_R is the certificate expiry date. Finally, a single certificate $Cert_i$ can be represented by the tuple $\langle PIDv_i, pk_i, T_R, \sigma_{TA_i} \rangle$.
- TA preloads a list of the generated certificates, their related secret keys $[sk_1, ..., sk_z]$, and the public parameters $PPs = \langle p, q, \mathbb{G}, P, a, b, H_1 \rangle$ into the V_i's OBU.

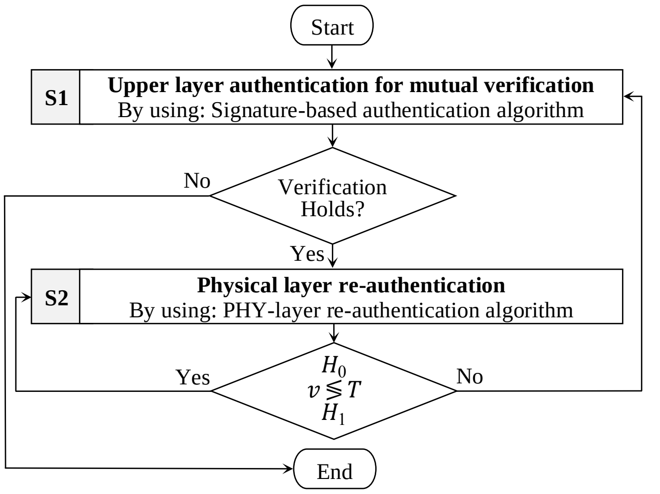

Fig. 1. Flowchart of the proposed cross-layer scheme.

TABLE I
NOTATIONS

Symbol	Definition
PPs	Scheme's public parameters
β	The system's master key
sk_{V_i}	The secret key of vehicle V_i
pk_{V_i}	Public key of vehicle V_i
$sk_{V_{i-j}}$	The symmetric session key between vehicles V_i and V_j
$Cert_{V_i}$	Digital public key certificate of vehicle V_i
T_R	Certificate expiry date in the order of a few minutes
σ_{TA}	The generated signature by the trusted authority (TA)
σ_{V_i}	The generated signature by vehicle V_i
PID_{V_i}	Pseudo-identity of vehicle V_i
T_i	The timestamp of the generated signature
H_1, H_2	One-way hash functions
ϕ_a, ϕ_b	The mapped signatures
$\mathcal{M}(.)$	Mapping operation
$\{sk_{V_{i-j}}\}_x, \{sk_{V_{i-j}}\}_y$	The x and y coordinates for the point $sk_{V_{i-j}} \in \mathbb{G}$
τ	Threshold value

S1.3. *Identity verification phase:* For secure communication between V_i and V_j, the following identification sub-steps must be executed:

S1.3.1. V_i picks up a certificate at random $Cert_{V_i} = \langle PID_{V_i}, pk_{V_i}, T_R, \sigma_{TA} \rangle$ and its related secret key sk_{V_i}, then signs the hashed $Cert_{V_i}$ at the T_1 timestamp using sk_{V_i} so that the generated signature can be expressed as $\sigma_{V_i} = sign(H_1(Cert_{V_i} \parallel T_1))_{sk_{V_i}}$. Finally, V_i sends the tuple $\langle Cert_{V_i}, T_1, \sigma_{V_i} \rangle$ to V_j.

S1.3.2. V_j uses the certified public key to verify the received signature $ver(\sigma_{V_i})_{pk_{V_i}}$, checks the freshness of the received timestamp T_1 to avoid replaying attacks, identifies the legitimacy of V_i by testing whether if $Cert_{V_i}$ is in the certificate revocation list (CRL), and stores V_i's $Cert_{V_i}$. The same process of signature generation is performed at the side of vehicle V_j by picking up at random $Cert_{V_j} = \langle PID_{V_j}, pk_{V_j}, T_R, \sigma_{TA} \rangle$ and its related secret key sk_{V_j}, computing the session key $sk_{V_{i-j}} = sk_{V_j}.pk_{V_i}$ and V_j's signature $\sigma_{V_j} = sign(H_1(Cert_{V_j} \parallel T_2))_{sk_{V_j}}$ at T_2 timestamp. Finally, V_j sends the tuple $\langle Cert_{V_j}, T_2, \sigma_{V_j} \rangle$ to V_i.

