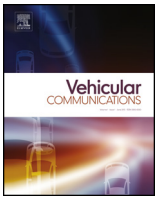
Vehicular Communications 39 (2023) 100547

Contents lists available at ScienceDirect

Vehicular Communications

journal homepage: www.elsevier.com/locate/vehcom



Adaptive chaotic map-based key extraction for efficient cross-layer authentication in VANETs

Mahmoud A. Shawky [a,*], Muhammad Usman [b], Muhammad Ali Imran [a], Qammer H. Abbasi [a], Shuja Ansari [a,*], Ahmad Taha [a,*]

[a] James Watt School of Engineering, University of Glasgow, G12 8QQ, Glasgow, UK
[b] School of Computing, Engineering and Built Environment, Glasgow Caledonian University, G4 0BA, Glasgow, UK

ARTICLE INFO

Article history:
Received 5 July 2022
Received in revised form 3 November 2022
Accepted 8 November 2022
Available online 14 November 2022

Keywords:
Chebyshev chaotic mapping
Cross-layer authentication
Doppler emulation
Physical-layer signatures
Secret key extraction
Vehicular ad-hoc networks

ABSTRACT

Vehicle-to-everything (V2X) communication is expected to offer users available and ultra-reliable transmission, particularly for critical applications related to safety and autonomy. In this context, establishing a secure and resilient authentication process with low latency and high functionality may not be achieved using conventional cryptographic methodologies due to their significant computation costs. Recent research has focused on employing the physical (PHY) characteristics of wireless channels to develop efficient discrimination techniques to overcome the shortcomings of crypto-based authentication. This paper presents a cross-layer authentication scheme for multicarrier communication, leveraging the spatially/temporally correlated wireless channel features to facilitate key verification without exposing its secrecy. By mapping the time-stamped hashed key and masking it with channel phase responses, we create a PHY-layer signature, allowing for verifying the sender's identity while employing the correlated channel responses between subcarriers to verify messages' integrity. Furthermore, we developed a Diffie-Hellman secret key extraction algorithm that employs the computationally intractable problems of the Chebyshev chaotic mapping for channel probing. Thus, terminals can extract high entropy shared keys that can be used to create dynamic PHY-layer signatures, supporting forward and backward secrecy. We evaluated the scheme's security strength against active/passive attacks. Besides theoretical analysis, we designed a 3-Dimensional (3D) scattering Doppler emulator to investigate the scheme's performance at different speeds of a moving vehicle and signal-to-noise ratios (SNRs) for a realistic vehicular channel. Theoretical and hardware implementation analyses proved the capability of the proposed scheme to support high detection probability at SNR $\geq$ 0 dB and speed $\leq$ 45 m/s.

1. Introduction

Due to the advancement in wireless communications and networking technology, vehicular ad-hoc networks (VANETs) have become more prevalent in recent years, thanks to their ability to improve safety and efficiency in transportation [1]. VANET is a form of a mobile ad-hoc network in the vehicle domain that enables direct vehicle-to-everything (V2X) communication (e.g., vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I)) via a dedicated short-range communication (DSRC) protocol [2]. In this protocol, a safety-related message is sent by each vehicle in the network every 100-300 *msec* in accordance with the IEEE 802.11P standard [3]. These messages support many safety-related applications, including traffic management services, collision avoidance, and traffic navigation [1]. Unfortunately, due to the communication nature of VANETs through open access wireless channels, the communication link can be compromised by an adversary, and the message contents can easily be altered, deleted, and replayed, which can lead to serious consequences, e.g., unsafe driving and accidents [4]. Therefore, identity authentication and message integrity are essential security services that must be established to guarantee secure communication between terminals [5]. Generally, the vehicular network comprises three primary entities: a trusted or certificate authority, numerous roadside units (RSUs), and vehicles mounted wireless devices known as onboard units (OBUs).

Public-key certification is commonly used in authentication [6], referred to as public key infrastructure-based (PKI-based) schemes. The main defect with this method is the high communication load

* Corresponding authors.
E-mail addresses: m.shawky.1@research.gla.ac.uk (M.A. Shawky), muhammad.usman@gcu.ac.uk (M. Usman), Muhammad.Imran@gla.ac.uk (M.A. Imran), Qammer.Abbasi@gla.ac.uk (Q.H. Abbasi), Shuja.Ansari@gla.ac.uk (S. Ansari), Ahmad.Taha@gla.ac.uk (A. Taha).

https://doi.org/10.1016/j.vehcom.2022.100547

resulting from distributing the certificate revocation list (CRL) of malicious vehicles between network terminals and the computation cost of checking this list for each received signature. In addition, centralizing certification services on servers could compromise access availability of high mobility terminals. Furthermore, storing a bunch of key pairs and their associated digital certificates requires a large storage capacity. In an effort to address these issues, several identity-based (ID-based) authentication schemes have been introduced [7–16], supporting VANETs' security and privacy requirements. Nevertheless, some of these schemes are subject to the high computation costs of bilinear pairing and map-to-point hashing operations, reducing the network efficiency, particularly in dense traffic conditions. By using group signature-based (GS-based) schemes, group members are able to sign messages anonymously, and only the group manager can track their real identities, thus assuring conditional privacy preservation [17]. However, in order to maintain forward and backward secrecy, the entire group must be reconstructed for each vehicle leaving or joining the group area, which is not feasible at high-speed terminals. In Fig. 1, we summarise the common performance limitations associated with crypto-based authentication in VANETs.

The 5G-based V2X network uses short-range communication in the millimetre wave band to increase the network capacity and the data transfer rate. Nevertheless, the frequent authentication handover poses a significant challenge due to the high computation cost of crypto-based approaches, deteriorating the quality of service. Therefore, the need for a fast and secure authentication process to support communication continuity is vital, which is incompatible with existing signature-based methods [18]. In response to this challenging scenario, recently, many keyless PHY-layer authentication schemes have contributed to a wide range of wireless applications as an efficient distinguishing technique to address the limitations of conventional cryptographic approaches [19–23]. In one of these techniques, the short-term spatially and temporally correlated channel features between two communicating wireless devices, such as the channel state information (CSI) [19], the received signal strength (RSS) [20], the power delay profile [21], and the power spectral density [22] are used to ensure that the received signals $R_X(t)$ and $R_X(t + \Delta t)$ are transmitted from the same source, for $\Delta t \leq$ coherence time T_c. This technique is referred to as the "feature tracking" mechanism.

One of the ways to discriminate between different devices is to exploit the slight variations of the hardware imperfections arising from the manufacturing process, e.g., carrier frequency offset [23], and analog front-end imperfections (I/Q imbalance) [18]. Besides keyless approaches, key/tag-based techniques have emerged to provide reliable authentication at the PHY-layer by superimposing a pre-agreed tagged signal onto the transmitted coded data packet [24]. However, the existing PHY-layer authentication techniques suffer from the following limitations:

1. For channel-based approaches, it is necessary to observe all the corresponding terminals to identify their distinct features within the limited coherence interval, which is not practicable in extremely dense applications. In addition to the low detection rate in conditions of significant channel variations.
2. For hardware imperfections approaches, the slight dissimilarities in the extracted features from different devices can mislead the decision rule.
3. In tag-based approaches, performance and security are traded off at different ratios of signal-to-tag power allocation.

In this sense, PHY-layer-based authentication cannot be used as a standalone solution as an initial legitimacy/identity detection must be carried out using traditional methods. However, it can be complementary to crypto-based approaches implemented at the link and application layers of the protocol stack. This is referred to as "cross-layer authentication" [18]. Hence, it is critical to select the proper PHY-layer method that is functionally compatible with the upper-layer cryptographic technique to satisfy the application requirements related to the range of communication, computation constraints, broadcasting rate, and channel variations.

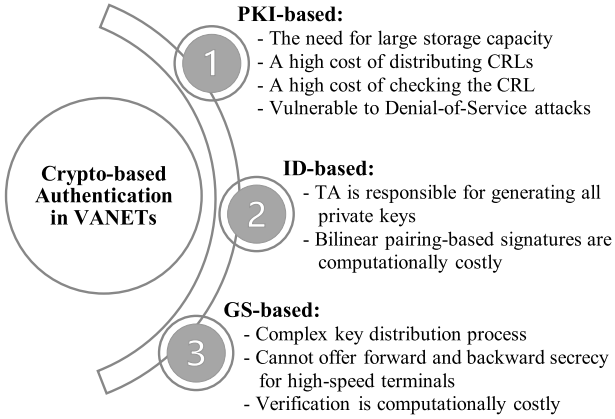


Fig. 1. Performance limitations of authentication in VANET.

In [25], a patent has been presented for RF fingerprinting integrated with PKI-based authentication. Reference [26] presents a different integration method for mobile MIMO systems, whereby PKI-based authentication is applied as an initial authentication step, followed by the feature tracking method for re-authentication. For improved performance, the Adaptive Kalman Filter is employed in [27] to predict the upcoming CSI and RSS based on the previous estimations and compare them with current observations in a 2-Dimensional hypothesis testing problem. Reference [28] integrates the physically unclonable function (PUF) of the integrated circuits with the pseudo-ID-based method. The strength of the PUF technique relies on the unpredictable response R generated from the input challenge C based on the PUF response P so that $R = P(C)$. Despite the ability of these cross-layer methodologies in increasing the authentication rate, they cannot be effectively used for V2X applications due to the high dynamic behaviour of the moving vehicles, which can cause fluctuations in channel fading between high and low levels in urban and rural areas, posing a challenging scenario [18,29]. Therefore, further research is needed to address this limitation.

This study leverages the existing PHY-layer authentication approaches to present an efficient way of identity and integrity verifications in VANETs. Using the key-based approach, we create a time-stamped "PHY-layer signature" for each transmitted data packet of the orthogonal frequency division multiplexing (OFDM) system, which is used to verify the sender's identity. To determine the message's integrity, we examine the correlation of the estimated channel responses between each pair of the received OFDM symbols in a binary hypothesis testing problem. The proposed scheme can serve as an alternative to existing signature-based schemes without violating VANETs security and privacy requirements. This eliminates the considerable computation and communication costs incurred by the need to generate and send a cryptographic signature for every transmission.

We developed a pairwise PHY-layer key agreement algorithm that takes advantage of the short-term reciprocal characteristic of the channel phase response to establish a high entropy secret key between two communicating terminals. Using this key, the PHY-layer signatures are dynamically updated for each session, ensuring forward and backward secrecy. The current state-of-the-art for secret key extraction has been developed, given that more than half a wavelength ($\lambda/2$) separates the network terminals. Thus allow-

ing for location decorrelation between legitimate and wiretapped channel responses, which can be specified by a zero-order Bessel function, where the first zero occurred at a $\lambda/2$ distance between the legitimate user and the adversary [29]. In fact, by applying this assumption in V2I communication, a compromised RSU allows an attacker to gain access to the surrounding vehicles' secret features, making this condition unrealistic in V2I applications. Therefore, we designed a Diffie-Hellman secret key extraction algorithm that incorporates the Chebyshev mapping operation [30] for probing the channel. By doing so, the algorithm does not need a $\lambda/2$ distance between terminals, thus providing an efficient performance for V2X applications. The following is a summary of the main contributions:

1. For key extraction, we proposed a fast and secure key agreement technique for V2X applications. Accordingly, we take advantage of the unique cryptographic properties of the Chebyshev chaotic mapping and the spatially and temporally correlated channel phase responses within the coherence period to design a PHY-layer key extraction algorithm for the OFDM-based DSRC system. A thresholding optimisation strategy is proposed to adjust the size of the thresholding region to the noisy channel phase estimation error in order to optimise the tradeoff relationship between the bit generation rate (BGR) and the bit mismatch rate (BMR), where the BGR is the number of the extracted bits and the BMR is the number of mismatched bits, out of the total number of channel samples.
2. For authentication, we offer key-based and feature tracking mechanisms to allow for PHY-layer identity and integrity verifications, respectively, employing the extracted key and following the initial legitimacy detection using the upper layer's signature-based approaches. By creating a PHY-layer signature as an alternative to the existing crypto-based signatures, the corresponding terminal can securely verify the sender's legitimacy, employing the correlated channel attributes to check the integrity of the received data.
3. For validation, we investigated the proposed scheme's theoretical effectiveness as well as its security robustness against passive and active attacks, including impersonation, replaying, and modification.
4. Further, we introduced a Doppler emulator block to simulate the Doppler components of a 3D scattering V2I scenario in the time domain, see Fig. 13. This block allows for empirically exploring the receiver operating characteristics of the PHY-layer authentication process at various speeds and SNRs for a realistic vehicular wireless channel using a software-defined radio platform, the Universal Software Radio Peripheral (USRP).

