An Efficient Cross-Layer Authentication Scheme for Secure Communication in Vehicular Ad-Hoc Networks

Mahmoud A. Shawky, *Student Member, IEEE*, Mirko Bottarelli, *Student Member, IEEE*, Gregory Epiphaniou, *Member, IEEE*, and Petros Karadimas, *Senior Member, IEEE*

***Abstract*—Intelligent transportation systems contribute to improved traffic safety by facilitating real-time communication between vehicles and infrastructures. In this context, message authentication is crucial to safeguard vehicular ad-hoc networks (VANETs) from malicious attacks. The current state-of-the-art for authentication in VANETs relies on conventional cryptographic primitives, introducing significant computation and communication overheads. This paper presents a cross-layer authentication scheme for vehicular communication, incorporating the short-term reciprocal features of the wireless channel for re-authenticating the corresponding terminal, reducing the overall complexity and computation and communication overheads. The proposed scheme comprises four steps: S1. Upper-layer authentication is used to determine the legitimacy of the corresponding terminal at the first time slot; S2. Upon the verification result, a location-dependent shared key with a minimum number of mismatched bits is extracted between both terminals; S3. Using the extracted key and under binary hypothesis testing, a PHY challenge-response algorithm for multicarrier communication is proposed for re-authentication; S4. In the case of false detection, the key extraction step (S2) is re-executed after adapting the quantisation levels at different conditions of channel non-reciprocity based on the feedback from the re-authentication step (S3). Simulation results show the effectiveness of the proposed scheme even at small signal-to-noise ratios. In addition, the immunity of the proposed scheme is proved against active and passive attacks, including signatures' unforgeability against adaptive chosen message attacks in the random oracle model. Finally, a comprehensive comparison in terms of computation and communication overheads demonstrates the superiority of the proposed scheme over its best rivals.**

***Index Terms*—Cross-layer authentication, PHY-layer re-authentication, Privacy-preserving, Pseudo-identity, VANETs.**

Manuscript received 11 February 2022; revised 15 November 2022 and 9 January 2023; accepted 7 February 2023. Date of publication 10 February 2023; date of current version 18 July 2023. The work of Petros Karadimas was supported by the Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/R041660/1: Bandwidth and Energy Efficient Compact Multi-Antenna Systems for Connected Autonomous Vehicles. The review of this article was coordinated by Prof. Heejo Lee. *(Corresponding author: Mahmoud A. Shawky.)*

Mahmoud A. Shawky is with the James Watt School of Engineering, University of Glasgow, G12 8QQ, Glasgow, U.K. (e-mail: 2569186S@student.gla.ac.uk).

Mirko Bottarelli and Gregory Epiphaniou are with the Secure Cyber Systems Research Group (SCSRG), Warwick Manufacturing Group(WMG), University of Warwick, CV4 7AL Coventry, U.K. (e-mail: mirko.bottarelli.1@warwick.ac.uk; gregory.epiphaniou@warwick.ac.uk).

Petros Karadimas is with the School of Computing, Engineering and the Built Environment, Edinburgh Napier University, EH11 4BN Edinburgh, U.K. (e-mail: p.karadimas@napier.ac.uk).

Digital Object Identifier 10.1109/TVT.2023.3244077

I. Introduction

GLOBALLY, road traffic injuries and fatalities reach about 1.3 million annually and are expected to become the fifth leading cause of death by 2030, according to the "2^{nd} global status report on road safety" [1]. In 2020, the European Commission reported a decrease in fatal road crashes by about 23% compared to 2010 [2], and it aims to reach zero fatalities by 2050. For the next decade, a safety framework plan is published in [3] to enhance safety and efficiency in transportation, adapting technology to develop and implement intelligent road systems based on sensors' data distributed via VANETs.

A typical VANET architecture consists of trusted/certificate authority (TA/CA), multiple fixed roadside units (RSUs), and onboard units. The latter is a vehicle-mounted wireless communication device that enables a vehicle to communicate with adjacent vehicles and surrounding RSUs via the dedicated short-range communication (DSRC) protocol [4]. In DSRC protocol, each vehicle sends a safety-related message every 100-300 $msec$. These messages support many road traffic applications, e.g., on-road services, and urban sensing [5]. For ease of understanding, the acronyms used in this paper are listed in Table I.

In VANETs, the wireless communication channel is an open access shared medium that makes it susceptible to many adversarial active and passive attacks. For instance, a malicious vehicle can frame an emergency to mislead other drivers into slowing down, and braking; impersonate a legitimate vehicle; replay a significant number of bogus messages, which creates an unrealistic traffic situation. These attacks can cause serious problems, e.g., traffic jams or accidents. Therefore, message authentication must be established to identify the sender's legitimacy. Until now, many of the existing authentication schemes are based on the conventional public key infrastructure (PKI) [6], [7], [8]. In these schemes, a digital certificate is used to prove the ownership of the public key attached to a particular user in the network. These certificates are issued, revoked, and stored by the CA. A digital public key certificate must be attached to each transmitted message which occupies 30% of the available bandwidth [9], degrading the communication performance. Moreover, a large storage area is needed to store these certificates [10]. Furthermore, revoking a malicious terminal by distributing its issued certificates among vehicles as a part of the certificate revocation list (CRL) creates an additional significant communication load.

TABLE I
LIST OF ACRONYMS

Acronym	Description
ACPPA	A Conditional Privacy Preservation Authentication
BP	Bilinear Pairing
CLT	Central Limit Theorem
CPPA	Conditional Privacy-Preserving Authentication
DSRC	Dedicated Short-Range Communication
ECC	Elliptic Curve Cryptosystem
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ID-MAP	Identity-based Message Authentication using Proxy vehicles
ID-SPS	Identity-based Security and Privacy Scheme
MIRACL	Multi-precision Integer and Rational Arithmetic C++ Library
NERA	New and Efficient RSU-based Authentication
OFDM	Orthogonal Frequency Division Multiplexing
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
ROC	Receiver Operating Characteristic
TPD	Tamper Proof Device

TABLE II
CLASSIFICATION OF PERFORMANCE EVALUATION METRICS

Evaluation metric	Classification category		
	Low	Medium	High
Computation overhead ($bytes$)	1 : 50	51 : 100	101 : 140
Communication overhead ($msec$)	1 : 3	3.1 : 6	6.1 : 10

Different techniques have been developed to ease the heavy burden of managing CRLs. Online certificate status protocol (OCSP) is an alternative revocation mechanism in which OCSP servers reply to the terminal's certificate queries with signed responses, indicating the validation status of these certificates [11]. However, the TA's master key must be distributed among servers to manage the heavy load of these queries, degrading VANET's security strength against compromised servers. An intruder with a compromised server's master key can abuse that key to create fake responses.

To tackle PKI limitations, Shamir introduced an identity-based security and privacy scheme (ID-SPS) in [12]. In this scheme, the recipient authenticates the received signatures based on the sender's public key while signing messages using its private key. However, such a scheme suffers from high computation and communication overheads of the large-scale mathematical cryptographic operations executed at the protocol stack's upper layers (link and application layers) that cannot support high scalability and low latency. Scalable networks can add extra terminals without degradation in performance, which is the main objective of many studies [13], [14], [15]. Reference [13] proposed an identity-based message authentication scheme using proxy vehicles, in which n signatures are distributed between $\lceil \frac{n}{d} \rceil$ proxy vehicles for the signature verification process, where $d \simeq 0.1n$. The choice of the proxy vehicles depends on calculating the vehicles' additional computational resources. However, if no vehicles existed with this criterion, all the transmitted signatures must be verified by the RSUs. In [14], the computational Diffie-Hellman problem of the elliptic curve cryptosystem is conducted for singular verification to avoid the high computational overhead of bilinear pairing operations. Batch verification is another way of identifying a set of received signatures at once. Reference [15] presented a new and efficient RSU based authentication scheme that uses bilinear pairing to verify signatures in batches. However, such a scheme will fail once a single invalid signature exists, and all the received signatures will be singularly verified.

In their study, Chaum et al. presented a different solution by introducing the group signature-based scheme that allows every group member to sign messages on behalf of the rest of the group without exposing their real identity [16]. Nevertheless, the group key must be updated and distributed by the TA for each vehicle getting in/out from the group region which makes such a scheme hard to support forward and backward secrecy, especially in the case of high-speed group members. In [17], RSUs are assigned as group managers to improve the transmission and computation overheads. However, compromised RSU makes vehicles' private information vulnerable to exposure. In reference [18], regional trusted authorities are distributed and used to provide vehicles with authentication services. Unfortunately, the significant overhead of the bilinear pairing verification process limits the authentication rate, accordingly the number of terminals to be added to the network. Furthermore, the high computation overhead of signing and verifying crypto-based signatures limits communication availability, thereby decreasing the scheme's resistance to denial-of-service attacks [19]. The term "communication overhead" in the context refers to the bandwidth and storage capacity needed to transmit data between vehicles [10]. While the term "computation overhead" refers to the processing power and computations required to perform various tasks within the network [10]. Therefore, an efficient authentication scheme must maintain a balance between low computation and communication overheads to support network scalability [20]. Table II classifies the overheads required for transmitting and verifying a single authentication request in VANETs [20].

In this challenging scenario, PHY-layer authentication has emerged as a lightweight distinguishing technique to address the shortcomings of conventional cryptographic approaches. The discrimination process is performed based on the spatial decorrelation of the wireless channel responses between different terminals in different geographic locations [21], [22], [23], [24], [25]. The inherent idea is to determine whether or not features observed from the same source are highly correlated within the channel coherence time T_c, known as the "feature tracking" technique. However, this technique suffers from a low probability of detection at significant channel variations and small signal-to-noise ratios (SNRs), making it impractical in resource-constrained and long-range applications [26]. Furthermore, all the corresponding terminals must be extensively observed to capture their wireless channel attributes within T_c, which is not feasible for dynamic and high-density applications [26]. To improve the authentication performance and the security strength, Machine/Deep learning-based multiple channel-attributes authentication schemes have been presented in [27], [28] by extracting a unique radio frequency fingerprint for each network terminal. However, the high complexity of these schemes constitutes a significant performance limitation due to the need for large data sets for training kernels/neurons,

which is not applicable in VANETs. Furthermore, each terminal in the network must be pre-registered to extract its distinctive features for the supervised authentication approach.

Besides feature tracking techniques, hardware impairment attributes such as carrier frequency offset and analogue front-end imperfection are device-dependent distinguishing features between terminals [29], [30], [31]. This approach has a significant weakness in that features extracted from different devices vary slightly, leading to false decision-making. Additionally, these features are also characterised by their instabilities due to voltage supply, temperature variations, and electromagnetic interference. A tag-based authentication scheme is introduced as a signal watermarking technique to address these issues. In this technique, a pre-agreed secret modulated signal is superimposed on the transmitted signal [32], [33], [34]. However, the tradeoff between decoding performance and security is a non-negligible issue under different signal-to-tag power allocation ratios. In summary, PHY-layer-based schemes cannot provide a completely alternative solution since an initial identity verification of the corresponding terminal is still needed based on the existing cryptographic protocols to identify its legitimacy and extract its distinctive features. Nevertheless, it can be a promising complementary solution for the re-authentication problem in VANETs, introducing what is known as "cross-layer authentication [26]."

The existing cross-layer authentication schemes are developed by integrating the physical layer (non-cryptographic) with the upper layer (cryptographic) operations [35]. This integration should be rational and practical to support the application nature in terms of dynamicity, resources availability, and channel conditions. Consequently, selecting the appropriate technique for re-authentication is essential. Since VANETs are close in nature to mobile communications, the rest of our review focuses on the existing cross-layer authentication schemes of VANETs and mobile applications. In references [9], [36], [37], authors integrated a PKI-based algorithm for entity authentication with feature tracking for re-authentication. Unfortunately, an extensive observation is still needed for successful authentication, which is not feasible in high-density traffic scenarios, along with the high vulnerability to the impersonation attack if the attacker is close enough ($\leq$ half of the wavelength $\lambda/2$) to one of the communicating terminals and succeeded in obtaining partial information about the pre-extracted feature. Reference [38] introduced another cross-layer approach for mobile communications. In this work, the PHY response is not transmitted in the bit form but is masked by the channel frequency response between the user terminal and the base station using a fault-tolerant hashing technique. However, the time taken to generate the response signal is not evaluated and compared to the minimum coherence time to ensure the short-term channel reciprocity between the communicating terminals.

Even though the cross-layer methods described above can provide enhanced authentication, they cannot be applied to VANETs applications due to vehicular channels' high mobility and temporal variability, a matter that deserves further investigation. We developed a key-based PHY-layer challenge-response algorithm for re-authentication to fill this gap. In this algorithm, the preliminary key is mapped and masked by the channel-phase response to generate the response signal that can only be equalized at the side of the intended receiver, employing the short-term channel reciprocity and the same encapsulated key. To guarantee the channel reciprocity between high-speed terminals, we estimated the time required to generate the response signal and compared it to an indicative minimum coherence time of vehicle-to-vehicle (V2V) communication, as a worst-case scenario. Furthermore, our study examined the detection probability of re-authentication at small SNRs for an acceptable false alarm probability. In addition, we proved the scheme's security strength against typical adversarial attacks, including replaying, impersonation, and denial-of-services.