S1.3.3. V_i in turn verifies the received signature, checks the freshness of T_2, tests whether if $Cert_{V_j}$ is in the CRL, and then computes the session key $sk_{V_{i-j}} = sk_{V_i}.pk_{V_j}$.

Fig. 2 presents the identity authentication phase structure. This process is frequently updated with different $Cert_{V_i}$ and $Cert_{V_j}$ to avoid location tracking attacks [1].

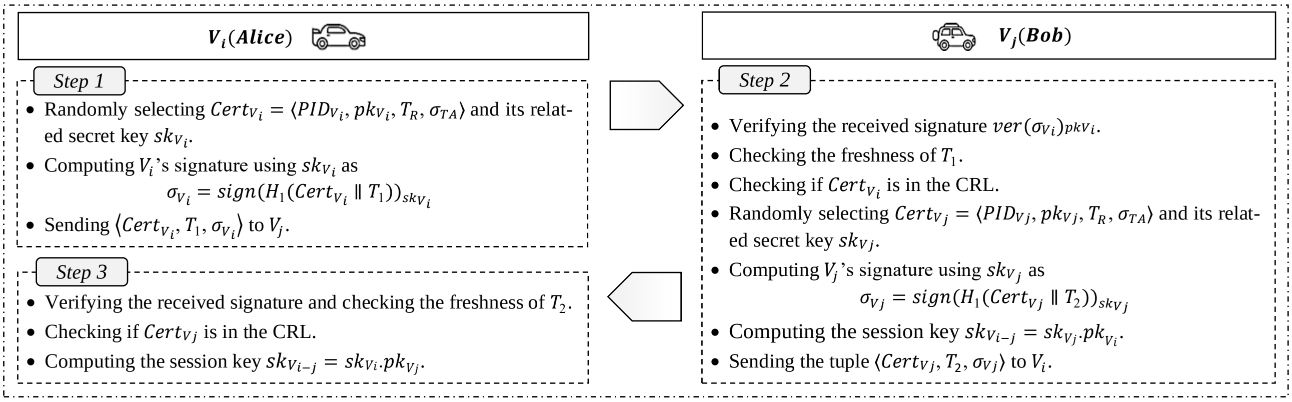

Fig. 2. Identity authentication phase structure.

C. PHY-Layer Re-authentication Algorithm

In this section, and after identifying the legitimacy of the corresponding terminal, the re-authentication process is presented in detail for OFDM system of N subcarriers, with all formulae expressed in the frequency domain. The computed session key $sk_{V_{i-j}} \in \mathbb{G}$ is used for generating the preliminary keys $[k_a, k_b]$ for $k_a = \{sk_{V_{i-j}}\}_x$ and $k_b = \{sk_{V_{i-j}}\}_y$. These sub-keys are used for generating the PHY-layer signature of the subsequent data packets, employing AF cooperative relaying between both terminals as shown in Fig. 3. Generally, the re-authentication step comprises three phases, i.e., system initialisation, PHY-layer signature generation, and verification.

S2.1. System initialisation phase: TA is also responsible for initialising the PHY-layer system public parameters as a part of the PPs presented in the signature-based algorithm.

• Mapping operation: $\mathcal{M}(X) \rightarrow Y$ is a 2-bits mapping operation that maps the input variable $X = \{x_1 x_2, ..., x_{2N-1} x_{2N}\}$ of length $|X| = 2N$ bits to generate Y as

$$Y_i = \mathcal{M}(X_i) = \begin{cases} 0 & X_i = [0\ 0] \\ \frac{\pi}{2} & X_i = [0\ 1] \\ \pi & X_i = [1\ 1] \\ \frac{3\pi}{2} & X_i = [1\ 0] \end{cases} \text{for } i = 1, \ldots, N \quad (1)$$

• Choosing the hash function H_2: $\{0,1\}^* \rightarrow \{0,1\}^{2N}$.

• Preloading the tuple $\langle H_2, \mathcal{M}(.) \rangle$ into vehicles' OBUs during the registration phase.

S2.2. *PHY-layer signature generation phase:* Let us consider $V_i(Alice)$ wants to send a safety-related message m to $V_j(Bob)$ within the same region. In that case, the PHY-layer signature generation process is performed through two main stages as follows.