The following structure summarizes the rest of the paper. Section 2 provides an overview of recent related works. Section 3 introduces the preliminary knowledge, while the scheme model is presented in Section 4. Performance evaluation and threat modelling are given in Section 5. In Section 6, simulation and hardware implementation analyses are presented. Finally, Section 7 concludes this study.

2. Related works

In recent years, various authentication studies have contributed to VANET applications. In [6], Raya et al. proposed a modified PKI-based scheme in which a large number of anonymous digital certificates along with their related public and private key pairs are stored in vehicles' tamper-proof devices (TPDs). By doing this, vehicles can sign messages anonymously for a period of time, avoiding location tracking attacks and supporting privacy preservation. In order to address PKI limitations regarding CRL management and the requirement for a large storage capacity, recently, several ID-based schemes have been developed [7–16]. Liu et al. [7] proposed the first proxy-based authentication scheme in which the proxy vehicles employ their computation availabilities to verify signatures in favour of the RSUs and broadcast their verification results. In fact, this work is limited to V2I communication without considering the scenario of V2V communication. In [8], Asaar et al. revealed that the scheme presented in [7] is vulnerable to impersonation and modification attacks, then presented a modified proxy-based scheme, offering superior computational performance. However, the improved scheme preloads the TA's master key into vehicles' TPDs, which is insecure due to the high vulnerability to side-channel attacks for imperfect TPDs. Resisting this type of attack, Bayat et al. [9] make use of the secure communication link between the TA and RSUs to store a dynamically updated master key into the RSUs' TPDs. Based on bilinear pairing properties and map-to-point hashing operations, they developed an ID-based scheme that supports batch verification. However, its significant computation complexity motivated Al-shareeda et al. [10] to design a free pairing conditional privacy-preserving authentication scheme, employing the online mode for updating TPD's secret parameters to avoid potential side-channel attacks. However, the communication cost remains high. In a lightweight ID-based solution, Wei et al. [11] employed the factorization problem of the Rivest-Shamir-Adleman cryptosystem for identity verification.

What's more, a recent study by Zhang et al. [12] demonstrated that the proposed scheme in [11] is vulnerable to the common modulus attack, which can expose the vehicles' secret parameters. Mitigating the computation load on the vehicles' side, reference [13] suggested a technique based on edge computing where the RSUs verify the received messages from adjacent vehicles and broadcast their verification results to surrounding vehicles. In [14], Limbasiya et al. demonstrated that [13] had security weaknesses related to concatenation and impersonation attacks, then developed a message authentication approach based on symmetric key cryptography. In reference [15], Lyu et al. employed the Timed Efficient Stream Loss-tolerant Authentication (TESLA) method along with the Elliptic Curve-based digital signatures to design a scheme that forecasts the vehicle's future position for immediate message authentication. Despite this, the high communication cost associated with the Merkle Hash Tree's added leaf values continues to pose a challenging issue. In order to reduce the cost of communication and maintain privacy, Zhong et al. [16] implemented a certificateless aggregation signature scheme that reduces the signature size. However, the authors neglected to consider V2V applications, which is an important aspect given that vehicles have a lower processing power than RSUs.

3. Preliminaries

In this section, the network structure is described, and then we review VANETs' security and privacy requirements and a number of fundamental concepts used in this study.

3.1. Network configuration

VANETs are typically composed of the following entities, see Fig. 2.

1. *The trusted authority* (*TA*): As a trusted third party, TA is responsible for initialising the public parameters and terminals' secret keys as well as preloading them onto registered vehicles and RSUs before joining the network. It is also capable of detecting and revoking misbehaving vehicles through their pseudo-identities.

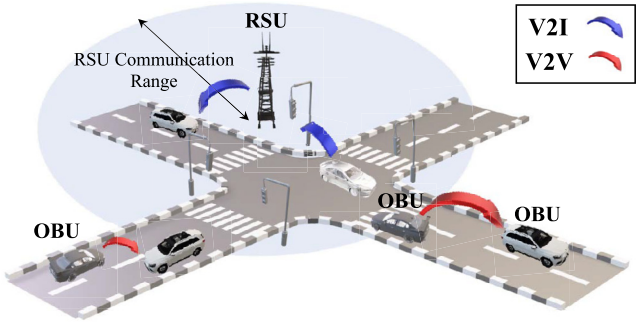


Fig. 2. VANETs architecture.

2. *The RSUs*: Road infrastructures on both sides have wireless communication devices to connect with nearby vehicles and wired communications to connect with the TA. As a gateway, it serves primarily as a cooperative relay and broadcast point within VANETs.
3. *Vehicles' OBUs*: Vehicles are equipped with onboard units that provide wireless communication services and perform all computing functions. Further, each OBU has enough computational resources to generate large integer numbers that function as the vehicle's secret parameters.

The notations used in this paper are listed in Table 1.

3.2. Security and privacy objectives

The proposed scheme complies with the requirements of VANETs, including security and privacy [5] as

1. *Message authentication*: Each message can be verified for authenticity and integrity by the recipient.
2. *Privacy preservation/identity anonymity*: Neither semi-trusted (RSUs) nor distrusted (adjacent vehicles) terminals can deduce identifiable information about the transmitter based on message contents.
3. *Forward and backward secrecy* [31]: A malicious adversary can't discover the shared keys for previous and upcoming sessions based on that of the current session.
4. *Security strength*: The proposed scheme must be immune to typical adversarial attacks as follows [32].
   (a) *Immunity to impersonation*: An adversary tries to forge a trusted terminal's secret parameters to impersonate it. In this case, we analyse two potential scenarios in which the attacker is further or closer than $\lambda/2$ distance from the transmitter (Tx) or the receiver (Rx).
   (b) *Immunity to modification*: In this case, an adversary tampers with the transmitted messages by altering or modifying their contents.
   (c) *Immunity to replaying*: In this case, an adversary retransmits previously broadcasted messages after a period to deteriorate the network performance.

3.3. Mathematical foundations

As part of the proposed scheme, the proposed secret key extraction algorithm takes advantage of the unique cryptographic properties of the Chebyshev chaotic mapping in terms of the significant computational complexities of solving the discrete logarithm and Diffie-Hellman problems to probe the channel. The following are some important theoretical concepts.

1. *Chebyshev chaotic mapping* [30]: $T_n(x)$ is a polynomial mapping function of input $x \in [-1, 1]$ and output $y \in [-1, 1]$ with a constant density $1/\left(\pi\sqrt{1-x^2}\right)$, and n is an integer number. The formulation of $T_n(x)$ is given by:

$$T_n(x) = \begin{cases} \cos\left(n \cdot \cos^{-1}(x)\right), & x \in [-1, 1] \\ \cos(n \cdot \theta), & x = \cos(\theta) \end{cases} \quad (1)$$

where $\theta \in [0, \pi]$.
2. In [33], the chaotic mapping operation in (1) is extended for x belongs to the interval $(-\infty, +\infty)$. The extended map function has two important properties denoted by the following definitions:
   (a) *Definition 1*: Given the two variables $x \in (-\infty, +\infty)$ and y, it is infeasible for an attacker to deduce the integer n, such that $T_n(x) \bmod p \equiv y$, where p is a large prime number. This problem is defined by the Discrete Logarithm Problem (DLP).
   (b) *Definition 2*: Given $x \in (-\infty, +\infty)$, $T_n(x) \bmod p$, and $T_m(x) \bmod p$, the attacker has no chance to estimate $T_{nm}(x) \bmod p$, referred to as the Diffie-Hellman Problem (DHP).
3. The Chebyshev mapping operation $T_n(x) : [-1, 1] \to [-1, 1]$ is employed in the key generation process by taking the inverse cosine of (1) and doubling the input range to get $T'_n(\theta) : [0, 2\pi) \to [0, 2\pi)$, denoted by

$$T'_n(\theta) = \begin{cases} n \cdot \theta \bmod p, & \theta \in [0, 2\pi) \\ n \cdot \cos^{-1}(x) \bmod p, & x = \cos(\theta) \end{cases} \quad (2)$$

where $p = 2\pi$, and n is a large integer number of order $\lceil \log_2(n+1) \rceil$ bits.

Table 1
List of Acronyms.

Symbol	Definition
θ_i	The initial primitive root of the i^{th} subcarrier
n_i, m_i	Tx and Rx secret parameters
r	The quantisation order
$\mathcal{M}(.)$	The mapping function
$\mathcal{M}^{-1}(.)$	The inverse of the mapping function
Δt	The transmission time interval
h_i, ξ_i	Channel amplitude and phase responses
k	The symmetric key and equals $(k_a \| k_b)$
T_r	The signal receiving time
T_Δ	The timestamp expiry period, e.g., [00:00:59]
n_τ	The normalization coefficient
u_a	Vehicle's speed
δ	The distance driven by the vehicle within Δt
r_l	Angle's resolution value of the l^{th} scatterer
ϕ_a, ϕ_b	The mapped signatures
$\alpha_{a,l}, \beta_{a,l}$	Azimuth and elevation angles of departure
Δ_l	The step angle (rad) of the l^{th} scatterer
$\mathcal{D}_l$	Direct distance between the Tx and scatterer
$d_{a,l}$	The Doppler component of the l^{th} scatterer
P_e, P_d	Probabilities of error and detection, respectively
P_{fa}	Probability of false alarm
a_1	The acceptable probability of error
a_2	The acceptable probability of false alarm

4. Scheme modelling

This section describes the adaptive Diffie-Hellman secret key extraction process, and then we present the PHY-layer re-authentication process in detail.

4.1. The Diffie-Hellman key extraction algorithm

Contrary to the current state-of-the-art, the proposed secret key extraction algorithm does not need a $\lambda/2$ distance between users. By employing the Chebyshev-based Diffie Hellman key exchanging protocol in the channel phase response-based key extraction process, the communicating terminals can obtain a high entropy secret key k in any wireless propagation environment (dynamic or even static). In addition, this mechanism allows the channel to be probed repeatedly within the same coherence period T_c, thereby increasing the BGR. In general, the key generation process involves channel probing and thresholding, information reconciliation, and privacy amplification. The former includes exchanging probe signals between vehicles to obtain channel estimates, quantising these estimates, and converting them into bit streams. The reconciliation stage corrects the mismatched bits. As for the privacy amplification stage, this further enhances the secrecy of the extracted bits by hashing the corrected secret key. By applying (2) for an OFDM system of N subcarriers, (2) can be rewritten as

$$T'_{n_i}(\theta_i) = \begin{cases} n_i \cdot \theta_i \bmod p, & \theta_i \in [0, 2\pi) \\ n_i \cdot \cos^{-1}(x_i) \bmod p, & x_i = \cos(\theta_i) \end{cases} \tag{3}$$

where $i = 1, \ldots, N$ and $p = 2\pi$. Let θ_i be the initial primitive root of the i^{th} subcarrier and equals $2\pi/2^r$ for $r \in \{1, 2, 3\}$. The choice of the r value depends on the size of the phase-based thresholding region. In the polar coordinates, for $r = 3, e^{j\theta_i} = e^{j\pi/4}$ is considered as the generator g of the finite cyclic group $Z_{2^r=2^3}$ of order 8, defined as $Z_8 = \langle g \rangle = \{1, g, g^2, g^3, g^4, g^5, g^6, g^7\}$ in which $g^{n_i \bmod 8} = e^{jn_i.\theta_i \bmod 2\pi} = e^{jT'_{n_i}(\theta_i)}$ such that $g^{8 \bmod 8} = e^{j2\pi \bmod 2\pi} = 1$. Any element in the group can create its subgroup. For example, $Z_4 = \langle g^2 \rangle = \{1, g^2, g^4, g^6\}$ of order 4 and $Z_2 = \langle g^4 \rangle = \{1, g^4\}$ of order 2, as shown in Fig. 3. Based on the cyclic group theorem [34], it is computationally infeasible to determine: 1) $T'_{n_i m_i}(\theta_i)$, given $T'_{n_i}(\theta_i)$ and $T'_{m_i}(\theta_i)$, where n_i and m_i are large integer private parameters of the i^{th} subcarrier at the side of Alice and Bob, respectively; 2) the secret parameter n_i, given θ_i and $T'_{n_i}(\theta_i)$, so that the attacker needs $2^{\lceil \log_2(n_i+1) \rceil - r}$ trials to construct a brute-force attack and have a correct estimation, similarly for m_i. Fig. 4 shows the Diffie-Hellman channel probing mechanism between the vehicle $V_i(Alice)$ and the RSU $R_j(Bob)$. For simplicity, in this study, all formulas are denoted in the frequency domain. In a three-step process, the probing and thresholding stage is performed in the half-duplex mode as follows.