Besides authentication, the spatial and temporal variations of the wireless channel can also be exploited to extract a unique location-dependent shared key between the communicating terminals, supporting forward and backward secrecy in VANETs (an adversary cannot predict the previous or upcoming shared key based on the current one [39]). A dynamic message authentication scheme is presented in [40], in which the message authentication code related to the original frame symbol is computed based on an extracted shared key. However, the whole scheme's communication overhead is not evaluated, including the secret key extraction process and the session key obtained from the key distribution algorithm. In reference [41], a channel-based secret key is extracted and used for PHY-layer authentication, whereas in reference [42], the extracted key is used for upper layers' cryptographic operations. The keys extracted are usually not identical due to the channel being probed in the half-duplex mode [43]. Consequently, the significant communication overhead of reconciling the discrepancies in the extracted key constitutes a significant challenge for such algorithms. In existing reconciliation approaches, such as the Cascade algorithm, around 60% of the extracted bits are exposed for reconciling 10% of mismatched bits [44]. Therefore, this stage is excluded in this study since the decision rule of the re-authentication process depends on the circular variance of the equalized received response, which gives the proposed scheme an advantage of successfully re-authenticating the corresponding terminal with a sufficient key-mutuality percentage not less than 70%.

The contributions of this paper are summarised as follows:

1) We propose a low-complexity cross-layer authentication scheme for VANETs applications, employing the short-term channel reciprocity and randomness for re-authentication to address some of the performance limitation issues, particularly those related to the significant overheads of signatures generation and verification.
2) A lightweight pseudo-identity-based algorithm is proposed to initially verify the legitimacy of the corresponding terminals at the first time slot, which increases the scheme's availability and mitigates the effect of the flooding type of DoS attacks on the network. For re-authentication, a location-dependent-based PHY-layer re-authentication step is proposed for the identity re-verification process, which helps in detecting and preventing Sybil types of attacks.

TABLE III
NOTATIONS

Symbol	Definition
RID_{V_i}	Real identity of the vehicle V_i
TID_{V_i}	Temporary identity of V_i
PPs	Algorithm's public parameters
β	TA's master key
r_{V_i}	Private key of V_i
PK_{V_i}	Public key of V_i
$PK_{V_i,TA}$	Public key of V_i and TA
PK_{RV_i}	Public key of the revoked vehicle RV_i
PID_{V_i}	Pseudo-identity of V_i, $PID_{V_i} = \{PID_i^1, PID_i^2\}$
σ_{V_i}	Signature generated by V_i
$SK_{V_{i-j}}$	Session key between two communicating vehicles V_i and V_j
GRL	General revocation list generated by TA
TID_{GRL}	List of revoked vehicles' TIDs generated by V_i
T_i	Signature's timestamp generated by V_i
T_r	Signature's receiving time at the intended receiver
T_Δ	Freshness expiry time [0:00:59]
$\perp$	Empty string

3) Furthermore, we present how the proposed scheme can fulfil the security and privacy requirements of VANETs. In this way, the unforgeability of signatures is proven against adaptive chosen message attacks in the random oracle model (for background, see [45]), ensuring the resistance of the proposed scheme to impersonation and modification attacks.
4) Besides theoretical analysis, we conducted an extensive simulation to examine the detection probability of the PHY-layer re-authentication process at small SNRs $\geq$ 5 dB. In addition, we investigated the timing analysis of the challenge-response process to ensure that the wireless channel exhibits short-term reciprocity under conditions of high-speed terminals of up to $\approx 30\ m/s$. Finally, the computation and communication comparison and security analysis show that the proposed scheme offers security and cost-saving advantages over crypto-based signatures.

The rest of this paper is organised as follows. The structure of the proposed cross-layer authentication scheme is presented in Section II, while Section III discusses the adopted threat model. Section IV presents extensive performance analysis and comparisons regarding computation and communication overheads. Finally, Section V concludes this paper.

II. Cross-Layer Authentication Scheme

In this section, the system model for the proposed cross-layer scheme is presented first. Next, we describe in detail each step in the following subsections.

A. System Model for the Proposed Cross-Layer Scheme

The novelty of the proposed scheme relies on exploiting the short-term channel reciprocity between two communicating terminals for re-authentication. The corresponding terminal is re-authenticated at the PHY-layer in a challenge-response process, providing an efficient and secure verification in a low processing time. Fig. 1 presents the flowchart of the proposed approach, which can be described through the following steps.

- *S1. Initial Authentication:* A conditional privacy preservation authentication algorithm (ACPPA) is proposed for mutual identity verification using the upper layer's authentication by exchanging pseudo-identities between both terminals.
- *S2. Secret Key Extraction:* If the initial verification holds, the key extraction algorithm in [43] is employed to extract a location-dependent shared key between both terminals. Otherwise, the authentication process is ended.
- *S3. PHY-Layer Re-authentication:* Under binary hypothesis testing [46], the re-authentication step is performed at the physical layer using a PHY challenge-response algorithm based on the extracted key with a sufficient number of matched bits.
- *S4. Thresholding Optimisation Feedback:* In the case of failure, the key extraction step (S2) is re-executed after adapting the thresholding values based on the feedback from the re-authentication step (S3).

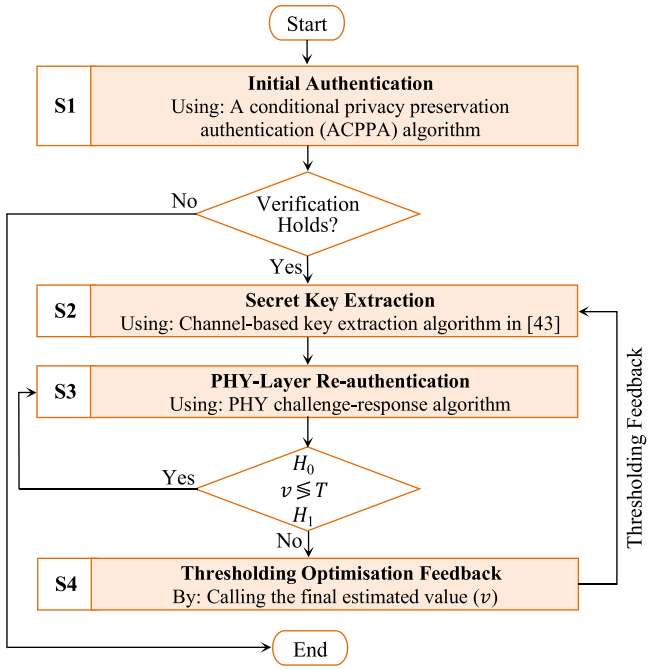

Fig. 1. Flowchart of the proposed authentication scheme.

The low complexity of the proposed scheme, i.e., our 1^{st} contribution, stems from the integration of the re-authentication step S3 into S1. In doing so, the computation and communication overheads associated with signing and distributing signatures are drastically reduced for each transmission. For the 2^{nd} contribution, we ensure scheme availability by designing a lightweight initial identity verification step represented in S1, mitigating the effect of DoS attacks. As for Sybil attacks detection, we integrated S2 into S3 to provide location-dependent-based re-authentication at the PHY layer. At last, the thresholding optimisation feedback step S4 is used to adjust the key extraction parameters of S2 based on the re-authentication feedback from S3. All network terminals are assumed to be working in the time-division duplex mode with a single antenna and separated by more than $\lambda/2$ distance. The channel responses between legitimate and wiretap channels are uncorrelated. RSUs and vehicles' OBUs are supposed to be synchronised with the TA.

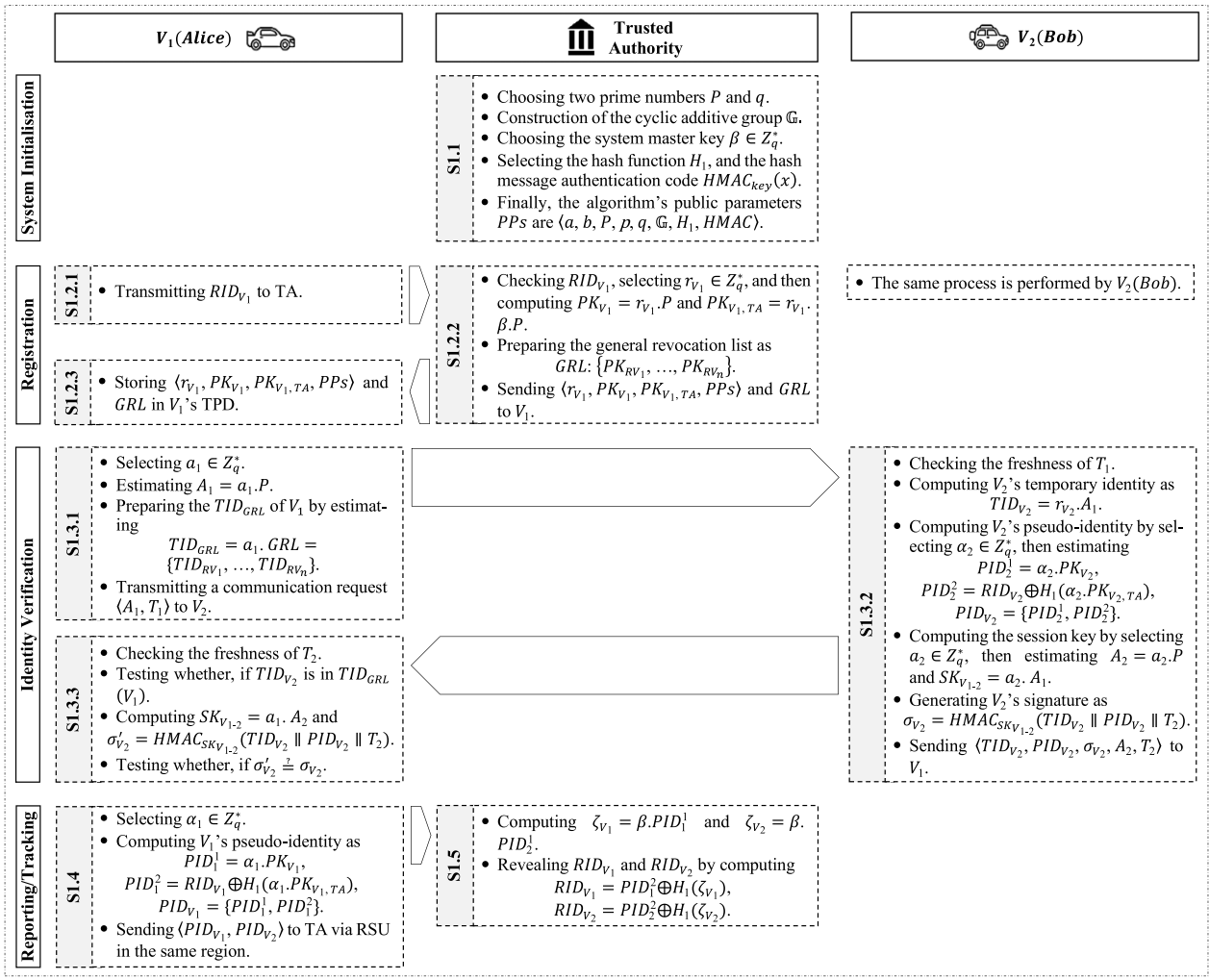

Fig. 2. The top-level description of the proposed ACPPA algorithm.

B. Overview of the Initial Authentication Step (S1)

The proposed ACPPA algorithm is presented in this subsection for V2V as a case study for vehicular communication in VANETs. This process aims to identify the legitimacy of the corresponding terminal initially. A location-dependent shared key will be extracted according to the signature verification result. A pseudo-identity-based algorithm is proposed to identify the corresponding terminal's legitimacy based on ECC scalar multiplications, avoiding using map-to-point hash functions and bilinear pairing time-consumed operations. The proposed algorithm consists of five phases - i.e., system initialisation, registration, identity authentication, reporting, and real identity tracking. The notations used in this subsection are listed in Table III. Fig. 2 presents the top-level description of the S1 algorithm's sub-steps detailed below.

S1.1: System initialisation phase: TA generates the system's public parameters via the following processes.

- Choosing two large prime numbers p andp q, and 160-bits elliptic curve E for 80-bits security defined by $y^2 = x^3 + ax + b \ mod \ p$ over a prime field F_p for $a, b \in F_p$, where $\Delta = 4a^3 + 27b^2 \neq 0$
- Construction of the cyclic additive group $\mathbb{G}$ of order q based on the generator P, so that $\mathbb{G}$ consists of all the points on E and the infinity point $\mathcal{O}$.
- Randomly choosing the system master key $\beta \in Z_q^*$.
- Selecting the hash function $H_1 : \mathbb{G} \rightarrow \{0,1\}^{N_1}$ and the hash message authentication code $HMAC_{key}(x) : (key : \mathbb{G}, x : \{0,1\}^*) \rightarrow \{0,1\}^{N_2}$.
- Finally, the algorithm's public parameters are $PPs : \langle a, b, P, p, q, \mathbb{G}, H_1, HMAC \rangle$.

S1.2: Registration phase: Before joining the network, each vehicle V_i must register with the TA to obtain the algorithm's public parameters according to the following sub-steps.

- *S1.2.1:* V_i transmits its unique RID_{V_i} (e.g., license number) to TA to check the validation status of the RID_{V_i}.
- *S1.2.2:* Ta prepares V_i's secret parameters as follows.
  – TA checks the RID_{V_i}, selects a random private number $r_{V_i} \in Z_q^*$ of V_i, and calculates its relevant public keys as $PK_{V_i} = r_{V_i}.P$, and $PK_{V_i,TA} = r_{V_i}.\beta.P$.