1) *Signature preparation stage:* V_i generates the signature of the hashed tuple $\langle PID_{V_i}, T_3, m \rangle$ by estimating ϕ_a and ϕ_b, in which $\phi_a = \mathcal{M}(H_2(k_a \parallel m \parallel PID_{V_i} \parallel T_3))$ and $\phi_b = \mathcal{M}(H_2(k_b \parallel m \parallel PID_{V_i} \parallel T_3))$ are created at T_3 timestamp.

2) *OFDM symbols initialisation stage:* In this stage, two subsequent OFDM symbols are initiated by V_i at two subsequent time slots t_0 and $t_0 + \Delta t$ for $\Delta t < T_c$ with random phases θ_i uniformly distributed over $[0, 2\pi)$ and the mapped signatures ϕ_a and ϕ_b. The generated signals of the i^{th} subcarrier can be formulated as

$$s_{a,i}(t_0) = exp(j(\theta_i + \phi_{a,i})) \quad (2)$$

$$s_{a,i}(t_0 + \Delta t) = exp(j(\theta_i + \phi_{b,i})) \quad (3)$$

where i ranges from 1 to N. Finally, the tuple $\langle PID_{V_i}, T_3, m \rangle$ is concatenated with the generated OFDM symbols and sent to V_j. The transmission can be done directly or through R intermediate cooperative relays using amplify and forward technique.

S2.3. *PHY-layer signature verification phase:* The received symbols by V_j at time t_1 and $t_1 + \Delta t$ can be formulated in a noiseless channel as

$$r_{b,i}(t_1) = \prod_R |h_{R,i}|\, exp(j(\theta_i + \phi_{a,i} + \sum_R \xi_{R,i})) \quad (4)$$

$$r_{b,i}(t_1 + \Delta t) = \prod_R |h_{R,i}|\, exp(j(\theta_i + \phi_{b,i} + \sum_R \xi_{R,i})) \quad (5)$$

where $\prod_R |h_{R,i}|$ and $\sum_R \xi_{R,i}$ are the i^{th} subcarrier fading coefficient and the channel-phase response between legitimate communication nodes, passing through a number of R intermediate terminals. In the same coherence interval, channel attributes between both terminals are correlated. Thus, the channel responses $(h_{R,i}(t_1), \xi_{R,i}(t_1))$ and $(h_{R,i}(t_1 + \Delta t), \xi_{R,i}(t_1 + \Delta t))$ are highly correlated for $\Delta t < T_c$. The received signals of equations (4) and (5) can only be equalized at the side of V_j based on the symmetric session key $sk_{V_{i-j}}$ and the received tuple $\langle PID_{V_i}, T_3, m \rangle$ according to the following stages.

1) *Signature equalization stage:* V_j computes $\hat{\phi}_a = \mathcal{M}(H_2(k_a \parallel m \parallel PID_{V_i} \parallel T_3))$ and $\hat{\phi}_b = \mathcal{M}(H_2(k_b \parallel m \parallel PID_{V_i} \parallel T_3))$. Then, V_j equalizes the received signals as

$$\begin{aligned} c_{1,i}(t_1) &= r_{b,i}(t_1) exp(-j(\hat{\phi}_{a,i})) \\ &= \prod_R |h_{R,i}|\, exp(j(\theta_i + \phi_{a,i} - \hat{\phi}_{a,i} + \sum_R \xi_{R,i})) \\ &= \prod_R |h_{R,i}|\, exp(j(\theta_i + \sum_R \xi_{R,i})) \end{aligned} \quad (6)$$

$$\begin{aligned} c_{2,i}(t_1 + \Delta t) &= r_{b,i}(t_1 + \Delta t) exp(-j(\hat{\phi}_{b,i})) \\ &= \prod_R |h_{R,i}|\, exp(j(\theta_i + \phi_{b,i} - \hat{\phi}_{b,i} + \sum_R \xi_{R,i})) \\ &= \prod_R |h_{R,i}|\, exp(j(\theta_i + \sum_R \xi_{R,i})) \end{aligned} \quad (7)$$