1. *Channel probing*: In this step, Alice initiates two subsequent OFDM symbols with random phases $T'_{2n_i}(\theta_i)$ and $T'_{n_i}(\theta_i)$ at time t_0 and $t_0 + \Delta t$ so that the transmitted signals can be formulated as

$$\begin{aligned} s_a(t_0) &= \sum_{i=1}^{N} \sqrt{\frac{2E_S}{T}} e^{j(2n_i\theta_i)} \\ s_a(t_0 + \Delta t) &= \sum_{i=1}^{N} \sqrt{\frac{2E_s}{T}} e^{j(n_i\theta_i)} \end{aligned} \tag{4}$$

where Δt is the transmission time interval $\ll T_c$. The received signal by Bob can be formulated as

$$\begin{aligned} r_b(t'_0) &= \sum_{i=1}^{N} \sqrt{\frac{2|h_i|^2 E_s}{T}} e^{j(2n_i\theta_i + \xi_{b,i})} + N_i \\ r_b(t'_0 + \Delta t) &= \sum_{i=1}^{N} \sqrt{\frac{2|h_i|^2 E_s}{T}} e^{j\left(n_i\theta_i + \xi'_{b,i}\right) +} N'_i \end{aligned} \tag{5}$$

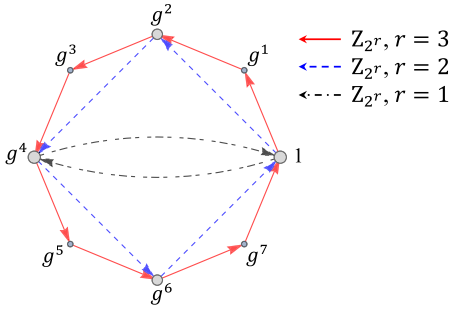


Fig. 3. Cycle graph of order 2^r, for $r = 1, 2, 3$.

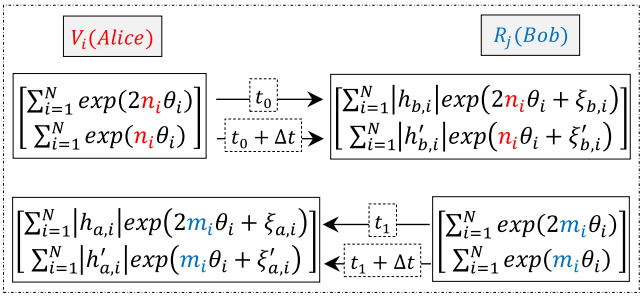


Fig. 4. Diffie-Hellman probing step in a noiseless channel.

where N_i and N'_i are complex additive Gaussian noises $\mathcal{CN}(0, 2EN_0)$ with zero means and variances $2EN_0$, h_i and ξ_i are the Rayleigh fading channel responses of the i^{th} subcarrier for the signal amplitude and phase, respectively, also ξ_i is a uniformly distributed random variable $U[0, 2\pi)$ for $i = 1, \ldots, N$. In a similar way to (4), Bob replies by initiating two OFDM symbols with phases $T'_{2m_i}(\theta_i)$ and $T'_{m_i}(\theta_i)$ at time t_1 and $t_1 + \Delta t$.

2. *Signal equalisation*: In this step, the received signals by Bob are equalized by calculating $e_b(t) = r_b(t'_0)\, r_b(t'_0 + \Delta t)^*$ so that $\angle e_{b,i}(t)$ can be expressed as

$$\angle e_{b,i}(t) = n_i\theta_i + \varepsilon_{b,i} + \left(\omega_{b,i} - \omega'_{b,i}\right) \tag{6}$$

where $\varepsilon_{b,i} = \xi_{b,i} - \xi'_{b,i}$ is the error results from the imperfect channel reciprocity and $\omega_{b,i}$ and $\omega'_{b,i}$ are the phase estimation errors resulted from N_i and N'_i in (5). It is noteworthy that observations at different nodes or timeslots are affected by independent realizations of the noise [35]. With more samples in the observation, the estimation error becomes a zero-mean Gaussian random variable with variance $\sigma^2 \geq$ Cramer-Rao bounds of the phase variance estimation [36], so that the distribution of ω and ω' are $\mathcal{N}(0, \sigma^2)$. Thus, the distribution of $\angle e_{b,i}(t)$ in (6) is also normally $\mathcal{N}(n_i\theta_i + \mathcal{E}_{b,i}, 2\sigma^2)$ with mean $n_i\theta_i + \mathcal{E}_{b,i}$ and variance $2\sigma^2$. After that, Bob computes the round function of $\angle e_{b,i}(t)$ to get $\hat{T}'_{n_i}(\theta_i)$ as

$$\begin{aligned} \hat{T}'_{n_i}(\theta_i) &= Round\left(\angle e_{b,i}(t)\right) \\ &= Round\left(n_i\theta_i + \varepsilon_{b,i} + \left(\omega_{b,i} - \omega'_{b,i}\right)\right) \end{aligned} \tag{7}$$

where $Round(x)$ is a function that rounds x to the nearest multiple of $2\pi/2^r$. Then, Bob obtains $T'_{n_i m_i}(\theta_i)$ by computing $T'_{m_i}(\hat{T}'_{n_i}(\theta_i))$. It is important to perform the *Round* function before calculating $T'_{m_i}(\hat{T}'_{n_i}(\theta_i))$ to avoid the significant error caused from multiplying $\varepsilon_{b,i}$ by the large integer number m_i. The same process is performed at the side of Alice to get $T'_{n_i m_i}(\theta_i) = T'_{n_i}(\hat{T}'_{m_i}(\theta_i))$. The estimated $T'_{n_i m_i}(\theta_i)$ at both sides

are inversely mapped $\mathcal{M}^{-1}(.)$ to convert it into bitstreams k. The order of the inverse mapping operation depends on the r value. For simplicity, a Gray code $\mathcal{M}^{-1}(.)$ of order $r = 2$ bits can be formulated as

$$\mathcal{M}^{-1}\left(T'_{n_i m_i}(\theta_i)\right) = \begin{cases} 00 & T'_{n_i m_i}(\theta_i) \in [-\frac{\pi}{4}, \frac{\pi}{4}) \\ 01 & T'_{n_i m_i}(\theta_i) \in [\frac{\pi}{4}, \frac{3\pi}{4}) \\ 11 & T'_{n_i m_i}(\theta_i) \in [\frac{3\pi}{4}, -\frac{3\pi}{4}) \\ 10 & T'_{n_i m_i}(\theta_i) \in [-\frac{3\pi}{4}, -\frac{\pi}{4}) \end{cases} \tag{8}$$

for $i = 1, \ldots, N$. Note that a Gray code spaces adjacent codes one hamming distance apart, thus reducing the BMR of the extracted keys.

3. *Thresholding optimisation*: In this step, the order of the thresholding region r is optimised for θ_i and $\mathcal{M}^{-1}(.)$ at both sides of the communicating terminals to provide a high secret bit generation rate (SBGR) for acceptable BMR, where SBGR is the number of correct/matched bits to the total number of channel samples. By adapting the size of the quantisation region $2\pi/2^r$ to different conditions of SNRs, the performance of the key extraction process will be optimised. A small quantisation region (i.e., high order of r) denotes high BGR and BMR, and vice versa for large regions. For zero-value private keys ($n_i = m_i = 0$) and negligible non-reciprocity parameter $\left(\varepsilon_{a(b),i} \approx 0\right)$ due to the small transmission time interval ($\Delta t \approx 16$ µs for 64 subcarriers and 16 cyclic prefix samples, in [37]), the distribution of the equalised phase $\angle e_{a(b)}(t)$ in (6) will be $\mathcal{N}\left(0, 2\sigma^2\right)$. Similar to [38], both terminals can exchange m probing packets and have their channel phase estimates $\left(\widehat{\xi}_a^{t_a}, \widehat{\xi}_b^{t_b}\right)$ at timestamps (t_a, t_b) to learn the noisy channel phase error distribution parameters, which equals $\mathcal{N}\left(\mu_{\xi,i}, var_{\xi,i} = \sigma^2\right)$ for mean $\mu_{\xi,i}$ and variance $var_{\xi,i}$ denoted by

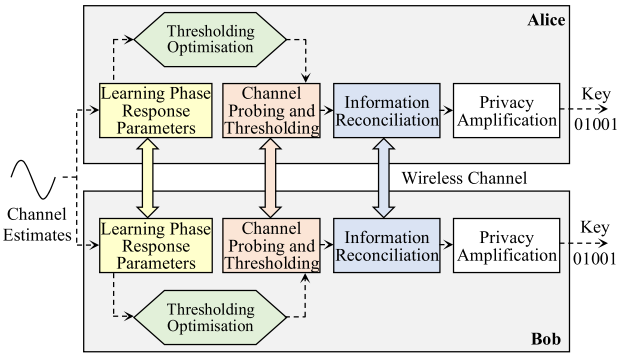
$$\begin{aligned} \mu_{\xi,i} &= \frac{1}{m}\sum_{x=1}^{m}\left(\widehat{\xi}_{a(b)}^{t_{a(b)}}(f_i)\right), \\ var_{\xi,i} &= \frac{1}{m-1}\sum_{x=1}^{m}\left(\widehat{\xi}_{a(b)}^{t_{a(b)}}(f_i) - \mu_{\xi,i}\right)^2 \end{aligned} \tag{9}$$

where m equals 100 probe packets, as recommended in [38]. By learning and doubling the estimated variance in (9), both terminals can learn the variance of $\angle e_{a(b)}(t)$'s distribution $2\sigma^2$ and agree on the quantisation order r. This method acts as a forward indicator for the channel probing and thresholding stage, see Fig. 5(a). Note that the quantisation region $2\pi/2^r$ is large for a large value of $var_{\xi,i}$, and vice versa for a small value, see Fig. 5(b).

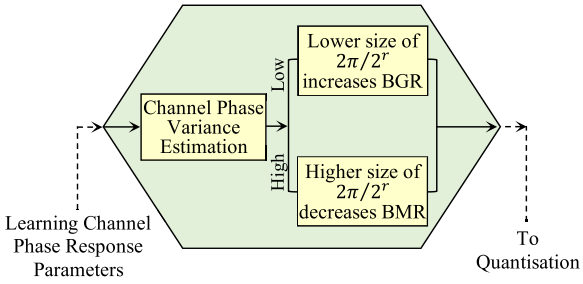
Finally, the extracted key will be used for the PHY-layer re-authentication process discussed in the following subsection.