– TA prepares the general revocation list GRL, which is a list of public keys of revoked vehicles is distributed between vehicles and RSUs and equals GRL: $\{PK_{RV_1}, PK_{RV_2}, \ldots, PK_{RV_n}\}$

S1.2.3: During V_i's registration, TA stores the tuple $\langle r_{V_i}, PK_{V_i}, PK_{V_i,TA}, PPs\rangle$ and GRL in V_i's TPD.

S1.3: Identity authentication phase: Mutual identity authentication between $V_1(Alice)$ and $V_2(Bob)$ is conducted when V_2 is in the transmission range of V_1. Without loss of generality, the one-way authentication process consists of three main stages.

- *S1.3.1: Communication request stage:* In this stage, a vehicle V_1 randomly selects $a_1 \in Z_q^*$, computes its corresponding public parameter $A_1 = a_1 \cdot P$, then prepares its revocation list by estimating the list of temporary identities TIDs of revoked vehicles based on the general revocation list GRL as $TID_{GRL}(V_1) = a_1 \cdot GRL = \{TID_{RV_1}, \ldots, TID_{RV_n}\}$, and sends a communication request $\langle A_1, T_1\rangle$ to V_2 at timestamp T_1.
- *S1.3.2: Signature generation stage:* In this stage, a vehicle V_2 checks the freshness of the received timestamp T_1 by testing whether $T_r - T_1 \leq T_\Delta$ holds or not, hides its real identity by computing its temporary identity $TID_{V_2} = r_{V_2} \cdot A_1$ and pseudo-identity PID_{V_2}. To generate a valid PID_{V_2}, V_2 chooses at random $\alpha_2 \in Z_q^*$, computes $PID_2^1 = \alpha_2 \cdot PK_{V_2}$ and $PID_2^2 = RID_{V_2} \oplus H_1(\alpha_2 \cdot PK_{V_2,TA})$ to attain its pseudo-identity $PID_{V_2} = \{PID_2^1, PID_2^2\}$. Then, V_2 calculates its signature σ_{V_2} by selecting at random $a_2 \in Z_q^*$, calculating its relevant public parameter $A_2 = a_2.P$ and the key $SK_{V_{1-2}} = a_2.A_1$ to obtain the signature $\sigma_{V_2} = HMAC_{SK_{V_{1-2}}}(TID_{V_2} \| PID_{V_2} \| T_2)$ created at the T_2 timestamp. Finally, V_2 replies to V_1's request by sending the tuple $\langle TID_{V_2}, PID_{V_2}, A_2, T_2, \sigma_{V_2}\rangle$ to V_1.
- *S1.3.3: Signature verification stage:* In this stage, V_1 checks the freshness of the timestamp T_2, verifies the legitimacy of V_2 by finding out if $TID_{V_2} \in TID_{GRL}(V_1)$, then checks the integrity of the received message by computing $SK_{V_{1-2}} = a_1 \cdot A_2$ and $\sigma'_{V_2} = HMAC_{SK_{V_{1-2}}}(TID_{V_2} \| PID_{V_2} \| T_2)$ and testing whether $\sigma'_{V_2} \stackrel{?}{=} \sigma_{V_2}$ holds or not. The same process is reversed between the communicating terminals for mutual authentication.

S1.4: Reporting phase: Misbehaving vehicles can be reported, let us consider V_1 wants to report V_2. In that case, V_1 randomly selects $\alpha_1 \in Z_q^*$, generates vehicle's pseudo-identity by computing $PID_1^1 = \alpha_1 \cdot PK_{V_1}$ and $PID_1^2 = RID_{V_1} \oplus H_1(\alpha_1 \cdot PK_{V_1,TA})$ to obtain $PID_{V_1} = \{PID_1^1, PID_1^2\}$. Finally, V_1 reports V_2 by sending the tuple $\langle PID_{V_1}, PID_{V_2}\rangle$ to TA through the RSU in the same region, in which PID_{V_1} and PID_{V_2} are the pseudo-identities of the reporter and misbehaving vehicles, respectively.

S1.5: Real identity tracking phase: The RIDs of the reporter and misbehaving vehicles can be revealed by the TA based on the received tuple $\langle PID_{V_1}, PID_{V_2}\rangle$ and TA's master key β by computing $\zeta_{V_i} = \beta.PID_i^1$ and $RID_{V_i} = PID_i^2 \oplus H_1(\zeta_{V_i})$.

The proof of correction is verified as follows:

$$\begin{aligned} RID_{V_i} &= PID_i^2 \oplus H_1(\zeta_{V_i}) \\ &= RID_{V_i} \oplus H_1(\alpha_i \cdot PK_{V_i,TA}) \oplus H_1\left(\beta \cdot PID_i^1\right) \\ &= RID_{V_i} \oplus H_1(\alpha_i \cdot PK_{V_i,TA}) \oplus H_1(\alpha_i \cdot \beta \cdot PK_{V_i}) \\ &= RID_{V_i} \oplus H_1(\alpha_i \cdot PK_{V_i,TA}) \oplus H_1(\alpha_i.PK_{V_i,TA}) = RID_{V_i} \end{aligned}$$

C. Review of the Secret Key Extraction Algorithm in [43] (S2)

Channel randomness is a natural-correlated resource for extracting a high entropy shared key between terminals. Generally, the key generation process consists of four stages - i.e., channel probing, quantisation/thresholding, information reconciliation, and privacy amplification. In our proposed scheme, we evoked the key extraction algorithm in [43] to obtain a symmetric shared key with equiprobabilities of 0 s and 1 s and a sufficient rate of secret bit generation, defined by the ratio of the number of matching bits to the total number of channel samples. In order to avoid the high communication overhead of reconciling the discrepancies in the extracted key, we excluded the information reconciliation and privacy amplification stages from the secret key generation process.

In high-density V2V channel conditions with many fixed and moving scatterers (e.g., other vehicles), the received signal is the superposition of L multipath components of different paths with different phase delays ϕ_l and fading coefficients $|a_l|$ [43]. The channel estimations at each side $Ch_{A\leftarrow B}(t)|_A$ for Alice and $Ch_{A\rightarrow B}(t)|_B$ for Bob can be formulated at instance time t as

$$Ch_{A\leftarrow B}(t)|_A \approx Ch_{A\rightarrow B}(t)|_B = \sum_{l=1}^{L} |a_l| \, e^{(j\phi_l)} e^{2\pi v_l t} \quad (1)$$

where v_l is the Doppler shift of each multipath component l which is the sum of that of Alice $v_{A,l}$, Bob $v_{B,l}$, and scatterers $v_{S,l}$ [48] as

$$v_l = v_{A,l} + v_{B,l} + v_{S,l} \quad (2)$$

Note that, the scatterers' speed can follow the Weibull distribution (with shape and scale parameters a and ω, respectively) [49].

Since the channel probing stage is performed in the half-duplex mode, channel gain complement method is utilized to compensate the channel non-reciprocity. However, zero-mean complex Gaussian noise $\mathcal{C}N(0, 2\sigma_C^2)$ still exists and is considered to be the difference between the uplink $Ch_{A\rightarrow B}(t)|_B$ and the downlink $Ch_{A\leftarrow B}(t + \Delta t)|_A$ channel responses at each side of the communicating terminals [43] as

$$Ch_{A\rightarrow B}(t)|_B = Ch_{A\leftarrow B}(t + \Delta t)|_A + \mathcal{C}N\left(0, 2\sigma_C^2\right) \quad (3)$$

where $\Delta t \leq T_c$. In [43], the perturb-observe algorithm is used to optimize the quantisation levels at different estimated non-reciprocity values σ_c based on the feedback from the information reconciliation stage, as shown in Fig. 3(a). In this paper, we excluded the information reconciliation stage. As a result, the PHY-layer re-authentication is used as alternative feedback for the thresholds optimisation engine, as illustrated in Fig. 3(b). This feedback indicates the level of mismatching resulting from different non-reciprocity values between the communicating terminals.

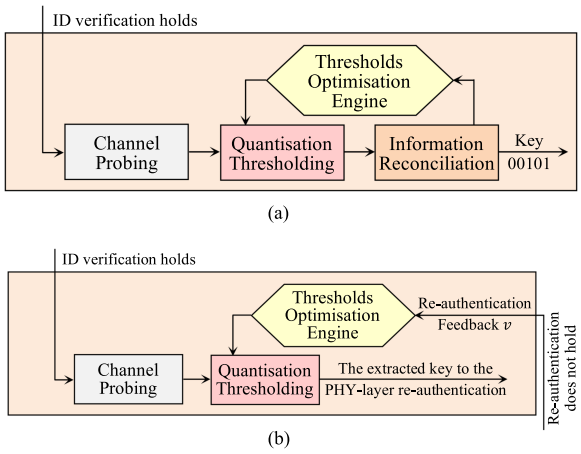

Fig. 3. PHY-layer secret key extraction algorithm. (a) Quantisation thresholds optimisation technique in [43]. (b) The developed thresholds optimisation technique.

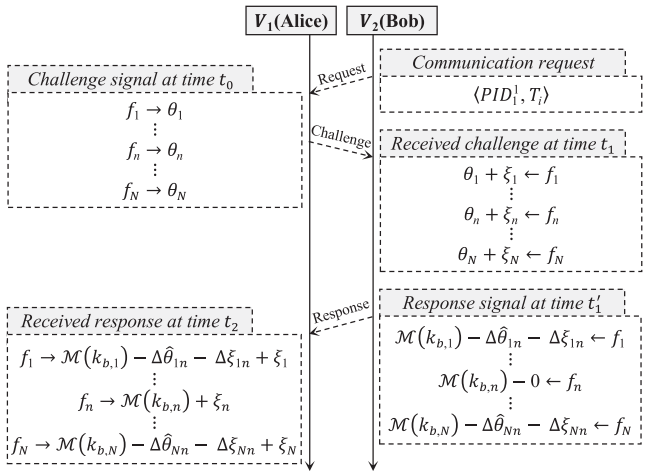

Fig. 4. One-way PHY challenge-response re-authentication algorithm for OFDM system in the frequency domain.

Step (S2) comprises three sub-steps as follows.

- *S2.1: Channel Probing:* Probing signals are exchanged between the communicating terminals to obtain highly correlated estimates within the coherence interval T_c.
- *S2.2: Quantisation thresholding:* Two thresholds quantisers (q_+, q_-) are used to convert the estimated channel observations into bits.
- *S2.3: Thresholds optimisation engine:* Applying a perturb-observe algorithm [43] to adapt the quantization levels in response to the feedback from the re-authentication step (S3).

Eventually, the extracted key $k_{\{a,b\}}$ is used for the mutual re-authentication process that is discussed in the following subsection (for more information about the secret key extraction algorithm, see reference [43]).

D. Overview of the PHY-Layer Re-Authentication Step (S3)

After identity verification and the extraction of the shared key $k_{\{a,b\}}$ between legitimate parties, Alice and Bob, the generated key is partitioned into two equal-length preliminary keys $k_{\{a,b\}} = (k_a \| k_b)$ used for the two-way re-authentication process. Alice transmits a challenge signal to Bob. The latter responds by encapsulating the mapped key k_b into the response signal that can be equalized at the side of Alice by exploiting the short-term channel reciprocity and the same encapsulated key. We considered a one-way re-authentication process for N subcarriers OFDM system as illustrated in Fig. 4. For mutual re-authentication, the process is reversed and repeated between terminals based on the second part of the extracted key k_a.

The detailed sub-steps are as follows:

S3.1: PHY communication request: Bob transmits a communication request to Alice. This request contains the pseudo-identity PID_1^1 of Alice and T_i timestamp.