2) *Signature verification stage:* V_j checks the freshness of the received timestamp T_3, then verifies the integrity of the received message by computing the circular variance [17] $Var(.)$ of $\angle c_i(t) = \angle(c_{1,i}(t_1) c_{2,i}^*(t_1 + \Delta t))$ as

$$v = Var(\sum_{i=1}^{N} \angle(c_{1,i}(t_1) c_{2,i}^*(t_1 + \Delta t)) \quad (8)$$

Suppose a third party $V_e(Eve)$ is trying to impersonate V_i or modify the message contents. In that case, it is considered that Eve initiated a different key K_e for the signature generation stage which can be represented as a binary hypothesis testing problem as:

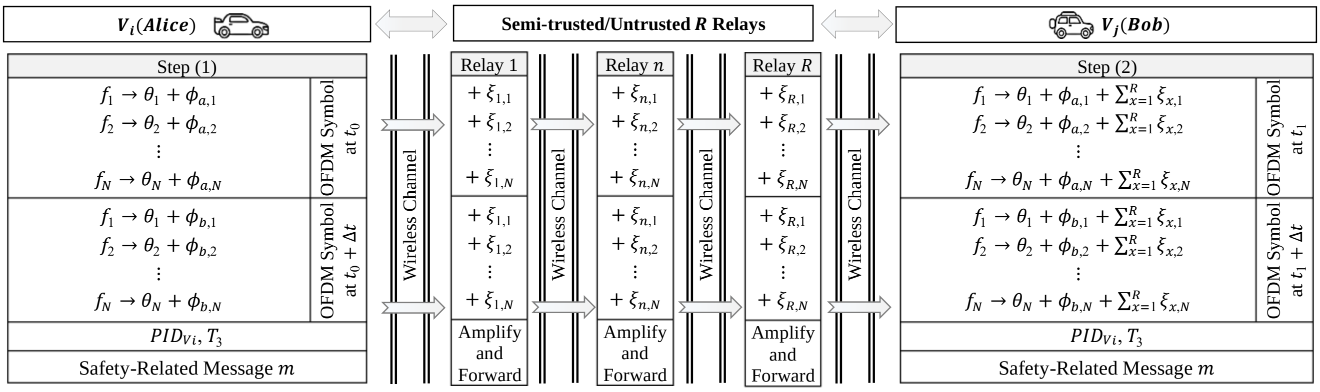

Fig. 3. PHY-layer re-authentication algorithm for multi-carrier communication.

$$v \underset{H_1}{\overset{H_0}{\lessgtr}} \tau, \text{ for} \begin{cases} H_0: & \hat{\phi}_a = \phi_a \ \&\ \hat{\phi}_b = \phi_b \\ H_1: & \hat{\phi}_a \neq \phi_a \ \&\ \hat{\phi}_b \neq \phi_b \end{cases} \quad (9)$$

Taking the value v in comparison with the threshold value τ leads to the final decision (H_0 denotes Alice is authenticated as a legitimate terminal, otherwise H_1).

III. Threat Modelling

Eve acts as an attacker who is familiar with the network configuration and scheme structure. However, she is unaware of the symmetric session key skv_{i-j} between legitimate parties, Alice and Bob. Considering Eve as a passive attacker who eavesdrops on the transmitted PHY-layer signatures and tries to derive the correct sub-keys, it is hard for Eve to differentiate between the mapped signatures ϕ_a and ϕ_b and random phases θ_i. Thus, Eve is considered to be an active adversary who is capable of executing three primary attacks as follows.

1) *Impersonation attack:* In this attack, Eve is trying to impersonate Alice to generate a correct PHY-layer signature. However, she cannot generate a correct estimation due to her unawareness of the authenticated key.
2) *Replay attack:* In this attack, Eve attempts to retransmit a previously sent message by Alice. However, the recipient checks the freshness of each received signature based on the attached timestamp T_3, making such an attack easy to detect.
3) *Modification attack:* In this attack, Eve alters Alice's message content and returns it to Bob. In contrast, she cannot compute the correct PHY-layer signature related to the altered message due to her unawareness about skv_{i-j}.

IV. Performance Evaluation

In this section, the effectiveness of the proposed scheme is evaluated based on simulation analysis, and then a comparison of computation and communication costs is presented.