4.2. PHY-layer re-authentication algorithm

In the first transmission slot, mutual identity authentication between the communicating terminals is performed using conventional signature-based algorithms implemented at the upper layers of the protocols stack. This facilitates legitimacy detection, as well as the exchange of authenticated Chebyshev probing sequences used to extract the symmetric shared key k. This key allows for re-authenticating the received messages sent from the same transmitter for the OFDM system of N subcarriers. This study extends our research introduced in [39]. In a two-step process, the identity of the corresponding terminal is re-authenticated



(a) Flowchart of the secret key extraction algorithm.



(b) Flowchart of the optimisation engine.

Fig. 5. Modelling of the key extraction algorithm.

using a PHY-layer signature-based identity authentication mechanism (PHY-SIAM), while the integrity of the attached data packet is verified using a PHY-layer feature tracking mechanism (PHY-FTM). In this study, we only assumed that the subcarriers are well separated to ensure independent fading. Fig. 6 depicts the structure of M OFDM symbols for $N = 64$ subcarriers in which $N/4$, and $3N/4$ subcarriers are used for channel probing and zero-padding, and signature/data transmission, respectively. The detailed steps are as follows.

1. *PHY-layer signature-based identity authentication mechanism* (*PHY-SIAM*): In this part, and after mutual identity verification, the receiver checks the sender's identity based on the extracted key k. This key is divided into two subkeys, k_a and k_b, with equal lengths, which are used to generate the PHY-layer signature of the attached data. The created signature is transmitted from the vehicle V_i to the RSU R_j within the same region along with its related data, as demonstrated in Fig. 7. In general, PHY-SIAM consists of three primary phases, i.e., initialisation, signature generation, and message verification.
   (a) *System initialisation*: In this phase, TA generates the PHY-layer public parameters and preloads them into all registered network terminals. Accordingly, the system is initially configured as follows.
   - Mapping operation: A Gray coded 2-bits mapping function is used to map the input variable $K = \{\kappa_1\kappa_2, \ldots, \kappa_{(3N/2)-1}\kappa_{3N/2}\}$ to ϕ, such that $\mathcal{M}(K) \rightarrow \phi$ is designed as

$$\phi_i = \mathcal{M}(K_i) = \begin{cases} 0 & K_i = [00] \\ \frac{\pi}{2} & K_i = [01] \\ \pi & K_i = [11] \\ \frac{3\pi}{2} & K_i = [10] \end{cases} \tag{10}$$

   for i=1, …, $3N/4$.
   - Secure hash function H_1: $\{0,1\}^* \rightarrow \{0,1\}^{3N/2}$.
   - Finally, the tuple $\langle H_1, \mathcal{M}(.)\rangle$ is preloaded into the network terminals during the registration.

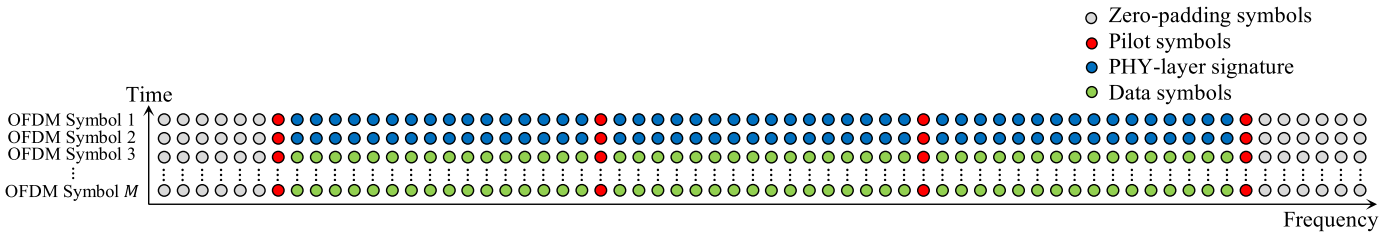


Fig. 6. Symbols structure for OFDM system of 64 subcarriers.

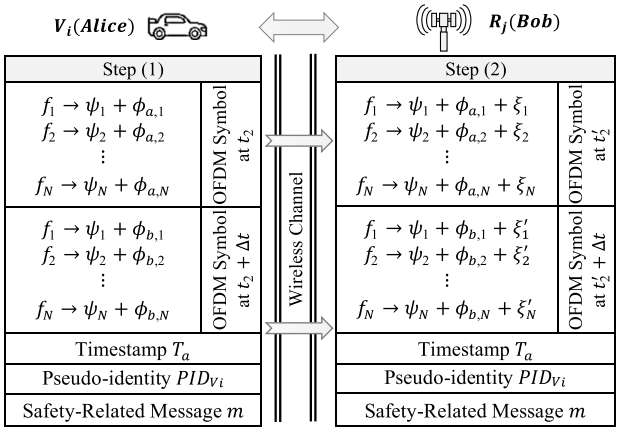


Fig. 7. The PHY-layer identity re-authentication mechanism in a noiseless channel.

(b) *Signature generation*: In this phase, each safety-related message m is attached with the sender's pseudo-identity PID_{V_i}, timestamp T_a, and two OFDM symbols. These symbols are collectively referred to as the PHY layer signature, which is generated in a two-stage process as follows.

- *Signature preparation*: In this stage, k_a is concatenated with the attached timestamp T_a, hashed, and mapped to obtain ϕ_a of the first OFDM symbol. T_a is defined here as a "nonce." Similarly, ϕ_b is obtained by using k_b for the second OFDM symbol. The following are the formulation of the mapping operations ϕ_a and ϕ_b.

$$\begin{aligned} \phi_a &= \mathcal{M}\left(H_1\left(k_a \| T_a\right)\right), \\ \phi_b &= \mathcal{M}\left(H_1\left(k_b \| T_a\right)\right) \end{aligned} \tag{11}$$

- *Signature generation*: In this stage, the mapped signatures are masked by uniformly distributed random phases $\psi_i \sim U[0, 2\pi)$ for $i = 1, \ldots, N$ with probability density function (PDF) $1/2\pi$. Afterwards, Alice initiates two subsequent signals, $s_a(t_2)$ and $s_a(t_2 + \Delta t)$, with time difference Δt less than the coherence time T_c, and frequencies $f_1, \ldots, f_N$. Then, Alice sends them to Bob in the form of

$$\begin{aligned} s_a(t_2) &= \sum_{i=1}^{N} \sqrt{\frac{2E_s}{T}} e^{j(\psi_i + \phi_{a,i})} \\ s_a(t_2 + \Delta t) &= \sum_{i=1}^{N} \sqrt{\frac{2E_s}{T}} e^{j(\psi_i + \phi_{b,i})} \end{aligned} \tag{12}$$

so that the received signals by Bob are denoted by

$$\begin{aligned} r_b\left(t_2'\right) &= \sum_{i=1}^{N} \sqrt{\frac{2\left|h_i\right|^2 E_s}{T}} e^{j\left(\psi_i + \phi_{a,i} + \xi_i\right)} + N_i \\ r_b\left(t_2' + \Delta t\right) &= \sum_{i=1}^{N} \sqrt{\frac{2\left|h_i\right|^2 E_s}{T}} e^{j\left(\psi_i + \phi_{b,i} + \xi_i'\right)} + N_i' \end{aligned} \tag{13}$$

- *Message verification*: In this stage, avoiding replaying attacks, Bob verifies the validity of the attached timestamp T_a by checking if $T_r - T_a \leq T_\Delta$ holds or not. If holds, the received OFDM symbols are verified to avoid impersonation attacks using the symmetric key k and the attached timestamp T_a. In a similar way to (11), Bob computes the mapped signatures ϕ_a' and ϕ_b', and calculates $r_b'\left(t_2'\right) = r_b\left(t_2'\right) e^{-j\phi_a'}$ and $r_b'\left(t_2' + \Delta t\right) = r_b\left(t_2' + \Delta t\right) e^{-j\phi_b'}$. Note that ξ_i and ξ_i' in (13) are highly correlated for $\Delta t \leq T_c$. Thus, Bob verifies the sender's identity by computing the circular variance $c.var(.)$ of $\angle c(t) = r_b'\left(t_2'\right) r_b'\left(t_2' + \Delta t\right)^*$ as

$$v = c.var\left(\sum_{i=1}^{N} \arctan\left(\frac{Im\left(c_i(t)\right)}{Re\left(c_i(t)\right)}\right)\right) \tag{14}$$

where the circular variance [40] $c.var(.)$ is given by

$$\begin{aligned} \alpha_i &= \begin{pmatrix} \cos\left(\angle\left(c_i\right)\right) \\ \sin\left(\angle\left(c_i\right)\right) \end{pmatrix}, \bar{\alpha} = \frac{1}{N} \sum_{i=1}^{N} \alpha_i, \\ v &= 1 - \|\bar{\alpha}\| \end{aligned} \tag{15}$$

where $\|.\|$ is the norm function. Suppose an impersonator, Eve, is attempting to masquerade as Bob. In this case, Eve uses a different key k_e to initiate a PHY layer signature, which is considered as a hypothesis testing problem, given that

$$\begin{matrix} H_0 \\ v \lessgtr \tau_1, \text{ for} \\ H_1 \end{matrix} \begin{cases} H_0: & \phi_a' = \phi_a \ \& \ \phi_b' = \phi_b \\ H_1: & \phi_a' \neq \phi_a \ \& \ \phi_b' \neq \phi_b \end{cases} \tag{16}$$

2. *PHY-layer feature tracking mechanism* (*PHY-FTM*): After verifying the sender's identity, the recipient can verify the integrity of the received message in order to avoid modification attacks. In this context, Bob employs the received probe symbols of the i^{th} subcarrier in the j^{th} OFDM symbol for channel estimation, where $j = 1, \ldots, M$ data symbols. The channel observations vector $\bar{H}_j$ of the j^{th} OFDM symbol consists of all the channel estimates obtained from the i^{th} subcarriers that hold probe symbols (i.e., subcarriers highlighted in red in Fig. 6). To determine whether the received data is sent from the same source, the recipient compares the channel observation vector of the j^{th} symbol with that of the $(j-1)^{th}$ symbol, starting from the PHY-layer signature at $j = \{1, 2\}$ to the M^{th} OFDM data symbol. In this study, the channel estimation is performed using

the iterative least square (ILS) [41] as well as the minimum mean-square error (MMSE) [42] methods. The integrity verification process can be characterised as a hypothesis testing problem in which H_0 indicates that all data packets are transmitted from the sender whose identity is verified using the proposed PHY-SIAM, otherwise H_1. The hypothesis testing of the normalised likelihood ratio test (LRT) can be represented as

$$\Lambda_{LRT} = \frac{n_{\tau_2} \left\| \bar{H}_j - \bar{H}_{j-1} \right\|^2}{\left\| \bar{H}_{j-1} \right\|^2}, \text{ for } j = 2, \ldots, M$$
$$\Lambda_{LRT} \underset{H_0}{\overset{H_1}{\lessgtr}} \tau_2 \tag{17}$$

where n_{τ_2} is the normalisation coefficient that makes the threshold value $\tau_2 \in [0, 1]$. While the hypothesis testing of the sequential probability ratio test (SPRT) [43] is formulated as

$$\Lambda_j = \frac{n_{\tau_2} \left\| \bar{H}_{M-j+1} - \bar{H}_{M-j} \right\|^2}{\left\| \bar{H}_{M-j} \right\|^2} \text{ for } j = 1, \ldots, M-1,$$
$$\Lambda_{SPRT} = n_{\tau_3} \sum_{j=2}^{M} \Lambda_j, \Lambda_{SPRT} \underset{H_0}{\overset{H_1}{\lessgtr}} \tau_3 \tag{18}$$

where n_{τ_3} is the normalisation coefficient that makes the threshold value $\tau_3 \in [0, 1]$. In SPRT-based hypothesis testing, the sum of the LRTs between the j^{th} and $(j-1)^{th}$ symbols $\forall j \in [2, M]$ is compared with the threshold value τ_3 to make the decision rule, which can improve the detection rate compared to the simple LRT.