S3.2: PHY challenge: Alice infers from the communication request that a pre-authenticated vehicle is trying to communicate with him. Then Alice initiates a PHY challenge frame for N subcarriers OFDM communication system and sends an initial challenge modulated sinusoidal signal to Bob with random phases θ_i uniformly distributed over $[0, 2\pi)$ with frequencies $f_1, \ldots, f_N$ so that the transmitted signal at instance time t_0 can be expressed as

$$s_a(t_0) = \sum_{i=1}^{N} \sqrt{\frac{2E_s}{T}} \cos(2\pi f_i t_0 + \theta_i), \theta_i \sim U[0, 2\pi) \quad (4)$$

At the receiver's terminal, the received signal by Bob at time t_1 is formulated in a noiseless channel as

$$r_b(t_1) = \sum_{i=1}^{N} \sqrt{\frac{2|h_i|^2 E_s}{T}} \cos(2\pi f_i t_1 + \psi_i) \quad (5)$$

where $\psi_i = \theta_i + \xi_i, h_i$ for $i = 1, 2, \ldots, N$ are independent and identically distributed $(i.i.d.)$ random variables with zero mean and variance $Var(h_i) = 2\sigma^2$, and $\angle(h_i) = \xi_i \sim U[0, 2\pi)$ which is the i^{th} subchannel-phase response of parallel Rayleigh fading channel of N subcarriers with probability density function $p(\xi_i) = 1/2\pi$. After that, Bob estimates the phase difference of the received signal $\Delta\hat{\psi}_{in} = \psi_i - \psi_n = \Delta\hat{\theta}_{in} + \Delta\xi_{in}$, in which n is a randomly selected subcarrier index that ranges from 1 to N and can be altered by Bob at each iteration. The phase difference estimation can be expressed as

$$u_i = r_{b,i} r_{b,n}^*, \Delta\widehat{\psi}_{in} = \tan^{-1}\left(\frac{imag(u_i)}{real(u_i)}\right) \quad (6)$$

S3.3: PHY response: A gray code mapping operation $\mathcal{M}(.)$ of order 2 bits is used to map the preliminary key $k_b = \{\varkappa_1\varkappa_2, \varkappa_3\varkappa_4, \ldots, \varkappa_{2N-1}\varkappa_{2N}\}$ of length $2N$-bits at the side of Bob as below:

$$\phi_i = \mathcal{M}(k_{b,i}) = \begin{cases} 0 & k_{b,i} = [\,0 \quad 0\,] \\ \frac{\pi}{2} & k_{b,i} = [\,0 \quad 1\,] \\ \pi & k_{b,i} = [\,1 \quad 1\,] \\ \frac{3\pi}{2} & k_{b,i} = [\,1 \quad 0\,] \end{cases} \quad (7)$$

for $i = 1, 2, \ldots, N$. After that, Bob responds to Alice's challenge by encapsulating the mapped key ϕ_i and the estimated

phase difference $\Delta\widehat{\psi}_{\text{in}}$ into the response signal and transmitting it to Alice at time t_1' as

$$s_b(t_1') = \sum_{i=1}^{N} \sqrt{\frac{2E_s}{T}} \cos(2\pi f_i t_1' + \phi_i - \Delta\widehat{\psi}_{in}) = \sum_{i=1}^{N} \sqrt{\frac{2E_s}{T}} \cos(2\pi f_i t_1' + \phi_i - \Delta\hat{\theta}_{in} - \Delta\xi_{in}) \quad (8)$$

The received signal by Alice at time t_2 is formulated in a noiseless channel as

$$r_a(t_2) = \sum_{i=1}^{N} \sqrt{\frac{2|h_i|^2 E_s}{T}} \cos(2\pi f_i t_2 + \phi_i - \Delta\hat{\theta}_{in} - \Delta\xi_{in} + \xi_i) = \sum_{i=1}^{N} \sqrt{\frac{2|h_i|^2 E_s}{T}} \cos(2\pi f_i t_2 + \phi_i - \Delta\hat{\theta}_{in} + \xi_n) \quad (9)$$

Equalizing $r_a(t_2)$ by estimating the phase θ_i of the initial signal $s_a(t_0)$, mapping the preliminary key k_b at the side of Alice $\hat{\phi}_i = \mathcal{M}(k_{b,i})$, and computing $r_a(t_2)e^{j(-\phi_i+\theta_i)}$ so that the estimated signal by Alice at time t_2' can be simplified as

$$\begin{aligned} c(t_2') &= r_a(t_2)\, e^{j\left(-\widehat{\phi}_i+\theta_i\right)} \\ &= \sum_{i=1}^{N} \sqrt{\frac{2|h_i|^2 E_s}{T}} \cos(2\pi f_i t_2' + \phi_i - \Delta\hat{\theta}_{in} \\ &\quad + \xi_n - \hat{\phi}_i + \theta_i) \\ &= \sum_{i=1}^{N} \sqrt{\frac{2|h_i|^2 E_s}{T}} \cos\left(2\pi f_i t_2' + \theta_n + \xi_n + \phi_{e,i}\right) \end{aligned} \quad (10)$$

where $\phi_{e,i}$ is an estimated phase difference error resulting from the i^{th} subcarrier that holds mismatched bits and can be expressed as

$$\phi_{e,i} = \phi_i - \hat{\phi}_i \begin{cases} value & \phi_i \neq \hat{\phi}_i \\ 0 & \phi_i = \hat{\phi}_i \end{cases} \quad (11)$$

S3.4: Verification process: Alice checks the legitimacy of Bob by verifying the encapsulated key. Suppose the PHY response is sent from a third party (Eve impersonates the legitimate party, Bob). In that case, it is assumed that Eve generated a random binary key vector k_e for authentication, which can be represented as a hypothesis testing problem as indicated:

$$v(t_2') = Var\left(\sum_{i=1}^{N} \angle c_i(t_2')\right) \underset{H_1}{\overset{H_0}{\lessgtr}} T, \quad \text{for} \quad \begin{cases} H_0: & \phi_i = \mathcal{M}(k_{b,i}) \\ H_1: & \phi_i = \mathcal{M}(k_{e,i}) \end{cases} \quad (12)$$

where T is the threshold value, and $Var(\sum_{i=1}^{N} \angle(c_i))$ is the circular variance of $\angle(c_i)$ which calculated as in [50] as

$$r_i = \begin{pmatrix} \cos(\angle(c_i)) \\ \sin(\angle(c_i)) \end{pmatrix}, \bar{r} = \frac{1}{N}\sum_i r_i \quad v = 1 - \|\bar{r}\| \quad (13)$$

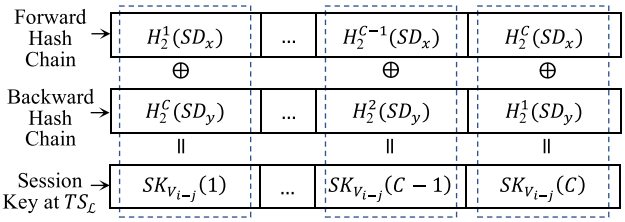

Fig. 5. Hash chains used to generate $SK_{V_{i-j}}(TS_{\mathcal{L}})$.

In binary hypothesis testing, the authentication judgment of the received signal r_a from the corresponding terminal is performed based on $v = (r_a, \phi_i)$. The decision rule is taken according to the estimated measurement v, if the received response is sent from Bob $r_{a\leftarrow b}$, then v is estimated according to the joint distribution of $p(r_{a\leftarrow b}, \phi_i = \mathcal{M}(k_{b,i}))$, while, the received response from Eve $r_{a\leftarrow e}$ obeys the distribution $p(r_{a\leftarrow e} \mid \phi_i = \mathcal{M}(k_{e,i})) \cdot \Pr(\widehat{\phi}_i = \mathcal{M}(k_{e,i}))$. As long as Eve possesses zero information about k_b, the hypothesis testing can be formulated a

$$T = \log \frac{p\left(r_{a\leftarrow b} \mid \phi_i = \mathcal{M}\left(k_{b,i}\right)\right)}{p\left(r_{a\leftarrow e} \mid \phi_i = \mathcal{M}\left(k_{e,i}\right)\right) \Pr(\widehat{\phi}_i = \mathcal{M}\left(k_{e,i}\right))} \quad (14)$$

The authentication judgment is further made by comparing v to the threshold value T. The proposed algorithm is an extension of the work introduced in [51]. Since the decision rule depends on the circular variance $v = Var(\sum_{i=1}^{N} \angle(c_i))$, the remaining phase constant $(\theta_n + \xi_n)$ in (10) will not affect the final estimation result of v, giving the privilege of randomly selecting the subcarrier index n of the phase difference operation in (6).

S3.5: Multi-vehicle communications: For each vehicle V_j communicates with a number of n vehicles in the network, V_j stores a $List$ of n tuples of vehicle's identities and their corresponding extracted shared keys as $List = \{Tuple_{V_1}, \ldots, Tuple_{V_n}\}$ in which $Tuple_{V_i} = \langle TID_{V_i}, PID_{V_i}, SK_{V_{i-j}} : k_{\{a,b\}} \rangle$. Considering vehicle V_i remains in the communication range of vehicle V_j for $\mathcal{T}$ seconds, then the duration $\mathcal{T}$ is divided into C time slots $TS_{\mathcal{L}}$ of length $\Delta\mathcal{T}$ for $TS_{\mathcal{L}} \in [(\mathcal{L}-1).\Delta\mathcal{T}, \mathcal{L}.\Delta\mathcal{T}]$ and $\mathcal{L} \in [1, C]$.

For successful PHY-layer re-authentication process of n vehicles, the session key at time slot $TS_{\mathcal{L}}$ is periodically updated C times for all the corresponding vehicles in the $List$ as shown in Fig. 5 and can be formulated as

$$\begin{aligned} SK_{V_{i-j}}(TS_L) &= (S_{L,x} \oplus S_{L,y}) \\ S_{L,x} &= H_2^L(SD_x), \quad S_{\mathcal{L},y} = H_2^{C-L+1}(SD_y) \end{aligned} \quad (15)$$

where SD_x and SD_y are the seed numbers and the x and y coordinates of the point $SK_{V_{i-j}} = \{SD_x, SD_y\} \in \mathbb{G}$, and $H_2^x(y)$ is the hash function $\{0,1\}^* \rightarrow \{0,1\}^{N_1}$ of the input variable y for x iterations. The computed $SK_{V_{i-j}}(TS_{\mathcal{L}})$ of length $N_1 = 160$ bits for SHA-1 hash function and the safety-related message m are concatenated with the transmitted PHY response for OFDM system of N subcarriers. The corresponding vehicle V_i verifies the received frame by searching in the $List$ for $k_{\{a,b\}}$ related to the received session key $SK_{V_{i-j}}(TS_{\mathcal{L}})$ from vehicle V_j. In other

words, the received $SK_{V_{i-j}}(TS_{\mathcal{L}})$ can be treated as an address to $k_{\{a,b\}}$ related to vehicle V_j. After that, V_i verifies the response signal by executing the verification process.

E. The Thresholding Optimisation Feedback Step (S4)

In this step, the feedback value v denotes the level of mismatching between the mapped keys $\phi_{e,i} = \phi_i - \widehat{\phi}_i$, indicating the degree of channel non-reciprocity between both terminals. This feedback is an input to the thresholds optimisation engine S2.3. In the case of false decision-making due to a high mismatching percentage, the key extraction step (S2) is re-executed after adjusting the quantisation region $(q_+ - q_-)$. Increasing the quantization region reduces the mismatching percentage, improving the detection probability of the re-authentication step at subsequent time slots.

III. Threat Model of the Proposed Scheme

In this section, design goals in terms of security and privacy objectives are introduced, and then, we discuss in detail how the proposed scheme satisfies these goals.

A. Design Goals for the Proposed Scheme

To achieve the 3^{rd} contribution, the proposed scheme must satisfy the following security and privacy objectives [10], [47].

1) *Privacy preservation:* Semi-trusted terminals (RSUs) or distrusted terminals (surrounding vehicles) cannot extract identifiable data about the sender from message contents.
2) *Non-Repudiation:* The transmitter cannot deny the authorship of the transmitted signatures.
3) *Traceability:* In the proposed scheme, vehicles communicate with each other using their temporary identities to preserve users' real identities, providing conditional privacy. Only TA has the privilege to trace the real identities of vehicles and prevent malicious vehicles from participating in the network.
4) *Unlinkability:* Distrusted terminals cannot track the transmitter behaviors by determining the origins of two different signatures.
5) *Resistance to attacks:* The attacker's priority is to disrupt the network by applying the following common attacks:

- *Replay attack:* The attacker retransmits previously captured data from the network after a period, which confuses the targeted terminal.
- *Impersonation attack:* The attacker is trying to frame as a legitimate terminal and making the transmitted data appears as a normal flow of data.
- *Modification attack:* The transmitted messages are modified or altered by the attacker.
- *Man-in-the-Middle (MITM) attack:* The attacker may alter and relay broadcasted messages between communicating terminals that believe they are standing in direct communication with each other.
- *Sybil attack:* The attacker generates multiple fabricated identities and tries to masquerade multiple legitimate users to affect the functionality of the network.
- *Denial-of-service (DoS) attack:* This paper considers the flooding type of DoS attack [52] in which the attacker tries to deteriorate the network's performance by overwhelming the targeted terminal with fake requests.

B. Security and Privacy Evaluation of the ACPPA Algorithm

In this part, we prove the security strength of the ACPPA algorithm in the Random Oracle Model, in which the unforgeability of the signature generation stage is discussed against adversary $\mathcal{A}$ who is trying to impersonate V_2 by estimating $\langle TID_{V_2}, PID_{V_2}, A_2, T_2, \sigma_{V_2}\rangle$ under RID_{V_2} : $\langle r_{V_2}, PK_{V_2}, PK_{V_2,TA}\rangle$. The hardness of the signature generation stage depends on three cryptographic mathematical problems represented in the following definitions.

1) *Definition 1:* ECDLP. Given $\langle a, b, P, p, q, \mathbb{G}\rangle$ and $Q = \gamma.P$, output $\gamma \in Z_q^*$.
2) *Definition 2:* Hashing problem. Given s', in which $s' = H_1(x)$, output $x \in \mathbb{G}$.
3) *Definition 3:* HMAC problem. Given h', in which $h' = HMAC_{key}(x)$, output $x \in \{0,1\}^*$ under key $\in \mathbb{G}$.

Signature generation stage is $(\tau_{\text{Sig.Gen}}, q_{ID}, q_s, \epsilon_{\text{Sig.Gen}})$ existentially unforgeable against identity and adaptive chosen message attacks in the ROM as

$$\epsilon_{\text{Sig.Gen}} \geq \epsilon\left(1 - \frac{q_{ID}^2 q_s^2}{|N_1|\,|N_2|}\right), \tau_{\text{Sig.Gen}} = (6.q_{ID} + q_S)\,T_m \tag{16}$$

where T_m is the run time of scalar multiplication, q_{ID} and q_s are the number of queries to oracles $H_1(.)$ and $HMAC_{key}(.)$, respectively, and $\epsilon_{\text{Sig.Gen}}$ and $\tau_{\text{Sig.Gen}}$ are the probability and time for adversary $\mathcal{A}$ to generate a non-trivial forgery (the proof of (16) is derived in the Appendix). The following proves that the ACPPA algorithm meets the mentioned design goals.