A. Simulation analysis

The probability density functions (PDFs) are evaluated at different signal-to-noise ratios (SNRs) in order to determine the detection probability P_d under different false alarm values P_{fa}. An extensive Monte-Carlo simulation is conducted to obtain accurate estimates of the PDFs. Since v in equation (8) is the circular variance of N samples, v is subject to the central limit theorem and can be approximated as a normally distributed random variable with means and variances $\mu_{H0,1}$ and $\sigma^2_{H0,1}$, respectively, as shown in Fig. 4. The PDFs for both hypotheses are ideally separated, allowing the determination of the proper threshold value τ.

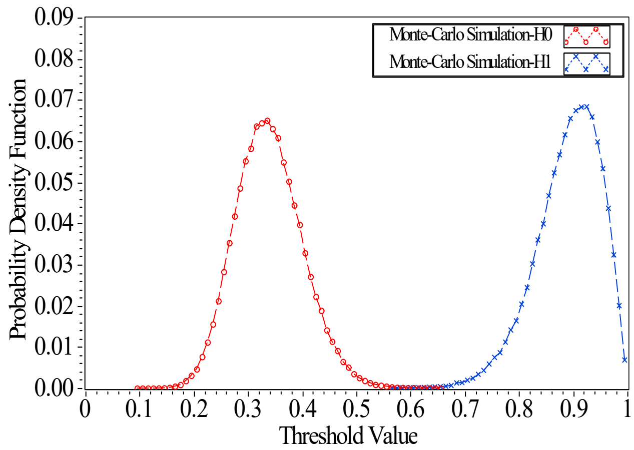

Fig. 4. PDFs for both hypothesis at SNR = 5 dB and $R = 0$ Relays.

In order to evaluate the performance of the proposed algorithm, the receiver operating characteristics (ROCs; P_d versus P_{fa}) are evaluated at different SNR values [5, 0, -2, -5] dB, as illustrated in Fig. 5. It can be noted that high $P_d \geq 0.9$ is obtained for end-to-end direct transmission at small SNR up to -2 dB and acceptable $P_{fa} \leq 0.1$. In Fig. 6, the ROCs are estimated for different numbers of R intermediate relays at SNR = 5 dB. This implies that increasing the number of relays reduces the ROCs. However, this can support V2V communication for longer distances. For higher performance and hence the PDFs obey the central limit theorem, a higher number of subcarriers could be considered, leading to high P_d at very small SNR values (-5 dB), as demonstrated in Fig. 7.

B. Computation and Communication Overheads

In this part, comparisons of computation and communication costs of verifying and transmitting n signatures are tabulated in II. In Table II, T_m, T_e, T_h, $T_{M\to P}$, and $T_{\mathcal{M}}$ are the time required for executing a scalar multiplication, bilinear pairing, hash function, map-to-point hash function, and mapping operation, respectively. The computational cost of the verification process is evaluated for the overall scheme to be $[T_m + n(2T_h + 2T_{\mathcal{M}})]$ in which T_m is the time needed to generate the shared session key at the first time slot, while $[2T_h + 2T_{\mathcal{M}}]$ is the consumed time for verifying n subsequent received PHY-layer signatures. The communication cost is $[1184 + n(2N + 192)]$ bits, assuming the size of the transmitted tuple $\langle Cert_{V_i}, T_i, \sigma_{V_i}\rangle$ = 832+32+320 = 1184 bits for the first transmission and $[2N+192]$ bits for the PHY-layer signature of length $2N$ and $\langle PID_{V_i}, T_i\rangle$ = 160+32 = 192 bits at the subsequent n transmissions.

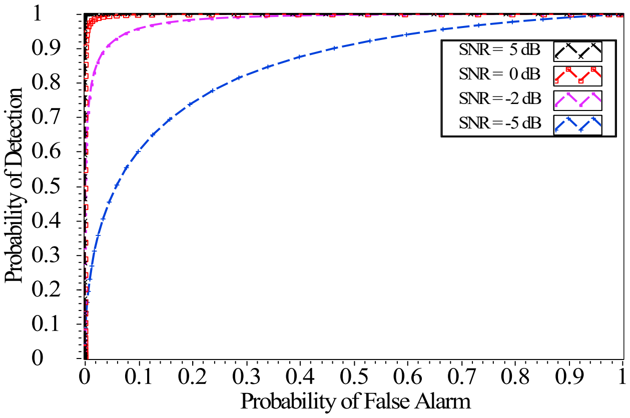

Fig. 5. ROCs at different SNR values and $R = 0$ Relays.