5. Performance evaluation and threat modelling

This section presents the theoretical analysis of the key extraction and re-authentication processes and then discusses in depth the security strength of the re-authentication algorithm.

5.1. Theoretical analysis of the key extraction algorithm

In order to evaluate the key extraction performance, it is necessary to calculate the probability of error/mismatching P_e. In this context and since the distribution of the equalised phase $\angle e_{a(b)}(t)$ in (6) is normally distributed $\mathcal{N}(T'_{n_i(m_i)}(\theta_i) = n_i(m_i)\theta_i, 2\sigma^2)$ at negligible $\varepsilon_{a(b),i}$, the cumulative distribution function (CDF) $\phi(.)$ can be formulated as

$$\phi(x) = \frac{1}{2}\left[1 + \text{erf}\left(\frac{x - T'_{n_i(m_i)}(\theta_i)}{2\sigma}\right)\right] \tag{19}$$

where the error function is given by $\text{erf}(z) = \frac{2}{\sqrt{\pi}} \int_0^z e^{-t^2} dt$. Thus, P_e is the probability that $\angle e_{a(b)}(t) \notin [T'_{n_i(m_i)}(\theta_i) - \pi/2^r, T'_{n_i(m_i)}(\theta_i) + \pi/2^r)$, which makes the output of the *Round* (.) function in (7) doesn't equal $T'_{n_i(m_i)}(\theta_i)$, i.e., $\hat{T}'_{n_i(m_i)}(\theta_i) \neq T'_{n_i(m_i)}(\theta_i)$. Finally, P_e is given by

$$P_e = 2\phi\left(T'_{n_i(m_i)}(\theta_i) - \frac{\pi}{2^r}\right), r \in \{1, 2, 3\} \tag{20}$$

For an acceptable probability of error less than or equal to the scalar value a_1, r can be calculated by both terminals to optimise the size of the thresholding region $2\pi/2^r$ based on the estimated learned parameter $var_\xi = \sigma^2$ in (9) as

$$x = \arg\max_{x'} \text{erf}\left(\frac{x' - T'_{n_i(m_i)}(\theta_i)}{2\sigma}\right) \leq a_1 - 1 \tag{21}$$

Given x, r can be obtained as

$$r = \arg\max_{r'} 2^{r'} \leq \frac{\pi}{x} \quad \text{for } r' = 1, 2, 3 \tag{22}$$

5.2. Detection vs. false alarm probabilities of re-authentication

As part of the performance evaluation, it is important to examine the receiver operating characteristics (ROC) of the identity verification process. ROC is a measurement of the detection probability P_d at different values of false alarm probabilities P_{fa}. To determine the ROC, the probability density function must be investigated. The estimated differential baseband signal $c_i = r'_b(t'_2)\, r'_b(t'_2 + \Delta t)^*$ of the i^{th} subcarrier can be simplified as

$$c_i = 2h_i h_i^* E e^{j(\varepsilon_{e,i})} + h_i^* N_i + h_i N'_i = X + jY \tag{23}$$

where $\mathcal{E}_{e,i} = \mathcal{E}_{a,i} - \mathcal{E}_{b,i}$ for $\mathcal{E}_{a,i} = \phi_{a,i} - \phi'_{a,i}$ and $\mathcal{E}_{b,i} = \phi_{b,i} - \phi'_{b,i}$ and $h_i = |h_i| e^{j\xi_i}$. Considering Alice is communicating with Bob (i.e., H_0), which makes $\mathcal{E}_{e,i}$ equals zero, so that the real and imaginary parts of (23) can be formulated as

$$X = 2|h_i|^2 E + Re\left(h_i^* N_i + h_i N'_i\right),$$
$$Y = Im\left(h_i^* N_i + h_i N'_i\right) \tag{24}$$

where the expectation $E(X) = 2|h_i|^2 E = \mu$ and $E(Y) = 0$ while the variance $var(X) = var(Y) = 4EN_0 h_i^2 \cong \sigma_0^2$. Similar to [44], the joint probability density function of X and Y can be expressed as

$$P\left(x,\, y|_{H_0}\right) = \frac{1}{2\pi\sigma_0^2} e^{\frac{-\left[(x-\mu)^2 + y^2\right]}{2\sigma_0^2}} \tag{25}$$

By changing the variables $R = \sqrt{x^2 + y^2}$ and $\Theta = \arctan(y/x)$. The joint probability density function of (25) yields to

$$P\left(R,\, \Theta|_{H_0}\right) = \frac{R}{2\pi\sigma_0^2} e^{\frac{\left[2\mu R\cos\Theta - R^2 - \mu^2\right]}{2\sigma_0^2}} \tag{26}$$

By integrating (26) over $R \in [0, \infty)$, (26) can be simplified as

$$P(\Theta \mid \Gamma) = \frac{1}{2\pi} e^{-\Gamma} + \frac{1}{\sqrt{\pi}} (\sqrt{\Gamma}\cos\Theta) \cdot e^{-\Gamma \sin^2\Theta} [1 - \mathbb{Q}(\sqrt{2\Gamma}\cos\Theta)] \tag{27}$$

where

$$\Gamma = \frac{h_i^2}{2} \cdot \frac{E_S}{N_0},$$
$$\mathbb{Q}(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt \tag{28}$$

Fig. 8 shows $P(\Theta)|_{H_0}$ parametrized by different Γ values. It can be observed that increasing Γ value decreases the variance of $P(\Theta)$, and vice versa. Since v in (14) represents the variance of a restricted number of N subcarriers, its distribution is normally with mean equals to the variance of $P(\Theta \mid \Gamma)$ and variance depends on the N value used to estimate v in (14), following the central limit theorem. Thus v's normal distribution for both hypotheses $H_{0,1}$ is represented by mean $\mu_{H_{0,1}} \cong E\left(v \mid H_{0,1}\right)$ and variance $\sigma^2_{H_{0,1}} \cong var\left(v \mid H_{0,1}\right)$, which can be formulated as

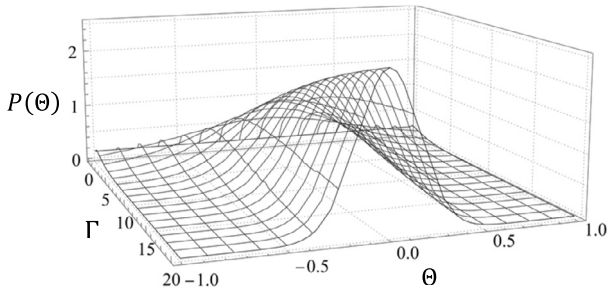


Fig. 8. The $P(\Theta)|_{H_0}$ parametrized by different Γ values.

$$\mathcal{F}\left(x \mid \mu_{H_i}, \sigma^2_{H_i}\right) = \frac{1}{\sqrt{2\pi\sigma^2_{H_i}}} e^{-\left(x-\mu_{H_i}\right)^2/2\sigma^2_{H_i}}, i = 0, 1 \tag{29}$$

with CDF equals

$$\phi\left(x \mid \mu_{H_i}, \sigma^2_{H_i}\right) = \frac{1}{2}\left[1 + \text{erf}\left(\frac{x-\mu_{H_i}}{\sqrt{2\sigma^2_{H_i}}}\right)\right], i = 0, 1 \tag{30}$$

In this study, we refer to the acceptable performance of re-authentication as the successful probability of detection $\phi(x \mid \mu_{H_0}, \sigma^2_{H_0})\Big|_{x=\tau_1}$ for an acceptable false alarm $\phi(x \mid \mu_{H_1}, \sigma^2_{H_1})\Big|_{x=\tau_1}$ less than or equal to the scalar value a_2. Thus, the threshold value τ_1 is obtained as

$$\tau_1 = \arg\max_{\tau_1'} \text{erf}\left(\frac{\tau_1' - \mu_{H_1}}{\sqrt{2\sigma^2_{H_1}}}\right) \leq 2a_2 - 1 \tag{31}$$

5.3. Security analysis of the re-authentication algorithm

As a part of this section, the security strength is evaluated against passive and active attacks. Consider Eve as a passive attacker who eavesdrops on the broadcasted messages and their associated PHY-layer signatures. In this case, there is no way for Eve to derive the symmetric key k from the message contents for two primary reasons: 1) By considering the signature generation stage as a single cryptographic process $C(.)$ with input $I(k, T_a, \psi_i, \xi_i)$ and output $O \leftarrow C(I)$; $C(.)$ depends on the current timestamp T_a, which denotes different output O given the same input variables (k, ψ_i, ξ_i); $C(.)$ depends on the randomly varying ψ_i, which masks the phase response ξ_i and the mapped signatures $\phi_{a(b)}$ thus Eve cannot differentiate between $\phi_{a(b)}, \psi_i$, and ξ_i. 2) For $y \leftarrow H_1(x)$, it is hard for Eve to deduce the input variable $x : \{0, 1\}^*$ given the hashed variable $y : \{0, 1\}^{3N/2}$. Therefore, Eve is considered an active attacker who can impersonate a legitimate terminal, replay a previously captured message, or alter message contents.

1. *Impersonation attacks*: In this attack, Eve tries to impersonate Alice by creating a valid PHY-layer signature. In this case, and since she is unaware of the symmetric key k, she cannot succeed under the challenge of forging Alice's signatures because of the reasons mentioned above that make such an attack easily detected.
2. *Replaying attacks*: In this attack, Eve captures the message created by Alice at time t and retransmits it after a period of time. However, each received message is checked for freshness using the attached timestamp T_a by verifying if $T_r - T_a \leq T_\Delta$ holds. Hence, providing immunity from replay attacks.
3. *Modification attacks*: In this attack, Eve attempts to alter the data packets. However, the integrity of the received messages is verified using the proposed feature tracking algorithm. In case of Eve is trying to alter only the subcarriers that hold the safety-related message m without any modification in the received probe symbols and the PHY-layer signature and retransmits the altered message at time $T_a + \Delta T_a$. In this scenario and if and only if $T_r - T_a \leq T_\Delta$, Eve can deceive the feature tracking mechanism at the side of Bob as the channel estimation vectors $\tilde{H}_j$, for $j = 1, \ldots, M$, will be highly correlated as all the probe symbols have the same channel response from Alice to Bob passing through Eve. However, the accumulated noises significantly increase the value of the estimated variance v in (14), thereby failing to pass the hypothesis test in (16), accordingly, the received message will be discarded. Thus, providing immunity against modification attacks.

6. Simulation and hardware implementation

This section presents the simulation of the key extraction and then describes the Doppler shift emulation employed for the hardware implementation of the re-authentication process.

6.1. Simulation analysis of the key extraction algorithm

During the tests, Monte-Carlo simulations are conducted of 100,000 runs to evaluate the key extraction performance. We created a Rayleigh environment suitable for modelling urban areas by using the generic stochastic vehicular channel modelled in [45] with $L = 16$ multipath components. Since the DSRC protocol operates within the range of 5.85 to 5.925 GHz [2], the carrier frequency f_c is set at 5.85 GHz. The parameters of the simulated channel are listed in Table 2. According to [46], the scatterers' speeds follow the Weibull distribution with shape ζ and scale ρ. Tx/scatterer speeds are set to 30 m/s. In this study, the extraction performance is defined as the achievable SBGR for an acceptable BMR $\leq a_1$, for $a_1 = 0.1$. In Fig. 9, the extraction performance is plotted at different SNR and r values. It can be noted that the highest SBGR is obtained for an acceptable BMR at the thresholding region of order 3 and SNR ≥ 22 dB. For $16 \leq$ SNR ≤ 22, $r = 2$ is evidently the optimum choice for an acceptable performance within this range. While $r = 1$ is clearly the unique acceptable quantisation order at $7 \leq$ SNR ≤ 16. In Fig. 10, the simulation analyses of the CDFs $\phi(T'_{n_i(m_i)}(\theta_i) + x)\,|_{T'_{n_i(m_i)}(\theta_i)=0}$, for $r = 1, 2, 3$, are compared to its theoretical formulation in (19) across different SNRs. The results show that there exists an optimal quantisation order r across different ranges of SNRs. By adjusting the r value to different SNR conditions, the extraction performance can be optimised for an acceptable P_e formulated in (20).