1) *Privacy preservation and identity anonymity:* The real identities RID_{V_i} of the communicating terminals are preserved from adversary $\mathcal{A}$ as the authentication process depends on exchanging the pseudo-identities $PID_{V_i} = \{PID_i^1, PID_i^2\}$ for $PID_i^1 = \alpha_i.PK_{V_i}$ and $PID_i^2 = RID_{V_i} \oplus H_1(\alpha_i \cdot PK_{V_i,TA})$, which means that the attacker needs to compute $\alpha_i.PK_{V_{i,TA}} = \alpha_i.r_{V_i}.\beta.P$ from $PID_i^1 = \alpha_i.PK_{V_i} = \alpha_i.r_{V_i}.P$. Since the tracking phase depends on the knowledge of TA's master key β, $\mathcal{A}$ has no chance to track or identify vehicles' real identities, providing conditional privacy preservation.
2) *Non-Repudiation:* Each side of the communicating terminals cannot deny its authorship of the generated signatures because the TID_{V_i} and PID_{V_i} can only be computed based on the RID_{V_i}, PK_{V_i}, and $PK_{V_i,TA}$ which are stored in V_i's TPD and only accessible by the vehicle itself.
3) *Traceability and revocation:* Only TA can check the validity of PID_{V_i}, estimate the RID_{V_i} of the misbehaving vehicle, and revoke it based on TA's master key β as clarified in the real identity tracking phase.
4) *Unlinkability:* For each vehicle V_j communicates with V_i, V_i's signatures are generated with different TID_{V_i} and PID_{V_i} whose values are evaluated based on randomly selected parameters a_j and $\alpha_i \in Z_q^*$ that are dynamically

updated. Accordingly, it is hard for $\mathcal{A}$ to determine the origins of two randomly captured signatures from the same vehicle.

5) *Attacks resistance:* The proposed algorithm is shown to be resilient to common types of attacks, e.g., replay, impersonation, modification, MITM, Sybil, and DoS attacks as follows:

- *Resistance to replay attack:* ACPPA algorithm resists replay attack as each terminal checks the freshness of each generated signature σ_{V_i} based on the attached timestamp T_i by testing whether $T_r - T_i \leq T_\Delta$ holds or not. In addition, the randomly generated variables a_j, a_i, and $\alpha_i \in Z_q^*$ are frequently updated to avoid such attacks as the signature generation process depends on the current parameters. These reasons make the ACPPA algorithm immune to replay attacks.
- *Resistance to impersonation attack:* In this attack, an adversary $\mathcal{A}$ tries to masquerade as a legitimate vehicle V_i by creating a valid signature $\langle TID_{V_i}, PID_{V_i}, A_i, T_i, \sigma_{V_i}\rangle$. To succeed, $\mathcal{A}$ must forge the signature σ_{V_i}, which is existentially unforgeable against identity and adaptive chosen message attacks proved in the ROM. Thus, ACPPA is resilient to such attacks.
- *Resistance to modification attack:* The integrity of the received signature can be easily detected by estimating $\sigma'_{V_i} = HMAC_{SV_{V_{i-j}}}(TID_{V_i} \| PID_{V_i} \| T_i)$, in which, the session key SK_{i-j} is computed using Diffie-Hellman key exchanging protocol under the difficulty of solving the ECDLP. After that, the verifier checks whether $\sigma'_{V_i} \stackrel{?}{=} \sigma_{V_i}$ holds. If not, such an attack is detected, and the received signature is rejected.
- *Resistance to MITM attack:* To avoid this attack, the recipient ensures that the message sender is a legitimate party. The proposed ACPPA algorithm uses the temporary identity TID_{V_j} to identify the sender's legitimacy, computed based on the session parameter $a_i \in Z_q^*$. To execute this attack, an adversary $\mathcal{A}$ must forge a valid signature, which is existentially unforgeable against identity and adaptive chosen message attacks proved in the ROM. Thus, this attack is prevented.
- *Resistance to Sybil attack:* An internal attacker (an authenticated user from inside the network who is aware of the network configuration) has multiple-fabricated PIDs that can be used singularly or simultaneously to masquerade multiple vehicles. This type of attack is common in many contributed VANETs' signatures-based techniques. In our scheme, a unique shared key is obtained using a location-dependent channel-based secret key extraction algorithm (S2). This means that there is no opportunity for a single vehicle in the network to extract more than a shared key within T_c. In other words, whatever the number of the generated PIDs, there is no chance of generating more than one shared key between two terminals within T_c that varies at different terminal speeds, mitigating the effect of such an attack on the network.
- *Resistance to DoS attack:* Considering communication availability and since this study aims to reduce the computation and communication overheads, this paper examines the common flooding type of DoS attack [53] on S1. In the latter (S1), the recipient verifies the sender's legitimacy and eventually discards fake requests (Fig. 1), preventing $\mathcal{A}$ from proceeding to S2. In this attack, an adversary $\mathcal{A}$ attempts to flood V_j with several requests in the form of $\langle A_i, T_i\rangle$ or flood V_i with signatures in the form of $\langle TID_{V_j}, PID_{V_j}, A_j, T_j, \sigma_{V_j}\rangle$. In both cases, the targeted terminal replies by signing or verifying $HMAC$-based signatures in which the computation overhead of the $HMAC_{key}(x)$ process is low within a few μsecs, which reduces the effect of DoS attacks on the network compared to the computationally-expensive ECDSA-based signatures.

C. Security Evaluation of the PHY Challenge-Response

In this subsection, the security strength of the PHY challenge-response algorithm is evaluated under different adversarial scenarios by considering Eve as a passive and active attacker who knows the algorithm's schematic diagram. Eve is a passive attacker who can eavesdrop on the challenge signal and its related response and try to deduce any helpful information about the extracted shared key. However, the key cannot be deduced easily from the PHY response for two main reasons: 1) the High sensitivity of the channel multipath components to the distance between the communicating terminals, which makes it hard to differentiate between the initial signal's random phases θ_i and channel-phase response ξ_i. 2) According to the Avalanche effect [54]; By considering the PHY response generation process as a separate cryptographic operation $R(.)$ with input $I = (\theta_i, \xi_i)$ and output $O \leftarrow R(I); R(.)$ depends on the phase difference operation $\Delta\widehat{\psi}_{in}$ in (6), in which, Bob's random choice of the subcarrier index $n \in [1, N]$ denotes different output O under the same input I with probability $1/N$. According to these reasons, it is hard for Eve to estimate sensible information about the extracted key. Thus, by considering Eve as an active attacker, three primary potential attacks can be constructed in this scenario: replay, impersonation, and modification attacks.

1) *Resistance to impersonation attack:* Under this attack, Eve attempts to impersonate Alice or Bob. Suppose Eve is trying to impersonate Bob by generating a valid response. In that case, she possesses zero information about the extracted shared key and the correct session key $SK_{V_{i-j}}(TS_{\mathcal{L}})$ and has no chance to pass the authentication process successfully. If Eve is trying to impersonate Alice by sending a challenge signal to Bob, she can barely succeed to drive Bob's authentication key k_b. However, Eve cannot estimate or predict the upcoming $SK_{V_{i-j}}(TS_{\mathcal{L}+1})$ to generate a correct response signal at $TS_{\mathcal{L}+1}$. In addition, she cannot pass the mutual authentication process as she knows nothing about the other part of the extracted key k_a.

2) *Resistance to replay attack:* Eve can capture the transmitted signal from a legitimate terminal at time t and retransmit it back at time $t+\Delta t$. The replayed signal can be the challenge signal as case 1 or the response signal as case 2. In case 1, the challenge signal can be treated as an impersonation attack when Eve is trying to impersonate Alice. She has no opportunity to estimate the subsequent $SK_{V_{i-j}}(TS_{\mathcal{L}+1})$ to generate a correct PHY response. In case 2, it depends on Δt. For $\Delta t > T_c$, the attack can easily be detected as the challenge signal varies over time; and the decision rule depends on the phase of the current challenge signal, while for $\Delta t \leq T_c$, Eve has no chance of success due to the small correlation coefficient of channel-phase responses between the legitimate and wiretap channels.
3) *Resistance to modification attack:* Eve attempts to alter the message contents. In that case, such an attack can easily be detected, and the altered message is rejected due to the lack of reciprocity between the channel-phase response of the forward link $Ch_{A\rightarrow B}(t)$ and that of the reverse link $Ch_{A\leftarrow E\leftarrow B}(t+\Delta t)$ for $\Delta t \leq T_c$.

IV. Performance Evaluation

In this section, satisfying the 4^{th} contribution, we evaluate the performance of the PHY challenge-response algorithm, as well as the computation and communication overheads, in order to elicit its advantages over existing alternatives.

A. Performance Analysis of the PHY Challenge-Response

As part of this section, the detection probability of the re-authentication process is evaluated. Then, simulation and timing analyses are presented.

1) *Detection P_D vs. false alarm P_{FA} probabilities*: Estimating the probability density function (PDF) is necessary to investigate the probabilities of detection and false alarm under different threshold values. Based on the hypothesis testing problem in (12), at a certain threshold value T, P_D is the probability of the corresponding terminal is successfully authenticated as a legitimate party, while P_{FA} is the probability of a third party being authenticated as an authorized terminal. By deriving the cumulative distribution function (CDF) from the PDF of both hypotheses, one can estimate the optimum value of T for an acceptable false alarm probability. According to the central limit theorem (CLT) [55], v in (12) is the circular variance of a specific number of $N \in \{64, 128, 256\}$ subcarriers that can be approximated as a normally distributed random variable with means $\mu_{H_{0,1}}$ and variances $\sigma^2_{H_{0,1}}$ for both hypotheses $H_{0,1}$.

$$\mu_{H_{0,1}} \triangleq E\left(v \mid H_{0,1}\right), \sigma^2_{H_{0,1}} \triangleq Var\left(v \mid H_{0,1}\right) \tag{17}$$

Thus, the PDF $\mathcal{F}(.)$ for both hypotheses $H_{0,1}$ can be formulated as

$$\mathcal{F}(x)|_{\mu_{H_{0,1}},\sigma^2_{H_{0,1}}} = \frac{1}{\sqrt{2\pi\sigma^2_{H_{0,1}}}} e^{-\left(x-\mu_{H_{0,1}}\right)^2/2\sigma^2_{H_{0,1}}} \tag{18}$$

Then, the CDF $\phi(.)$ for both hypotheses can be expressed as

$$\phi(x)|_{\mu_{H_{0,1}},\sigma^2_{H_{0,1}}} = \frac{1}{2}\left[1+\text{erf}\left(\frac{x-\mu_{H_{0,1}}}{\sqrt{2\sigma^2_{H_{0,1}}}}\right)\right] \tag{19}$$

where the error function $erf(z) = \frac{2}{\sqrt{\pi}}\int_0^z e^{-t^2}dt$. Successful authentication is estimated for $v \mid H_0 \leq T$, in which the threshold value T is obtained for acceptable probability of false alarm $P_{FA} = \phi(T)\mid_{\mu_{H_1},\sigma^2_{H_1}} \leq \alpha$ as

$$\phi(T)\mid_{\mu_{H_1},\sigma^2_{H_1}} = \frac{1}{2}\left[1+\text{erf}\left(\frac{T-\mu_{H_1}}{\sqrt{2\sigma^2_{H_1}}}\right)\right] \leq \alpha \tag{20}$$

Then,

$$T = \underset{T'}{\arg\max}\ \ erf\left(\frac{T'-\mu_{H_1}}{\sqrt{2\sigma^2_{H_1}}}\right) \leq 2\alpha - 1 \tag{21}$$

Given T, the probability of detection can be estimated as

$$P_D = \phi(T)\mid_{\mu_{H_0},\sigma^2_{H_0}} \tag{22}$$

2) *Simulation results:* The empirical PDFs under both hypotheses $H_{0,1}$ are estimated through Monte-Carlo simulations. For better performance and since v in (12) obeys the CLT, the decision rule can be taken based on the mean value $\bar{v}$ of the last computed M estimates of v, decreasing the variances $\sigma^2_{H_0}$ and $\sigma^2_{H_1}$ of v's distributions in (18). Thus, the hypothesis testing problem can be expressed as

$$\bar{v} = \frac{1}{M}\sum_{\tau=0}^{M-1} v\left(t'_2-\tau\right) \underset{H_1}{\overset{H_0}{\lessgtr}} T, \text{for} \begin{cases} H_0: & \phi_i = \mathcal{M}\left(k_{b,i}\right) \\ H_1: & \phi_i = \mathcal{M}\left(k_{\text{e},i}\right) \end{cases} \tag{23}$$