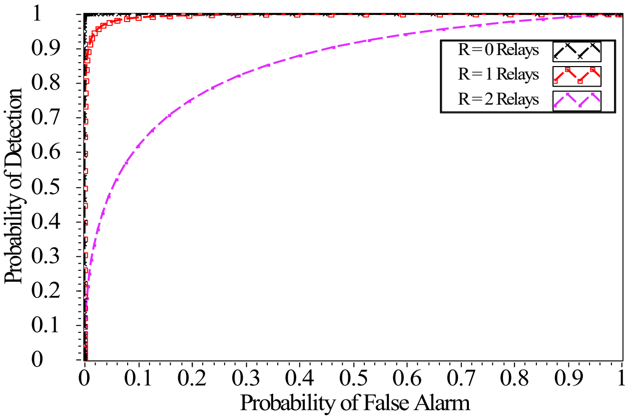

Fig. 6. ROCs at SNR = 5 dB and different number of Relays.

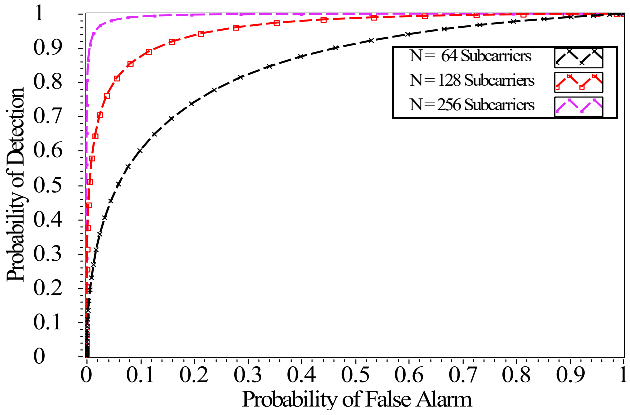

Fig. 7. ROCs at SNR = -5 dB, $R = 0$ Relays and different N subcarriers.

Fig. 8 shows the computation and communication costs of verifying and transmitting 1000 signatures from a single vehicle. It can be noted that the proposed scheme can save [77%, 94%] computation and [64%, 37%] communication costs compared to CPPA [4] and NERA [5], respectively.

V. Conclusions

This paper exploits the inherent wireless channel properties to create a PHY-layer OFDM signature that functions as an alternative to the traditional cryptographic signatures, reducing the considerable signalling and computation overheads of PKI-based approaches. Extensive simulations proved that the proposed scheme is effective and can provide a high authentication rate at small SNR values. In addition, we carefully evaluated the immunity of this work against possible passive and active attacks, thus proving that the novel algorithm successfully ensures the integrity of message contents. Furthermore, comparisons are made in terms of computation and communication costs to prove that the proposed scheme can save significant costs compared to conventional techniques. In future work, a PHY-layer secret key extraction algorithm such as [18] could be used to create a dynamic PHY-layer signature using the extracted location-dependent shared key.

TABLE II
Computation and Communication Costs

Schemes	Computation cost	Communication cost (bytes)
CPPA [4]	$(n+2)T_m$	$107n$
NERA [5]	$3T_e + nT_m + nT_{M\rightarrow P}$	$62n$
Ours	$T_m + n(2T_h + 2T_{\mathcal{M}})$	$148+n(N/4+24)$