What's more, the extracted bitstreams are checked for any statistical defects by using the well-known randomness test suite developed by the National Institute of Standards and Technology (NIST) [47]. By doing so, each test returns a P-value, as shown in Table 3. This value is compared to the significance level (0.01) to determine whether the extracted bitstreams have successfully passed the test. It can be noted that the extracted keys have sufficient randomness, as their chaotic characteristics are mostly determined by the randomly selected users' secret parameters n_i and m_i of the Chebyshev mapping operation in (3).

6.2. Hardware implementation and Doppler shift emulation

In a realistic V2I scenario, measuring the ROCs at different Tx speeds of a moving vehicle is a challenging issue for performance evaluation due to the speeds' instability of the transmitter at different distances from the receiver, resulting in an unstable and inaccurate measurement of the detection probabilities. Therefore, we

Table 2
Channel Simulation Settings.

Description	Value
The number of multipath components L	16
Maximum speed of the Tx	30 m/s
Maximum speed of the Rx (for V2I scenario)	0 m/s
Maximum speed of the scatterers	30 m/s
Azimuth angles of departure (arrival) $\alpha_{A(B),l}$	$U[-\pi, \pi)$
Elevation angles of departure (arrival) $\beta_{A(B),l}$	$U[0, \pi/3)$
Scatterers' angles of incident/departure $\alpha_{1(2),l}$	$U[-\pi, \pi)$
The Weibull distribution's scale coefficient ρ	2.985
The Weibull distribution's shape coefficient ζ	0.428
Carrier frequency f_c	5.85 GHz

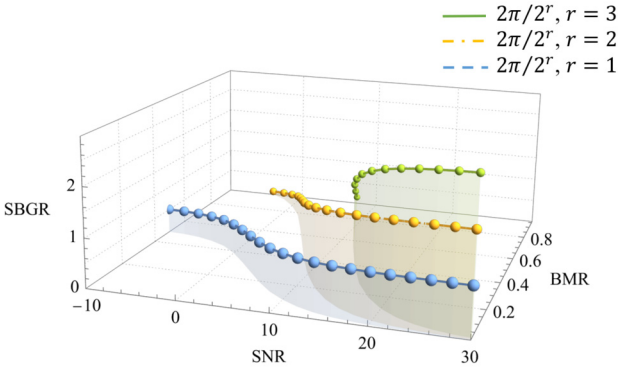


Fig. 9. Key extraction performance at different r values.

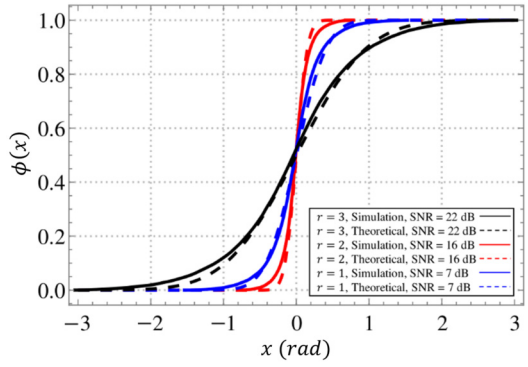


Fig. 10. $\phi\left(T'_{n_i(m_i)}(\theta_i)+x\right)|_{T'_{n_i(m_i)}(\theta_i)=0}$ at different SNRs.

Table 3
Randomness Evaluation of the Extracted Keys.

NIST Statistical Test Suite (128 bits)	P-value
Block Frequency Test	0.486427
Long Runs Test	0.487804
Monobit Test	0.58592
Key Entropy	0.300445
Maurer Universal Statistical Test	0.163067
Discrete Fourier Transform (Spectral) Test	0.495118
Overlapping Template Matchings Test	0.486427

evaluated the re-authentication performance using the two channels of the ETTUS-Universal Software Radio Peripheral (USRP) X310 device as separate Tx/Rx terminals and the LabView as a software-defined radio. The evaluation is conducted in a real vehicular wireless channel by setting a fixed distance (5 meters) between the Tx

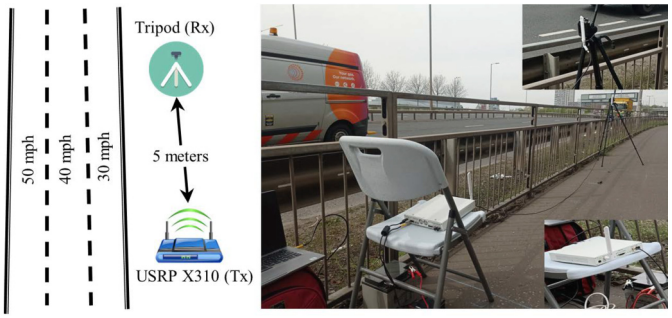


Fig. 11. Experimental settings for performance evaluation.

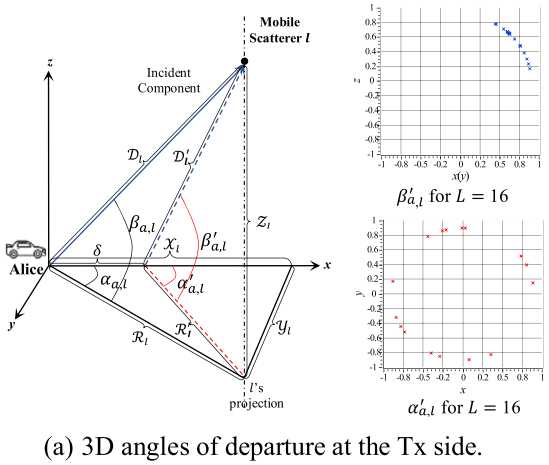


Fig. 12. 3D V2V departure angles of the l^{th} scatterer.

and Rx antennas, as shown in Fig. 11, and varying the power of the added complex Gaussian noise at the side of the Rx (i.e., different SNRs). This subsection presents a solution for a realistic Doppler emulation. By simulating the Doppler components of a moving vehicle at the Tx side, we successfully investigated the ROCs of the re-authentication process at different speeds for the OFDM communication system. Fig. 12(a) and 12(b) show the 3D azimuth and elevation angles of departure $\alpha_{a,l}(t_2) \sim U[-\pi, \pi)$ and $\beta_{a,l}(t_2) \sim U[0, \pi/3)$ for the l^{th} multipath component of the j^{th} OFDM symbol at the Tx side. It can be noted from the same figure that the upcoming $\alpha'_{a,l}(t_2 + \Delta t)$ and $\beta'_{a,l}(t_2 + \Delta t)$ of the $(j+1)^{th}$ symbol depends on the speed of the transmitter u_a and the transmission time Δt between the j^{th} and $(j+1)^{th}$ symbols. The distance δ (meter) driven by the Tx can be obtained as

$$\delta = u_a \times \Delta t \tag{32}$$

In urban areas, it is assumed that the direct distance $\mathcal{D}_l$ between the transmitter Tx and the scatterer l with coordinates $\{\mathcal{X}_l, \mathcal{Y}_l, \mathcal{Z}_l\}$ is a uniformly distributed random variable within few meters from the transmitter $\mathcal{D}_l \sim U[1, 3]$ since most of the received power at the Rx side is coming from the multipath components with short distances, referred to as specular components

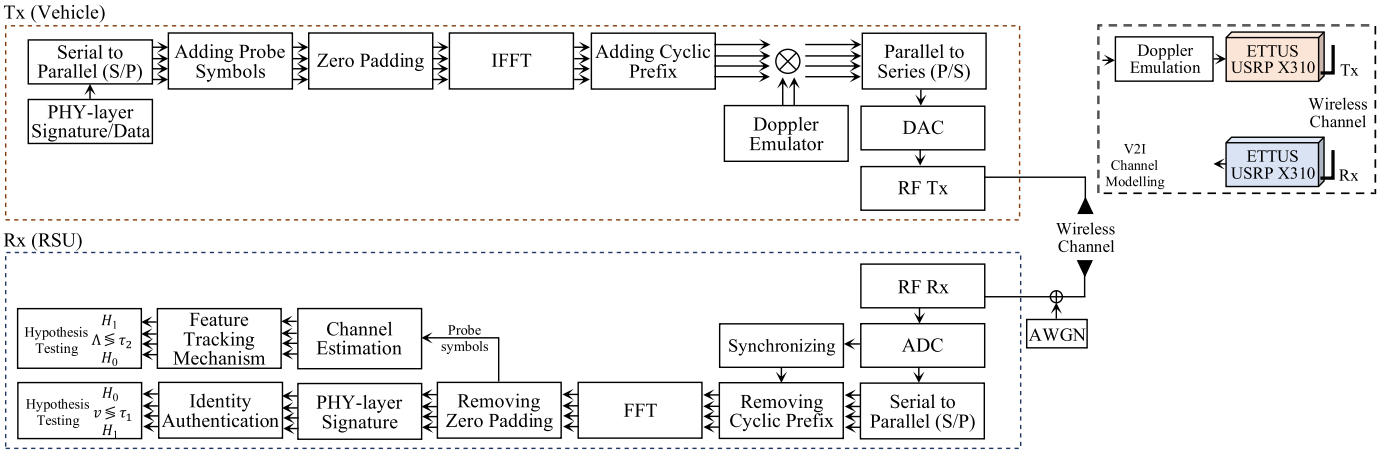


Fig. 13. OFDM Tx/Rx block diagram.

[45]. In this scenario, the upcoming azimuth angle $\alpha'_{a,l}$ of the l^{th} multipath component can be formulated using trigonometric as

$$\alpha'_{a,l} = \arctan\left(\frac{\mathcal{D}_l \cos\left(\beta_{a,l}\right)\sin\left(\alpha_{a,l}\right)}{\mathcal{D}_l \cos\left(\beta_{a,l}\right)\cos\left(\alpha_{a,l}\right) - \delta}\right) \tag{33}$$

By dividing the range of the azimuth angle (2π) into a number of r_l step angles $\Delta_l(\text{rad}) = \left|\alpha'_{a,l} - \alpha_{a,l}\right|$, as shown in Fig. 12(c). In this case, the resolution value r_l of the l^{th} scatterer can be approximated by

$$r_l = \left\lfloor \frac{2\pi}{\left|\alpha'_{a,l} - \alpha_{a,l}\right|} \right\rfloor \tag{34}$$

so that the azimuth angle of the j^{th} OFDM symbol equals $\alpha'_{a,l}(j) = \alpha_{a,l} + (j-1)\Delta_l$ for $j = 1, \ldots, M$. While the elevation angle $\beta'_{a,l}(j)$ is approximated using trigonometric by

$$\beta'_{a,l}(j) = \left|\arctan\left(\frac{\sin(\beta_{a,l})\sin\left(\alpha'_{a,l}(j)\right)}{\cos\left(\beta_{a,l}\right)\sin\left(\alpha_{a,l}\right)}\right)\right| \tag{35}$$

Then, the Doppler shift at the Tx side can be expressed as

$$v_{a,l} = u_a \frac{f_c}{c}\cos\left(\alpha'_{a,l}(j)\right)\cos\left(\beta'_{a,l}(j)\right) \tag{36}$$

where c is the speed of light. Eventually, the l^{th} Doppler multipath component can be approximated by

$$d_{a,l}(t) = e^{j2\pi v_{a,l} t} \tag{37}$$

The Doppler emulation steps at the Tx side can be summarised in the algorithmic form as shown in Algorithm 1. By creating $L = 16$ Doppler components at the Tx side, and convoluting them with the generated symbols before transmitting through the USRP, as shown in Fig. 13, we can determine how the speed of the transmitter affects the re-authentication performance.