Note that, (12) equals (23) at $M=1$. Fig. 6 presents the simulation results, and the theoretical normal distributions $\mathcal{F}(x) \mid H_0$ and $\mathcal{F}(x) \mid H_1$ of (18) for OFDM system with 64 subcarriers at SNR $=$ 5 dB and $M = \{1, 3\}$. As a proof of concept, Fig. 6(b) shows that the variance of $\bar{v}$'s distributions for both hypotheses is smaller than that of v's distributions in Fig. 6(a), enhancing the authentication performance. Moreover, from the same figure, the theoretical and simulation distributions are well matched, as well as $\mathcal{F}(x) \mid H_0$ is well separated from $\mathcal{F}(x) \mid H_1$, making it easier to choose the optimum threshold value T. By decreasing the SNR, the overlapping between both distributions increases, which increases the false alarm probability $\phi(x\mid_{\mu_{H_1},\sigma^2_{H_1}})|_{x=T}$. Since the secret key extraction algorithm is executed without the information reconciliation and privacy amplification stages, the re-authentication process is performed based on the mutuality percentage $R(\%)$ of the extracted key between both terminals that can be expressed as

$$R(\%) = \left(1-\frac{BMR}{BGR}\right)\times 100 \tag{24}$$

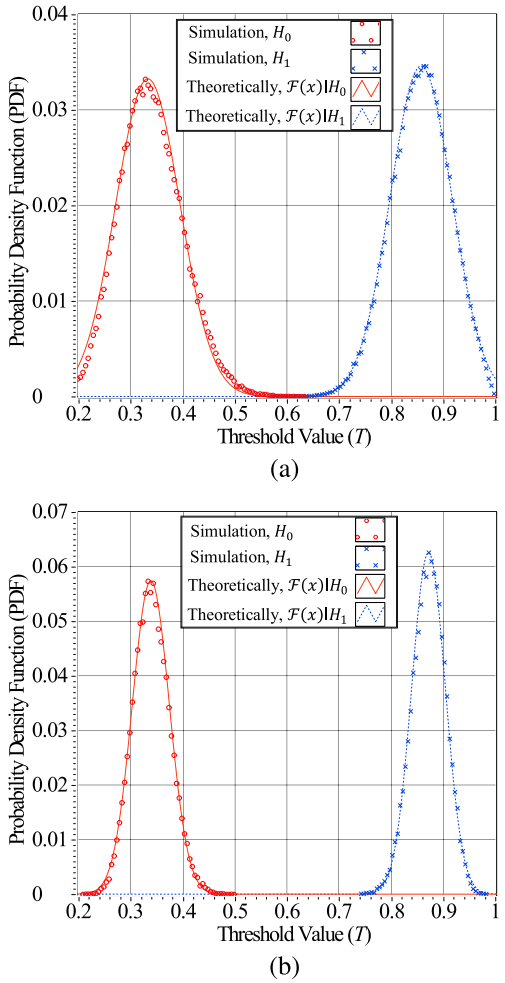

Fig. 6. Simulation and theoretical $\bar{v}$'s distribution for both hypotheses $H_{0,1}$ at $M = \{1, 3\}$ and SNR = 5 dB. $\bar{v}$'s distribution is based on the mean value of v's last M estimates. (a) $\bar{v}$'s PDF for both hypotheses at $M = 1$ and SNR = 5 dB. (b) $\bar{v}$'s PDF for both hypotheses at $M = 3$ and SNR = 5 dB.

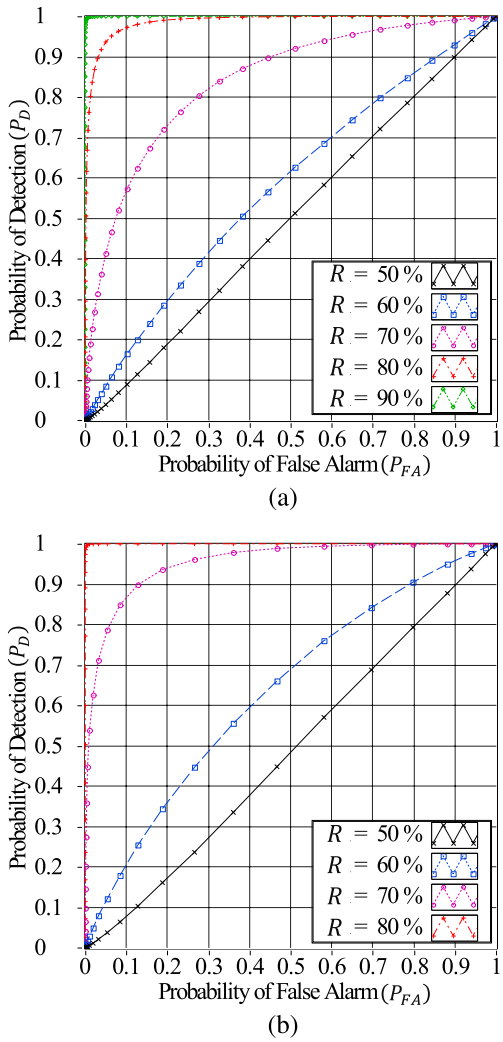

Fig. 7. P_D versus P_{FA} at SNR = 5 dB and $M = \{1, 3\}$ for different key mutuality percentages $R(\%)$. (a) ROCs at $M = 1$ and and $R = \{50, 60, 70, 80, 90\}\%$. (b) ROCs at $M = 3$ and $R = \{50, 60, 70, 80\}\%$.

for

$$BGR = \frac{no.\ extracted\ bits}{no.\ channel\ samples},$$
$$BMR = \frac{no.\ erroneous\ bits}{no.\ channel\ samples} \tag{25}$$

where BGR and BMR are the bit generation rate and bit mismatch rate, respectively [43]. The independent mapping operation $\mathcal{M}(.)$ in (7) is a one-to-one mapping operation (each 2-bits for each subcarrier) which means that a sufficient number of matched bits in the extracted key from S2 is required to discriminate between Bob and Eve, avoiding false decision making. In other words, a sufficient mutuality, indicated by R in (24), must be assured to successfully authenticate the communicating vehicle. Fig. 7 shows the receiver operating characteristics (ROCs; P_D versus P_{FA}) at different $R = \{50, 60, 70, 80, 90\}\%$ percentages and $M = \{1, 3\}$. It can be noted from Fig. 7 that Alice and Bob must maintain over 80% and 70% mutuality of the shared key for $M = 1$ and 3, respectively, to achieve a high $P_D \geq 0.9$ at $P_{FA} \leq 0.1$.

In case of miss-detection $v \mid H_0 > T$, we use v in (12) as a feedback to express the mutuality percentage R of the extracted key from S2. The value of $v \in [0, 1]$ in (12) is exploited to indicate the level of channel non-reciprocity, modeled through the standard deviation σ_c in (3). In [43], the perturb-observe algorithm is used to adjust the quantisation levels at different σ_c values by employing the cumulative distribution function and average fade duration statistics to determine the new threshold levels. Fig. 8 demonstrates the relationship between the expectation $E(v \mid R)$ at different $R = [50, 100]\%$ and SNR = $\{5, 10\}$ dB. It can be noted that increasing the matching percentage R decreases the expectation $E(v \mid R)$ and vice versa. This proves the ability of the re-authentication process to be an alternative to the information reconciliation stage for the thresholds optimisation engine S2.3.

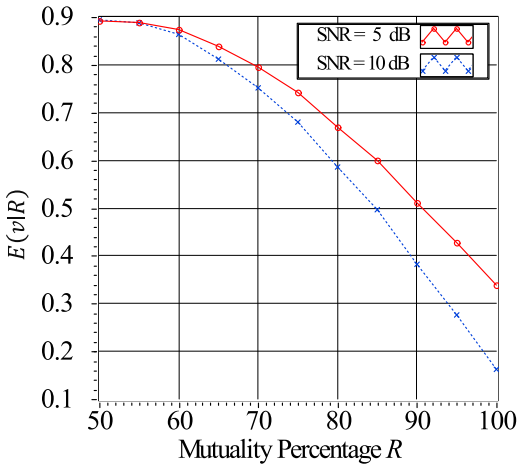

Fig. 8. The key mutuality percentages $R(\%)$ versus the expectation value of v in (17) $E(v \mid R)$ at SNR = {5, 10} dB.

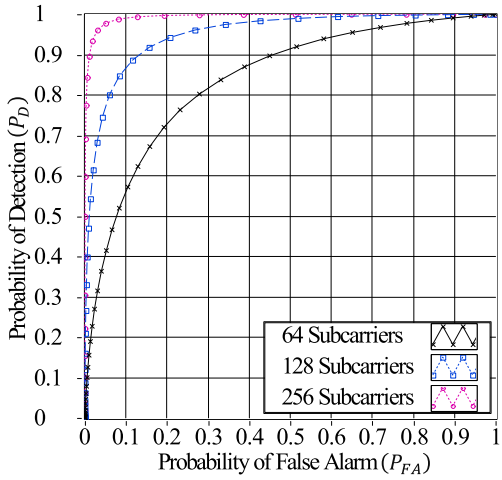

Fig. 9. P_D versus P_{FA} at $R = 70\%$, $M = 1$, SNR = 5 dB, and number of subcarriers $N = \{64, 128, 256\}$ subcarriers.

TABLE IV
COMPUTATIONAL OVERHEAD OF THE PHY CHALLENGE-RESPONSE ALGORITHM IN $msec$

Execution Time	N=64	N=128	N=256
Challenge $T_{PHY_{chang}}$	0.562	1.011	2.053
Response $T_{PHY_{resp}}$	0.39	0.823	1.72
Verification $T_{PHY_{verf}}$	0.125	0.291	0.469

3) *Timing analysis:* In a real environment and the case of high-speed dynamic terminals, the time difference between transmitting the PHY challenge and receiving its related response must be less than the coherence time $(t_2 - t_0) < T_c$, which is the sum of the uplink $(t_1 - t_0)$ and the downlink $(t_2 - t_1')$ propagation time and the processing time of generating the PHY response $(t_1' - t_1)$, where t_0, t_1, t_1', and t_2 are the time of the signals in (4), (5), (8), and (9), respectively. For V2V communication, the DSRC bandwidth is assigned from 5.85 to 5.925 GHz [8]; thus, the maximum Doppler shift arising from the vehicles' and scatterers' speeds, $u_{V_{1(2)}}$ and u_S, is $f_{d(max)} = (u_{V_{1(max)}} + u_{V_{2(max)}} + 2u_{S(max)})/\lambda =$ 2360 Hz [43], where $u_{V_{1(max)}} = u_{V_{2(max)}} = u_{S(max)} =$ 30 m/s at 5.9 GHz carrier frequency. While the minimum coherence time is $T_{c(min)} = 1/f_{d(max)} = 0.4237\ msec$ [43]. The propagation time T_P is evaluated to be 10 μsec for 3 km distance between both terminals.

Since v's distribution obeys the CLT [55], increasing the number of subcarriers N decreases the variances $\sigma^2_{H_0}$ and $\sigma^2_{H_1}$ of v's distribution in (18), improving the ROCs at small mutuality percentages, as demonstrated in Fig. 9. Table IV presents the processing time of the PHY challenge $T_{PHY_{chang}}$, response $T_{PHY_{resp}}$, and verification $T_{PHY_{verf}}$ processes at different numbers of subcarriers $N = \{64, 128, 256\}$ subcarriers, which evaluated using Intel Core i7 2.7 − GHz processor with 16.0 GB RAM. From Table IV, the estimated $T_{PHY_{resp}}$ is in the order of 0.39 $msec$ at $N = 64$ subcarriers; thus, the total processing time $(2T_P + T_{PHY_{resp}})$ is 0.41 $msec\mid_{N=64}$, smaller than $T_{c(min)}$. In addition, it can be noted from the same table that increasing the number of subcarriers (i.e., $N = \{128, 256\}$ subcarriers), increases the processing time $T_{PHY_{resp}}$, limiting the efficiency of the proposed algorithm at high-speed terminal conditions (i.e., $(2T_P + T_{PHY_{resp}}) = 0.843\ msec\mid_{N=128} = 1.74\ msec\mid_{N=256} > T_{c(min)}$). It is considered a tradeoff between high ROCs at low mutuality percentages and that at high-speed terminals.

B. Comparison of Computation and Communication Overheads

Computation and communication complexities are important aspects to be considered when evaluating system performance. Table V compares computation and communication overheads for verifying and sending n signatures from a single vehicle using the proposed scheme, ID-MAP [13], CPPA [14], and NERA [15]. The following time quantities, $T_m, T_e, T_{M\to P}, T_{HMAC}$, and $T_{PHY_{verf}}$, represent the time consumed by scalar multiplication of the ECC, bilinear pairing, map-to-point hashing, hash message authentication code, and PHY-layer verification (S3.4), respectively. Furthermore, Table V classifies the performance metrics of each scheme according to the classification represented in Table II.

1) *Computation overhead analysis:* This part demonstrates the computational comparison in detail. For an accurate computational evaluation, in Table VI, the execution time of multiple cryptographic operations over different curve parameters is computed in [56] by using Intel Core i7 and the widely used MIRACL cryptographic library [57]. In our scheme, the time consumed for verifying n received signatures from a single vehicle is $T_m + T_{HMAC} + nT_{PHY_{verf}}$, in which $T_m + T_{HMAC}$ is the running time for the signature verification stage (S1.3.3) at the first time slot and $nT_{PHY_{verf}}$ for the PHY-layer verification (S3.4) of the subsequent n received PHY-responses.