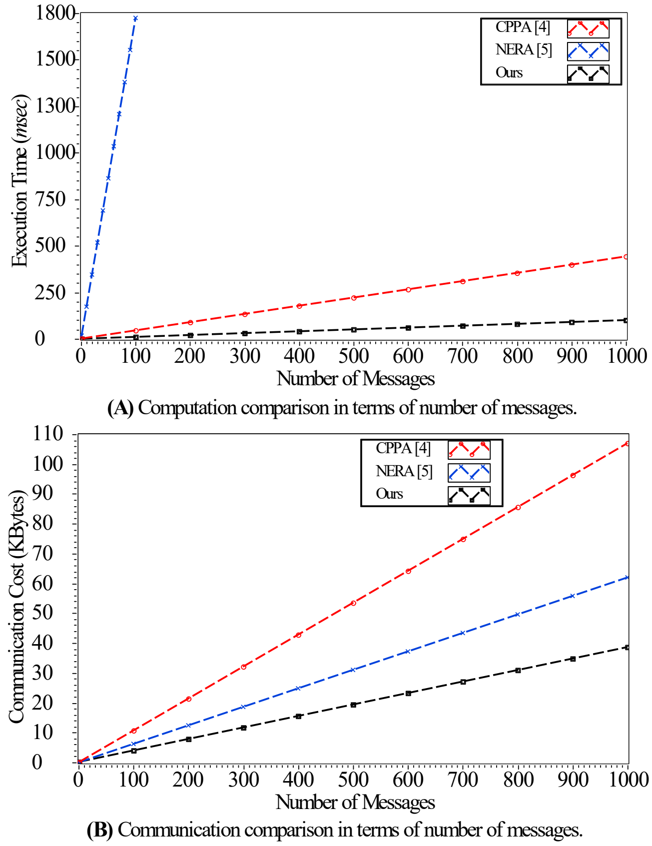

Fig. 8. Comparisons of compuation and communication costs.

References

[1] W. Jaballah, M. Conti, and C. Lal, "Security and Design Requirements for Software-defined VANETs", *Computer Networks*, vol. 169, March 2020.

[2] X. Wang, P. Hao, and L. Hanzo, "Physical-Layer Authentication for Wireless Security Enhancement: Current Challenges and Future Developments", *IEEE Communications Magazine*, vol. 54, no. 6, pp. 152-158, June 2016.

[3] M. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "An Efficient Identity-Based Conditional Privacy-Preserving Authenticat-ion Scheme for Secure Communication in a Vehicular Ad Hoc Netw-ork", *Symmetry*, vol. 12, October 2020.

[4] N. W. Lo., and J. L. Tsai, "An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks without Pairings", *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319-1328, May 2016.

[5] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A New and Efficient RSU based Authentication Scheme for VANETs", *Wireless Networks*, vol. 26, pp. 3083-3098, June 2019.

[6] Y. Liu, L. Wang, and H. Chen, "Message Authentication using Proxy Vehicles in Vehicular Ad hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3697-3710, August 2015.

[7] W. Chin, T. Le, and C. Tseng, "Authentication Scheme for Mobile OFDM based on Security Information Technology of Physical Layer over Time-Variant and Multipath Fading Channels", *Information Sciences*, vol. 321, pp. 238-249, November 2015.

[8] J. Liu, and X. Wang, "Physical Layer Authentication Enhancement using Two-Dimensional Channel Quantization", *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4171-4182, June 2016.

[9] W. Hou, X. Wang, J. Chouinard, and A. Refaey, "Physical Layer Authentication for Mobile Systems with Time-Varying Carrier Frequency Offsets", *IEEE Transactions on Communications*, vol. 62, no. 5, pp. 1658-1667, May 2014.

[10] P. Ramabadran, P. Afanasyev, D. Malone, M. Leeser, D. McCarthy, B. O'Brien, R. Farrell, and J. Dooley, "A Novel Physical Layer Authentication with PAPR Reduction based on Channel and Hardware Frequency Responses", *IEEE Transactions on Circuits and Systems*, vol. 67, no. 2, pp. 526-539, February 2020.

[11] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Networks", *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, September 2013.

[12] X. Wu, and Z. Yang, "Physical-Layer Authentication for Multi-Carrier Transmission", *IEEE Communications Letters*, vol. 19, no. 1, pp. 74-77, January 2015.

[13] 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, April 2019.

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

[15] Hong Wen, and Pin-Han Ho, "Physical Layer Technique to Assist Authentication based on PKI for Vehicular Communication Netwo-rks", KSII Transactions on Internet and Information Systems, vol. 5, no. 2, February 2011.

[16] P. Gope, A. Kumar Das, N. Kumar, and Y. Cheng, "Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks", *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, September 2019.

[17] P. Berens, "CircStat: A MATLAB Toolbox for Circular Statistics", *Journal of Statistical Software*, vol. 31, issue 10, September 2009.

[18] M. Bottarelli, P. Karadimas, G. Epiphaniou, D. Kbaier B. Ismail, and C. Maple, "Adaptive and Optimum Secret Key Establishment for Secure Vehicular Communications and Sensing", *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2310-2321, March 2021.