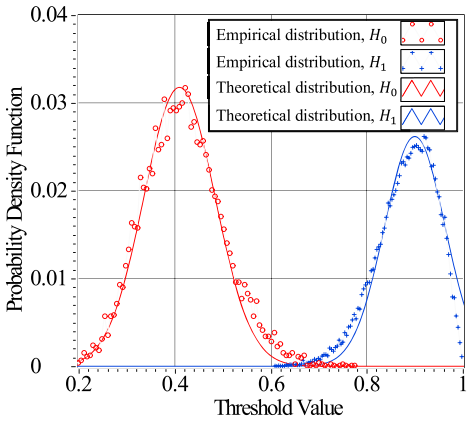
6.3. Hardware implementation results

Experimentally, we set f_c to 5.85 GHz and the sampling rate to 1 MHz. It is vital to examine the effect of the distance between the Tx and Rx antennas by comparing different SNRs independently from the Tx speed. Fig. 14(a) shows the empirical PDFs of the identity authentication mechanism for both hypotheses $H_{0,1}$ in comparison to their theoretical Gaussian distribution $\mathcal{F}(x)\,|_{H_{0,1}}$ in (29) at SNR = 5 dB, N = 64 subcarriers, and Tx speed u_a = 30 m/s. Based on the results, the theoretical and empirical Gaussian distributions are well-matched, and both hypotheses are well-separated, allowing for an easy determination of the threshold value τ_1. In the same settings, Fig. 14(b) compares the empirical LRT with the SPRT-Rician distribution of the feature tracking mechanism for the H_0 hypothesis.

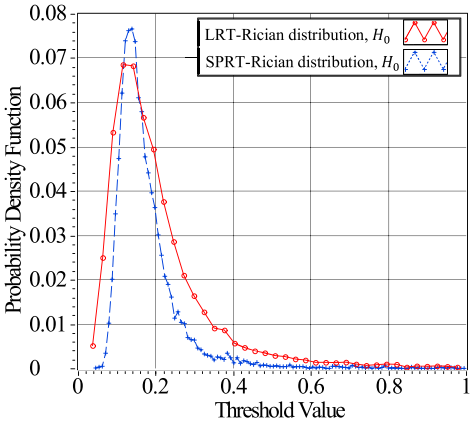
Algorithm 1 Doppler Shift Emulation

Require
Adjust the speed of the Tx $u_a \geq 0$ m/s
Adjust the transmission time interval $\Delta t = 16$ µs
Adjust the value of L to 16 multipath components
Calculate the horizontal distance $\delta = u_a \times \Delta t$
for $j = 1 : M$ **do**
  for $l = 1 : L$ **do**
    Select the Tx azimuth angle $\alpha_{a,l} \leftarrow U[-\pi, \pi)$
    Select the Tx elevation angle $\beta_{a,l} \leftarrow U[0, \pi/3)$
    Select the direct distance $\mathcal{D}_l \leftarrow U[1, 3]$
    Calculate the upcoming azimuth angle $\alpha'_{a,l}$ using (33)
    Calculate the step angle $\Delta_l(\text{rad}) = \left|\alpha'_{a,l} - \alpha_{a,l}\right|$
    Get the j^{th} azimuth angle $\alpha'_{a,l}(j) = \alpha_{a,l} + (j-1)\Delta_l$
    Get the j^{th} elevation angle $\beta'_{a,l}(j)$ using (35)
    Using $\alpha'_{a,l}(j)$ and $\beta'_{a,l}(j)$ of the j^{th} OFDM symbol
    Calculate $v_{a,l}$ using (36)
  Return the Doppler component $d_{a,l}$ using (37)
  end for
end for

Fig. 14(b) illustrates two important observations: 1) The distribution is Rician due to the direct line-of-sight path between the Tx and Rx antennas; 2) The variance of the SPRT-distribution is smaller than that of the LRT since the SPRT is considered to be a LRT for a plurality of M OFDM symbols, indicating better performance than the LRT. In Fig. 15(a), the ROC curves are plotted at SNR = [10, 5, 0, -2] dB, N = 64 subcarriers, and u_a = 30 m/s. It can be seen that the proposed mechanism for identity authentication offers acceptable performance ($P_{fa} \leq 0.1$) at SNR $\geq$ 0 dB. In addition, we investigated the ROCs at different Tx speeds u_a = [30, 35, 40, 45, 50] m/s and SNR = 5 dB, see Fig. 15(b). In test settings up to 45 m/s, it is proven that PHY-SIAM exhibits high authentication performance. Further, we identified the ROCs at N = [64, 128, 256] subcarriers, u_a = 30 m/s, and SNR = -2 dB, as shown in Fig. 15(c). As can be seen in the figure, increasing the number of subcarriers results in enhanced ROC since PDFs follow the central limit theorem. Therefore, the more subcarriers, the smaller the variance $var(v \mid H_{0,1})$ of the Gaussian distribution of v in (29), which, in



(a) PDFs for hypothesis testing of the PHY-SIAM.



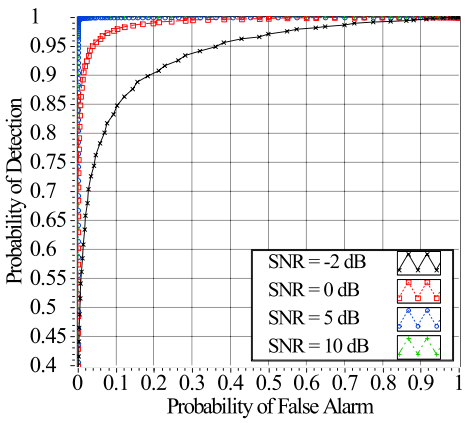
(b) PDFs for hypothesis testing of the PHY-FTM.

Fig. 14. PDFs for both hypotheses of the re-authentication process at 64 subcarriers, u_a = 30 m/s, and SNR = 5 dB.

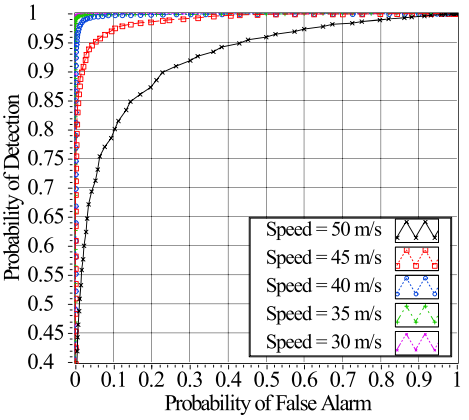
turn, leads to reduced overlapping between the two hypotheses, thereby improving the authentication performance.

7. Conclusions

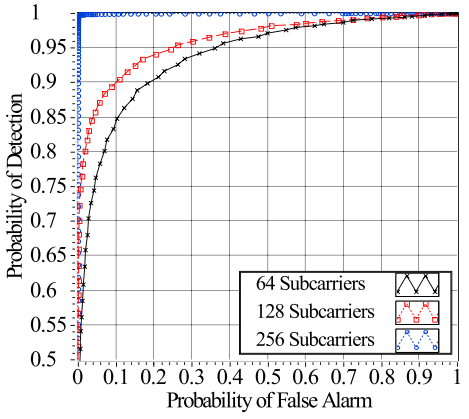
This study proposes a novel, efficient, and secure cross-layer authentication scheme that supports forward and backward secrecy in VANETs. Our work demonstrates that by using the cryptographic features of the Chebyshev mapping in combination with the physical-layer properties, it is possible to obtain high entropy secret bitstreams, not only applicable for V2V but also for V2I. With the proposed key extraction technique, the tradeoff relation between BMR and BGR is optimised for optimal performance in any wireless propagation conditions, moving beyond the current state-of-the-art in achieving SBGR $\simeq$ 0.85 $\sim$ 2.76 bits/packet at SNR of 7 $\sim$ 22 dB. By leveraging the existing PHY-layer authentication techniques, we introduce PHY-SIAM and PHY-FTM, two PHY-layer re-authentication mechanisms that we use for identity and integrity verification, respectively, mitigating the considerable costs of traditional cryptographic techniques. Besides theoretical analysis, an efficient Doppler emulator is developed to experimentally investigate the re-authentication performance of a realistic vehicular wireless channel at different speeds and SNRs of a V2I scenario. Experimental measurements demonstrate the effectiveness of the re-authentication algorithm in providing high detection at low false alarm probabilities ($P_{fa} \leq 0.1$) for SNR $\geq$ 0 dB and Tx speed $\leq$ 45 m/s. Our current research activities aim at exploring the use of the number theory in the process of key extraction and



(a) ROCs at different SNRs for $u_a = 30$ m/s and $N = 64$.



(b) ROCs at different speeds for SNR = 5 dB and $N = 64$.



(c) ROCs at different N for $u_a = 30$ m/s and SNR = -2 dB.

Fig. 15. ROCs of the PHY-SIAM at different parameters for a fixed distance (5 m) between the Tx and Rx.

authentication at the PHY-layer, addressing potential performance limitations in VANETs.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgements

This work was supported by the Egyptian Ministry of Defence.