TABLE V
COMPUTATION AND COMMUNICATION OVERHEADS OF VERIFYING AND DISTRIBUTING n SIGNATURES

Scheme	Computation overhead at the		Classification based on Table II	Communication overhead at the		Classification based on Table II
	proxy vehicle	endpoint terminal		proxy vehicle	endpoint terminal	
ID-MAP	$(d+6)T_m$	$5\lceil\frac{n}{d}\rceil T_m$	Low (endpoint)	$204d$	$184\lceil\frac{n}{d}\rceil + 124n$	High (endpoint)
CPPA	–	$(n+2)T_m$	Low	–	$107n$	High
NERA	–	$3T_e + nT_m + nT_{M\to P}$	Medium	–	$62n$	Medium
Our scheme	–	$T_m + T_{HMAC} + nT_{PHY_{verf}}$	Low	–	$176 + 58.5n$	Medium

TABLE VI
COMPUTATIONAL OVERHEAD OF DIFFERENT CRYPTOGRAPHIC OPERATIONS IN $msec$ [56]

Definition of the operation	Symbol	Run time
Scalar multiplication of the ECC in $\mathbb{G}$	T_m	0.442
Point addition of the ECC in $\mathbb{G}$	T_a	0.0018
Scalar multiplication of the BP in $\mathbb{G}_1$	T_{sm-BP}	1.709
Point addition of the BP in $\mathbb{G}_1$	T_{pa-BP}	0.0071
One-way hash function operation	T_h	0.0001
The map-to-point hashing operation in $\mathbb{G}_1$	$T_{M\to P}$	4.406
Bilinear Tate pairing operation in $\mathbb{G}_1$	T_e	4.211

In ID-MAP [13], the verification process at the side of the proxy vehicle costs about $(d+6)T_m$ (for $d_{\max} = 300$ messages as recommended in [58]), while this value at the endpoint terminals is $5\lceil\frac{n}{d}\rceil T_m$. Furthermore, it can be noted from Table V that the verification processes in CPPA [14] and NERA [15] require about $(n+2)T_m$ and $3T_e + nT_m + nT_{M\to P}$, respectively.

To verify 1000 subsequent signatures sent from a single vehicle, the time required for the verification process at the endpoint in our scheme is 125.4 $msec$ $[= T_m + T_{HMAC} + nT_{PHY_{verf}} = 0.44 + 0.0008 + (1000 \times 0.125)]$ for $T_{HMAC} = 0.0008$ $msec$ and $T_{PHY_{verf}} = 0.125$ $msec$ of 64 subcarriers, while this value in ID-MAP at $\lceil\frac{n}{d}\rceil$ proxy vehicles and the endpoint (RSU) are 135.2 $msec$ $[= (d+6) \times T_m = 306 \times 0.44]$ and 8.84 $msec$ $[= 5 \times \lceil\frac{n}{300}\rceil \times T_m = 5 \times \lceil\frac{1000}{300}\rceil \times 0.44]$, respectively. It can be noted that ID-MAP provides lower computational overhead at the RSU as an endpoint terminal than our proposed scheme, as shown in Fig. 10, whereas the latter provides a lower computational overhead than that of ID-Map at the side of the proxy vehicles. However, if there are no existing proxy vehicles with enough computational resources, all the generated signatures will be singularly verified by the RSU with computational overhead equals 443 $msec$ $[= (d+6) \times T_m = 1006 \times 0.44]$. The time required for the verification process in CPPA and NERA are 442.8 $msec$ $[= (n+2) \times T_m = 1002 \times 0.44]$ and 4858 $msec$ $[= 3T_e + nT_m + nT_{M\to P} = (3 \times 4.2) + (1000 \times 0.44) + (1000 \times 4.4)]$, respectively. It is proven that the proposed scheme is more computationally efficient than the mentioned signature-based schemes [14], [15], and [13] at the side of the proxy vehicle. Also, applying the proposed approach in V2I authentication using proxy vehicles as a future work can provide better performance than [13] at the RSU as an endpoint terminal.

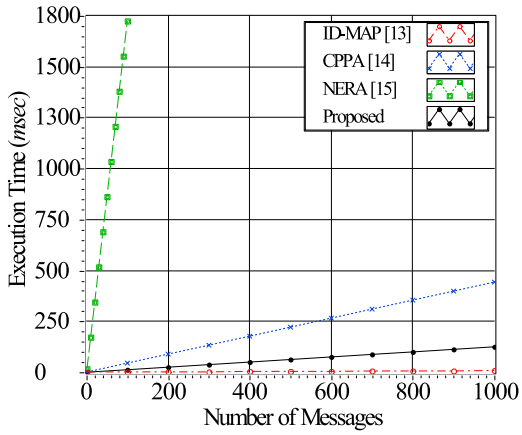

Fig. 10. Computation overheads of verifying $n = 1000$ subsequent signatures transmitted from a single vehicle.

2) *Communication overhead analysis:* In this subsection, we evaluate and compare the proposed scheme's communication overhead. For 80 bits security level of the ECC, we assumed $|q|$ and $|\mathbb{G}|$ to be 20 and 40 bytes, respectively. In addition, the length of the timestamp is assumed to be 4 bytes. The size of the communication request $\langle A_1, T_1\rangle$ in (S1.3.1) is $40 + 4 = 44$ bytes, where $A_1 \in \mathbb{G}$. Also, the size of the generated signature $\langle TID_{V_2}, PID_{V_2}, \sigma_{V_2}, A_2, T_2\rangle$ in (S1.3.2) is $40 + 60 + 32 + 40 + 4 = 176$ bytes long for Hash-SHA-1 and HMAC-SHA256 with 160 and 256 output-bits, respectively, and $(TID_{V_2}, PID_2^1, A_2) \in \mathbb{G}$.

This part presents a detailed comparison of communication overheads. From Table V, the overall communication overhead of the proposed scheme equals $176 + 58.5n$ bytes, which is the sum of that of the ACPPA signature at the first time slot (176 bytes), PHY communication request ($22.5n$ bytes), PHY response with key length of 128 bits for 64 subcarriers ($16n$ bytes), and $SK_{V_{i-j}}(TS_{\mathcal{L}})$ of length ($20n$ bytes) at subsequent n time slots. From Table V, the signature size sent to the proxy vehicles in ID-MAP [13] is $204d$, while this value at the endpoint (RSU) is $184\lceil\frac{n}{d}\rceil + 124n$. In CPPA [14] and NERA [15], the lengths of the generated signatures are $107n$ and $62n$, respectively. To transmit 1000 subsequent signatures from a single vehicle, the size of the transmitted signatures in our scheme is 58674 bytes $[= 176 + (58.5 \times 1000)]$, while this value in ID-MAP [13] at the proxy vehicle, ID-MAP [13] at the endpoint terminal, CPPA [14], and NERA [15] are 61200 bytes $[= 204 \times 300]$ for $d = 300$, 124736 bytes $[=$

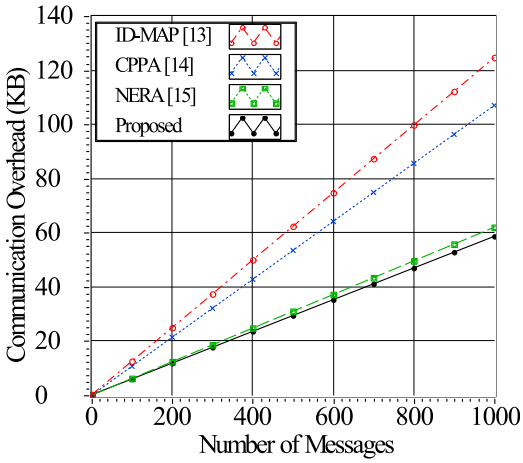

Fig. 11. Communication overheads of transmitting $n = 1000$ subsequent signatures from a single vehicle.

$(184 \times \lceil \frac{1000}{300} \rceil) + (124 \times 1000)]$, 107000 bytes $[= 107 \times 1000]$, and 62000 bytes $[= 62 \times 1000]$, respectively, as shown in Fig. 11. Compared to traditional methods, our scheme has the lowest communication overhead.

Based on the overall computation and communication analyses, we conclude that the proposed scheme outperforms CPPA [14]. Even though ID-MAP [13] is slightly more computationally efficient under a specific condition of proxy vehicles' existence, it has a significantly higher communication overhead in V2I communication, see Fig. 11. Furthermore, Fig. 10 shows that NERA [15] is significantly more computationally costly than all its competitors since it is bilinear pairing-based, despite having a slightly higher communication overhead than ours in Fig. 11. In this regard, the proposed scheme's lightweight re-authentication at the physical layer maintains a balance and optimises the trade-off between the computation and communication overheads between the computation and communication overheads, thereby enhancing network scalability. Aside from this, considering the channel's physical characteristics, our scheme is more effective in detecting Sybil attacks and reducing the impact of the flooding type of DoS attacks on the network, as demonstrated in Section III. Both of these attacks are common for signature-based authentication.

V. Conclusion

In this paper, we introduced a novel cross-layer authentication scheme for secure vehicular communication. In this scheme, a signature-based authentication algorithm is proposed to determine the legitimacy of the corresponding vehicle at the first time slot, employing the secret key generation algorithm in [43] for extracting a high entropy shared key with a minimum number of mismatched bits, avoiding the high communication overhead of the information reconciliation stage. The proposed scheme is the first authentication scheme that uses the PHY-layer challenge-response algorithm in VANETs applications, offering a high and successful authentication rate of up to 8000 $signatures/sec$. Simulation and implementation results proved the capability of the proposed algorithm to support a high probability of detection ≥ 0.9 at low false alarm probabilities ≤ 0.1 under small SNR values ≥ 5 dB, and key mutuality percentages $\geq 70\%$. According to the comprehensive comparison, the time required for verifying 1000 signatures in our scheme is improved by $71\%, 72\%$, and 97% compared to ID-MAP [13] at the side of the proxy vehicle, CPPA [14], and NERA [15], respectively. As a further advantage, the proposed scheme can detect and mitigate Sybil and Dos attacks, which are common for crypto-based authentication approaches. In future work, the proposed cross-layer scheme could be applicable in authentication-based proxy vehicles, providing higher performance than traditional proxy vehicle-based techniques. We will also investigate the performance of the scheme in a realistic vehicular wireless channel at different vehicle speeds for VANET applications.

Proof: Considering an adversary $\mathcal{A}$ who is trying to forge σ_{V_2} of the vehicle V_2 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 $T_{H_1}[.]$ and $T_{HMAC}[.]$ to simulate random oracles $H_1(.)$ and $HMAC_{key}(.)$, then answers $\mathcal{A}$'s oracle queries as follows:

- *Identity (ID) queries:* For a query $(TID_{V_2}, PID_2^1, A_2)$, C holds $\langle A_1, (a_2, \alpha_2 \in Z_q^*)\rangle$, randomly selects r_{V_2} and $\beta \in Z_q^*$, then computes $A_2 = a_2 \cdot P, PID_2^1 = \alpha_2 \cdot r_{V_2} \cdot P, PK_{V_2,TA} = r_{V_2} \cdot \beta \cdot P, \varrho = \alpha_2 \cdot PK_{V_2,TA}$, and $TID_{V_2} = r_{V_2} \cdot A_1$. If $T_{H_1}[\varrho]$ is defined, then C halts, returns $\perp$, and sets $false \leftarrow true$, otherwise, it sets $T_{H_1}(\varrho) \leftarrow H : \{0,1\}^{N_1}$, and returns $(TID_{V_2}, PID_2^1, A_2)$ to $\mathcal{A}$ under (r_{V_2}, β).
- *Sign queries:* For a query $(PID_2^2, \sigma_{V_2}, T_2)$, C selects $RID_{V_2} \in \{0,1\}^{N_2}$ at timestamp T_2, obtains H from ID queries, then computes $SK_{V_{1-2}} = a_2 \cdot A_1$ and $PID_2^2 = RID_{V_2} \oplus H$. If $T_{HMAC}[TID_{V_2} \| PID_{V_2} \| T_2]$ is defined, C halts, returns $\perp$, and sets $false \leftarrow true$. Otherwise, it sets $HMAC_{SK_{V_{1-2}}}(TID_{V_2} \| PID_{V_2} \| T_2) \leftarrow \sigma_{V_2} : \{0,1\}^{N_2}$, and returns $(PID_2^2, \sigma_{V_2}, T_2)$ to $\mathcal{A}$ under RID_{V_2}.

Finally, it is assumed that $\mathcal{A}$ successfully generated a forged signature $\langle TID_{V_2}, PID_{V_2}, \sigma_{V_2}, A_2, T_2\rangle$ under $\langle r_{V_2}, \beta, RID_{V_2}\rangle$ based on q_{ID} and q_s queries for ID and Sign 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*:* Algorithm C did not abort due to signature simulation.
- *Event* E_2*:* Non-trivial forgery is successfully returned by adversary $\mathcal{A}$.

The probability $\Pr[\neg false]$ must be computed, in which false indicates that the algorithm C aborts as a result of ID and Sign queries. The probability is evaluated according to the following claims.

Claim 1. $\Pr[E_1] = \Pr[\neg false] \geq 1 - \frac{q_{ID}^2 q_S^2}{|N_1||N_2|}$

Proof: The probability $\Pr[false]$ can be evaluated by estimating the multiplication of the following probabilities.

- *Scenario 1.* $false \leftarrow true$ is obtained in the ID queries if H is occurred by chance in a previous query to the oracle

$H_1(.)$ under (r_{V_2}, β). There are at most q_{ID} queries in table $T_{H_1}[.]$, the probability for a single ID query is at most $\frac{q_{ID}}{|N_1|}$, and the probability for q_{ID} queries is $\frac{q_{ID}^2}{|N_1|}$.

- *Scenario 2*. $false \leftarrow true$ is obtained in the Sign queries if σ_{V_2} is occurred by chance in a previous query to the oracle $HMAC_{SK_{V_{1-2}}}(.)$ under $SK_{V_{1-2}} \in \mathbb{G}$ and RID_{V_2}. There are at most q_s queries in table $T_{HMAC}[.]$, the probability for a single Sign query is at most $\frac{q_s}{|N_2|}$, and the probability for q_s queries is $\frac{q_s^2}{|N_2|}$.

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

Proof: $\Pr[E_2 \mid E_1]$ is the probability that $\mathcal{A}$ generates a valid forgery, and C does not halt due to $\mathcal{A}$'s ID and Sign queries which means that all responses to these queries are valid. Therefore $\mathcal{A}$ will produce a valid forgery with probability ϵ.

At last, the probability that $\mathcal{A}$ successfully impersonates V_2 by computing a non-trivial forgery under $\langle r_{V_2}, \beta, RID_{V_2} \rangle$ is at least

$$\epsilon_{\text{Sig.Gen}} = \epsilon \left(1 - \frac{q_{ID}^2 q_S^2}{|N_1|\,|N_2|}\right)$$

REFERENCES

[1] WHO, "2nd Global Safety Report on Road Safety 2011–2020." [Online]. Available: https://www.who.int/groups/united-nations-road-safety-collaboration/decade-of-action-for-road-safety-2011-2020

[2] CARE, "European road accident database," Jun. 2020. [Online]. Available: https://ec.europa.eu/transport/media/news/2020-06-11-road-safety-statistics-2019_en

[3] UNECE, "A foundational safety system concept to make roads safer in the decade 2021-2030," Jul. 2020. [Online]. Available: https://unece.org/transport/publications/safety-system-concept-make-roads-safer

[4] R. Jiang and Y. Zhu, "Wireless access in vehicular environment," *Encyclopaedia Wireless Netw.*, pp. 1463–1468, Jan. 2020.

[5] D. Manivannan, S. Moni, and S. Zeadally, "Secure authentication and privacy preserving techniques in vehicular ad-hoc networks (VANETs)," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100247.

[6] M. Raya and J. P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw.*, 2005, pp. 11–21.

[7] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Int. Trans. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.

[8] S. Wang, K. Mao, F. Zhan, and D. Liu, "Hybrid conditional privacy preserving authentication scheme for VANETs," *Peer-to-Peer Netw. Appl.*, vol. 13, pp. 1600–1615, Apr. 2020.

[9] J. Wang, Y. Shao, Y. Ge, and R. Yu, "Physical-layer authentication based on adaptive Kalman filter for V2X communication," *Veh. Commun.*, vol. 26, Jul. 2020, Art. no. 100281.

[10] M. A. Al-Shareeda, M. Anbar, and I. Hasbullah, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors J.*, vol. 21, no. 2, pp. 2422–2433, Jan. 2021.

[11] M. Myers et al., "X.509 internet public key infrastructure online certificate status protocol - OCSP (RFC 2560)," *IETF*, vol. 2560, pp. 1–23, Jun. 1999.

[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptol. Technol.*, 1984, pp. 47–53.

[13] M. R. Asaar, M. Salmasizadeh, W. Susilo, and A. Majidi, "A secure and efficient authentication technique for vehicular ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5409–5423, Jun. 2018.

[14] N. W. Lo. and J. L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.

[15] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A new and efficient RSU based authentication scheme for VANETs," *Wireless Netw.*, vol. 26, pp. 3083–3098, Jun. 2019.

[16] D. Chaum and E. V. Heyst, "Group signatures," *Workshop Theory Appl. Cryptol. Techn.*, vol. 547, pp. 257–265, 1991.

[17] L. Zhang, Q. Wu, A. Solanas, and J. D. Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[18] 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.

[19] K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Hybrid algorithm to detect DDoS attacks in VANETs," *Wireless Pers. Commun.*, vol. 114, pp. 3613–3634, Jun. 2020.

[20] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, Jul. 2017, Art. no. 1930.

[21] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[22] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1791–1802, Sep. 2013.

[23] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171–4182, Jun. 2016.

[24] J. Liu, X. Wang, and H. Tang, "PHY layer authentication enhancement using maximum SNR ratio based cooperative AF relaying," *Wireless Commun. Mobile Comput.*, vol. 4, pp. 1–16, Jan. 2017.

[25] W. Chin, T. Nghia Le, and C. Tseng, "Authentication scheme for mobile OFDM based on security information technology of physical layer over time-variant and multipath fading channels," *Inf. Sci.*, vol. 321, pp. 238–249, Nov. 2015.

[26] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[27] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, Mar. 2019.

[28] R. Liao et al., "Deep-learning-Based physical layer authentication for industrial wireless sensor networks," *Sensors*, vol. 19, no. 11, May 2019, Art. no. 2440.

[29] W. Hou, X. Wang, J. Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, May 2014.

[30] X. Li, J. Liu, B. Ding, Z. Li, H. Wu, and T. Wang, "A SDR-based verification platform for 802.11 PHY layer security authentication," *World Wide Web*, vol. 23, pp. 1011–1034, Jan. 2019.

[31] P. Ramabadran et al., "A novel PHY layer authentication with PAPR reduction based on channel and hardware frequency responses," *IEEE Trans. Circuits Syst.*, vol. 67, no. 2, pp. 526–539, Feb. 2020.

[32] Y. Ran, H. Al-Shwaily, C. Tang, G. Yun Tian, and M. Johnston, "Physical layer authentication scheme with channel-based tag padding sequence," *IET Commun.*, vol. 13, pp. 1776–1780, Apr. 2019.

[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 Things J.*, vol. 7, no. 5, pp. 3977–3990, May 2020.

[34] N. Zhang et al., "Physical layer authentication for Internet of Things via WFRFT-based gaussian tag embedding," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 9001–9010, Sep. 2020.

[35] H. Wen, J. Zhang, R. Liao, J. Tang, and F. Pan, "Cross-layer authentication method based on radio frequency fingerprint," U.S. Patent 10251058 B2, Apr. 02, 2019.

[36] H. Wen and P.-H. Ho, "Physical layer technique to assist authentication based on PKI for vehicular communication networks," *KSII Trans. Internet Inf. Syst.*, vol. 5, no. 2, pp. 440–456, Feb. 2011.

[37] S. Althunibat, V. Sucasas, G. Mantas, and J. Rodriguez, "Physical-layer entity authentication scheme for mobile MIMO systems," *IET Commun.*, vol. 12, no. 6, pp. 712–718, Mar. 2018.

[38] J. Yang, X. Ji, K. Huang, M. Yi, and Y. Chen, "AKA-PLA: Enhanced AKA based on physical layer authentication," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 7, pp. 3747–3765, Jul. 2017.

[39] M. Yao, X. Wang, Q. Gan, Y. Lin, and C. Huang, "An improved and privacy-preserving mutual authentication scheme with forward secrecy in VANETs," *Secur. Commun. Netw.*, vol. 2021, pp. 1–12, Apr. 2021.

[40] H. N. Noura, R. Melk, A. Chehab, and J. Fernandez, "Efficient and secure message authentication algorithm at the physical layer," *Wireless Netw.*, vol. 26, no. 6, pp. 4869–4883, Jun. 2020.

[41] L. Cheng, L. Zhou, B. Seet, W. Li, D. Ma, and J. Wei, "Efficient physical-layer secret key generation and authentication schemes based on wireless channel-phase," *Mobile Inf. Syst. (Hindawi)*, vol. 2017, pp. 1–13, Jul. 2017.

[42] M. Mitev, A. Chorti, M. Reed, and L. Musavian, "Authenticated secret key generation in delay-constrained wireless systems," *EURASIP J. Wireless Commun. Netw.*, vol. 122, Jun. 2020.
[43] M. Bottarelli, P. Karadimas, G. Epiphaniou, D. K. Ben Ismail, and C. Maple, "Adaptive and Optimum Secret Key Establishment for Secure Vehicular Communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2310–2321, Mar. 2021.
[44] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.
[45] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. 1st ACM Conf. Comput. Commun. Secur.*, 1993, pp. 62–73.
[46] B. C. Levy, "Binary and mary hypothesis testing," in *Principles of Signal Detection and Parameter Estimation*. Boston, MA, USA: Springer, pp. 27–32, 2008.
[47] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management—A consolidated proposal for terminology," *Version*, vol. 31, pp. 1–83, Jan. 2007.
[48] P. Karadimas and D. Matolak, "Generic stochastic modeling of vehicle-to-vehicle wireless channels," *Veh. Commun.*, vol. 1, no. 4, pp. 153–167, Aug. 2014.
[49] P. Karadimas, E. D. Vagenas, and S. A. Kotsopoulos, "On the scatterers' mobility and second order statistics of narrowband fixed outdoor wireless channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2119–2124, Jul. 2010.
[50] P. Berens, "CircStat: A MATLAB toolbox for circular statistics," *J. Stat. Softw.*, vol. 31, no. 10, pp. 1–21, Sep. 2009.
[51] X. Wu and Z. Yang, "Physical-layer authentication for multi-carrier transmission," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 74–77, Jan. 2015.
[52] D. York, "Control channel attacks: Fuzzing, DoS, SPIT, and toll fraud," in *Proc. 7th Deadliest Unified Commun. Attacks, Syngress*, 2010, pp. 71–92.
[53] M. J. Faghihniya, S. M. Hosseini, and M. Tahmasebi, "Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network," *Wireless Netw.*, vol. 23, pp. 1863–1874, Apr. 2017.
[54] H. Feistel, "Cryptography and computer privacy," *Sci. Amer.*, vol. 228, no. 5, pp. 15–23, May 1973.
[55] I. Dinov, N. Christou, and J. Sanchez, "Central limit theorem: New SOCR applet and demonstration activity," *J. Statist. Educ.*, vol. 16, no. 2, pp. 1–15, Jul. 2008.
[56] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.
[57] M. Scott, "MIRACL Cryptographic Library: Multiprecision Integer and Rational Arithmetic C/C++ Library," Aug. 2019. [Online]. Available: https://github.com/miracl/MIRACL
[58] Y. Liu, L. Wang, and H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3697–3710, Aug. 2015.

Mahmoud A. Shawky (Student Member, IEEE) was born in 1990 in Saudi Arabia. He received the B.Sc. degree in electronics and electrical engineering from Air Defence College, Alexandria University, Alexandria, Egypt, in 2012, and the M.Sc. (Eng.) degree in authentication mechanisms in computer network protocols from Alexandria University. He is currently working toward the Ph.D. degree with the James Watt School of Engineering, University of Glasgow, Glasgow, U.K. He has demonstrated his expertise in the field through his participation in various conferences and professional events. His research interests include cryptography and number theory, digital signatures, authentication in wireless communications, and physical layer security. He Chaired a session at the VTC-Fall conference in 2022, showcasing his leadership and ability to effectively communicate complex ideas to an audience.

Mirko Bottarelli (Student Member, IEEE) was born in Milan, Italy, in 1980. He received the bachelor's and master's degrees in computer science from Università degli Studi di Milano Bicocca, Milan, Italy, in 2004 and 2006, respectively. He is currently working toward the Ph.D. degree with the Warwick Manufacturing Group, University of Warwick, Coventry, U.K. He is currently a Lecturer of cyber security with the Faculty of Mathematics and Computer Science, University of Wolverhampton, Wolverhampton, U.K. He is also a Member of the Order of Engineers in Italy and a Software Architect and Engineer. His research interests include wireless communication, information theory, physical layer security, blockchain technologies, and other related areas.

Gregory Epiphaniou (Member, IEEE) is currently holds a position as an Associate Professor of security engineering with the University of Warwick, Coventry, U.K. His role involves bid support, applied research and publications. Part of his research interests is formalised around a research group in wireless communications with the main focus on crypto-key generation, exploiting the time-domain physical attributes of V-V channels. He led and contributed to several research projects funded by EPSRC, IUK, and local authorities totalling more than £8M. He is also the main Inventor of a patented-pending technology on a distributed ledger system (GB2576160A/US200042497A1). He was previously holding a position as a Reader in Cybersecurity and acted as deputy Director with the Wolverhampton Cybersecurity Research Institute. He has taught in many universities, both nationally and internationally, a variety of areas related to proactive network defence with more than 120 international publications in journals, and conference proceedings and author in several books and chapters. He holds several industry certifications in Information Security and worked with several government agencies, including the UK MoD, in Cybersecurity related projects. He currently holds a subject matter expert panel position with the Chartered Institute for Securities and Investments. He acted as a technical committee member for several scientific conferences in Information and network security and was a Key Member in the development of WS5 for the formation of the UK Cybersecurity Council.

Petros Karadimas (Senior Member, IEEE) received the M.Eng. and Ph.D. degrees from the Department of Electrical and Computer Engineering, University of Patras, Patras, Greece, in 2002 and 2008, respectively. From December 2009 to August 2011, he was a Research Fellow with the Centre for Wireless Network Design, University of Bedfordshire, Luton, U.K., where he was a Lecturer in electronic engineering in September 2011. In August 2016, he was a Lecturer in electrical and electronic engineering with the James Watt School of Engineering, University of Glasgow, Glasgow, U.K., where he established a research group focusing on design and optimization of antenna arrays and MIMO antennas informed by electromagnetic wave propagation and information theory principles. He also led a cross-disciplinary research activity in physical layer security for vehicular communications. He initiated the development and establishment of the Communications Sensing and Imaging research theme of the James Watt School of Engineering, University of Glasgow. Since January 2022, he has been an Associate Professor with the School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh, U.K. His research interests include radio propagation and wireless channel modeling, antenna arrays and MIMO antennas, communication and information theory, and physical layer wireless security and secrecy.