References

[1] Toor, P. Muhlethaler, A. Laouiti, Vehicle ad hoc networks: applications and related technical issues, IEEE Commun. Surv. Tutor. 10 (3) (2008, July) 74–88.
[2] J.B. Kenney, Dedicated short-range communications (DSRC) standards in the United States, Proc. IEEE 99 (2011, July) 1162–1182.
[3] Hyunseo Oh, C. Yae, D. Ahn, H. Cho, 5.8 GHz DSRC packet communication system for ITS services, in: Gateway to 21st Century Communications Village, IEEE VTS 50th Vehicular Technology Conference, vol. 4, 1999, September, pp. 2223–2227.
[4] J.T. Isaac, S. Zeadally, J.S. Camara, Security attacks and solutions for vehicular ad hoc networks, IET Commun. 4 (7) (2010, April) 894–903.
[5] M.B. Mansour, C. Salama, H.K. Mohamed, S.A. Hammad, VANET security and privacy–an overview, Int. J. Netw. Secur. Appl. 10 (2) (2018, March).
[6] M. Raya, J. Hubaux, Securing vehicular ad hoc networks, J. Comput. Secur. 15 (2007, January) 39–68.
[7] Y. Liu, L. Wang, H. Chen, Message authentication using proxy vehicles in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 64 (8) (2014, September) 3697–3710.
[8] M.R. Asaar, M. Salmasizadeh, W. Susilo, A. Majidi, A secure and efficient authentication technique for vehicular ad-hoc networks, IEEE Trans. Veh. Technol. 67 (2018, April) 5409–5423.
[9] M. Bayat, M. Pournaghi, M. Rahimi, M. Barmshoory, NERA: a new and efficient RSU based authentication scheme for VANETs, Wirel. Netw. 26 (2019, June) 3083–3098.
[10] M.A. Al-shareeda, M. Anbar, S. Manickam, I.H. Hasbullah, An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network, Symmetry 12 (10) (2020, October) 1687–1712.
[11] Z. Wei, J. Li, X. Wang, C. Gao, A lightweight privacy-preserving protocol for VANETs based on secure outsourcing computing, IEEE Access 7 (2019, April) 62785–62793.
[12] G. Zhang, Y. Liao, Y. Fan, Y. Liang, Security analysis of an identity-based signature from factorization problem, IEEE Access 8 (2020, January) 23277–23283.
[13] J. Cui, L. Wei, J. Zhang, Y. Xu, H. Zhong, An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 20 (5) (2019, May) 1621–1632.
[14] T. Limbasiya, D. Das, Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication, IEEE Syst. J. 14 (1) (2020, March) 520–529.
[15] C. Lyu, D. Gu, Y. Zeng, P. Mohapatra, PBA: prediction-based authentication for vehicle-to-vehicle communications, IEEE Trans. Dependable Secure Comput. 13 (1) (2016, February) 71–83.
[16] H. Zhong, S. Han, J. Cui, J. Zhang, Y. Xu, Privacy-preserving authentication scheme with full aggregation in VANET, Inf. Sci. 476 (2019, February) 211–221.
[17] A. Shamir, Identity-based cryptosystems and signature schemes, in: Proc. Workshop Theory Applications Cryptograph. Technology, vol. 196, 1984, pp. 47–53.
[18] X. Wang, P. Hao, L. Hanzo, Physical-layer authentication for wireless security enhancement: current challenges and future developments, IEEE Commun. Mag. 54 (2016, June).
[19] R. Liao, H. Wen, J. Wu, F. Pan, A. Xu, Y. Jiang, F. Xie, M. Cao, Deep-learning-based physical layer authentication for industrial wireless sensor networks, Sensors 19 (11) (2019, May).
[20] A.K. Jadoon, J. Li, L. Wang, Physical layer authentication for automotive cyber physical systems based on modified HB protocol, Front. Comput. Sci. 15 (3) (2021, June).
[21] W. Chin, T.N. Le, C. Tseng, Authentication scheme for mobile OFDM based on security information technology of physical layer over time-variant and multipath fading channels, Inf. Sci. 321 (2015, November) 238–249.
[22] J.K. Tugnait, Wireless user authentication via comparison of power spectral densities, IEEE J. Sel. Areas Commun. 31 (9) (2013, September).
[23] X. Li, J. Liu, B. Ding, Z. Li, H. Wu, T. Wang, A SDR-based verification platform for 802.11 PHY layer security authentication, World Wide Web 23 (2019, January) 1011–1034.
[24] Y. Ran, H. Al-Shwaily, C. Tang, G.Y. Tian, M. Johnston, Physical layer authentication scheme with channel based tag padding sequence, IET Commun. 13 (2019, April) 1776–1780.
[25] H. Wen, J. Zhang, R. Liao, J. Tang, F. Pan, Cross-Layer Authentication Method Based on Radio Frequency Fingerprint, US 10251058B2, United States Patent, 2019, April.
[26] S. Althunibat, V. Sucasas, G. Mantas, J. Rodriguez, Physical-layer entity authentication scheme for mobile MIMO systems, IET Commun. 12 (2018, January) 712–718.
[27] J. Wang, Y. Shao, Y. Ge, R. Yu, Physical-layer authentication based on adaptive Kalman filter for V2X communication, Veh. Commun. 26 (2020, December).
[28] P. Gope, A.K. Das, N. Kumar, Y. Cheng, Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks, IEEE Trans. Ind. Inform. 15 (9) (2019, September).
[29] M. Bottarelli, G. Epiphaniou, D. Kbaier, P. Karadimas, H. Al-Khateeb, Physical characteristics of wireless communication channels for secret key establishment: a survey of the research, Comput. Secur. 78 (2018, August) 454–476.
[30] J. Cui, Y. Wang, J. Zhang, Y. Xu, H. Zhong, Full session key agreement scheme based on chaotic map in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 69 (8) (2020, August) 8914–8924.
[31] M. Yao, X. Wang, Q. Gan, Y. Lin, C. uang, An improved and privacy-preserving mutual authentication scheme with forward secrecy in VANETs, Secur. Commun. Netw. 2021 (2021, April).
[32] M. Arif, G. Wang, M.Z. Bhuiyan, T. Wang, J. Chen, A survey on security attacks in VANETs: communication, applications and challenges, Veh. Commun. 19 (2019, October).
[33] L. Zhang, Cryptanalysis of the public key encryption based on multiple chaotic systems, Chaos Solitons Fractals 37 (3) (2008, August) 669–674.
[34] D. Jungnickel, On the uniqueness of the cyclic group of order n, Am. Math. Mon. 99 (6) (1992) 545–547.
[35] Q. Wang, H. Su, K. Ren, K. Kim, Fast and scalable secret key generation exploiting channel phase randomness in wireless networks, in: Proceedings of IEEE INFOCOM, 2011, June, pp. 1422–1430.
[36] D. Rife, R. Boorstyn, Single-tone parameter estimation from discrete-time observations, IEEE Trans. Inf. Theory 20 (5) (1974, September) 591–598.
[37] L. Cheng, L. Zhou, B. Seet, W. Li, D. Ma, Jibo Wei, Efficient physical-layer secret key generation and authentication schemes based on wireless channel-phase, in: Mobile Information Systems, 2017, Hindawi, 2017, July.
[38] H. Liu, Y. Wang, J. Yang, Y. Chen, Fast and practical secret key extraction by exploiting channel response, in: Proceedings of IEEE INFOCOM, 2013, April, pp. 3048–3056.
[39] M.A. Shawky, Q.H. Abbasi, M.A. Imran, S. Ansari, A. Taha, Cross-layer authentication based on physical-layer signatures for secure vehicular communication, in: 33rd IEEE Intelligent Vehicles Symposium (IV22), 2022, June.
[40] P. Berens, CircStat: a MATLAB toolbox for circular statistics, J. Stat. Softw. 31 (10) (2009, September).
[41] Y. Qiao, S. Yu, P. Su, L. Zhang, Research on an iterative algorithm of LS channel estimation in MIMO OFDM systems, IEEE Trans. Broadcast. 51 (1) (2005, March) 149–153.
[42] Y. Li, L.J. Cimini, N.R. Sollenberger, Robust channel estimation for OFDM systems with rapid dispersive fading channels, IEEE Trans. Commun. 46 (7) (1998, July) 902–915.
[43] A. Wald, Sequential tests of statistical hypotheses, Ann. Math. Stat. 16 (2) (1945, June) 117–186.
[44] H. Koorapaty, A.A. Hassan, S. Chennakeshu, Secure information transmission for mobile radio, IEEE Commun. Lett. 4 (2) (2000, February) 52–55.
[45] P. Karadimas, D. Matolak, Generic stochastic modeling of vehicle-to-vehicle wireless channels, Veh. Commun. 1 (4) (2014, October) 153–167.
[46] P. Karadimas, E.D. Vagenas, S.A. Kotsopoulos, On the scatterers' mobility and second order statistics of narrowband fixed outdoor wireless channels, IEEE Trans. Wirel. Commun. 9 (7) (2010, July) 2119–2124.
[47] E.B. Barker, NIST, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 800th edition, National Institute of Standards and Technology, 2000, December.

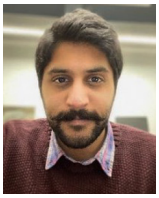
Mahmoud A. Shawky was born in 1990 in Saudi-Arabia. He received his B.Sc. degree in Electronics and Electrical Engineering in 2012 from Air Defence College, Alexandria University, M.Sc. (Eng.) degree in Authentication Mechanisms in Computer Network Protocols from Alexandria University, Alexandria, Egypt. He is currently a lecturer in the Egyptian Air Defence College. He is currently pursuing a Ph.D. degree in James Watt School of Engineering, University of Glasgow, UK. His research interests are in the area of cryptography and number theory, digital signatures, authentication in wireless communications and cyber security.

Dr. Muhammad Usman (Senior Member, IEEE) is a Lecturer in the Department of Electrical and Electronic Engineering at Glasgow Caledonian University (GCU), UK. Before Joining GCU, he was a Research Associate at the University of Glasgow, UK, in the EPSRC funded COG-MHEAR programme grant. This transformative research aims to re-design current hearing aids and assistive technology, where his role was to integrate end-user context in visually-assisted hearing-aid design in a privacy-preserving manner. He is endorsed by the

Royal Academy of Engineering as Global Talent. He holds a Ph.D. degree (cum laude) in information and communication technologies from the University of Trento, Italy. He has as exceptional research output record in the field of 5G and beyond 5G cellular systems, radio frequency (RF) sensing, network security, Internet-of-Things (IoT) and developing intelligent systems for healthcare sector. He is senior member of IEEE. His research interests include RF sensing, wireless communication, software-defined networks, cyber security and assistive technologies for intelligent healthcare systems.

Dr. Muhammad Ali Imran is Professor of Communication Systems at the University of Glasgow, Dean of University of Glasgow UESTC, and Head of the Communications, Sensing and Imaging group (110^{+} researchers). He is an Affiliate Professor at the University of Oklahoma, USA, a visiting Professor at the 5G Innovation Centre of Institute for Communication Systems at the University of Surrey, UK and an Affiliate Research Professor with AI Research Centre of Ajman University, UAE. He has led a number of multimillion-funded international research projects (grant income £15M over last 10 years) encompassing the areas of energy efficiency, fundamental performance limits, sensor networks and self-organising cellular networks. He also led the new physical layer work area for 5G innovation centre at Surrey University. He has a global collaborative research network spanning both academia and key industrial players in the field of wireless communications. He has taught on international short courses in USA, Pakistan, Tunisia, Malaysia and China. He has published over 400 peer-reviewed research papers. He has been awarded the IEEE Comsoc's Fred Ellersick award 2014 and FEPS Learning and Teaching award 2014. He has given an invited TEDx talk (2015) and more than 20 plenary talks and panels at international conferences. He was cochair of the NGNI Symposium of IEEE ICC 2019, and the founder of IEEE Workshop BackNets 2015. He has chaired several tracks/workshops at international conferences including IWCMC, Global SIP, Crowncom, European Wireless, Stemcom 5G, ICC, VTC. He has been a guest editor for IET Communications, IET Signal Processing, IEEE Communications Magazine, IEEE Wireless Communication Magazine, IEEE Access and IEEE JSAC. He is Associate Editor for IEEE Transactions on Communications and IEEE Open Access. He is a senior member of the IEEE and a Senior Fellow Higher Education Academy (SFHEA), UK. He received his Ph.D. Degree from Imperial College London, UK.

Dr. Qammer H. Abbasi is a Reader with the James Watt School of Engineering, University of Glasgow, Deputy Head for the Communication Sensing and Imaging group (110^{+} researchers), Deputy Theme Lead for Quantum & Nanotechnology in the University's Advance Research Centre, Co-Manager of the RF and Terahertz Laboratory, Lead for Healthcare and Internet of things use cases with the Scotland 5G Center Urban Testbed Program and Director for the Dual Ph.D. Degree program, UK. He has a grant portfolio of £6M and has contributed to more than 350^{+} leading international technical journal and peer reviewed conference papers, as well as ten books. He is Associate Editor for IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology, IEEE Sensors, IEEE Internet of Things and IEEE open access Antenna and Propagation, Senior Editor for Frontiers IoT and Sensors Networks section. He is a committee member for IEEE APS Young professional, Sub-committee Chair for IEEE YP Ambassador program, IEEE 1906.1.1 standard on nano communication, IEEE APS/SC WG P145, IET Antenna & Propagation and healthcare networks. He has been a member of the technical program committees of several IEEE flagship conferences and acted as TPC chair and executive chair for 4^{th}, 5^{th} and 6^{th} international UCET conference 2019, 2020, 2021 in addition to being General Chair of EAI Bodynets 2021. He is an expert reviewer for the UK National Commission for UNESCO's, EPSRC and MRC UK (panel member, 2020), Qatar national research funds, Flemish funding council (FWO, panel member), Belgium, OSF Poland, British council, UAE and KSA funds. He serves regularly as an organiser of conferences, special sessions, workshops and TPC member for several IEEE flagship conferences. He has received several research recognitions including the URSI 2019 Young Scientist Award, the UK Exceptional Talent Endorsement by the Royal Academy of Engineering, the Sensor 2021 Young Scientist Award, the National Talent Pool Award in Pakistan, the International Young Scientist Award by NSFC China, the National Interest Waiver by USA, the University Research Excellence Award from TAMUQ for two consecutive years, the Reward for Excellence from the University of Glasgow, the Research Culture Award from the University of Glasgow, and the Pakistan Award for services to Antenna and RF community. In addition, his work has received media coverage from BBC news, Scotland TV, Analog IC tips, Microwaves & RF newsletters, Vertical news, Pakistan Dawn News, Fiercewireless, City42, Dunya news and Chinese news. He is an IEEE senior member and Chair of the IEEE AP/MTT Scotland joint chapter as well as a Fellow of the Royal Society of Arts.



Dr. Shuja Ansari (SMIEEE) is a Lecturer in the Glasgow College UESTC at the University of Glasgow, UK. He received the M.Sc. degree (distinction) in Telecommunications Engineering in 2015, and the Ph.D. degree in Engineering in 2019 from Glasgow Caledonian University (GCU), UK. He joined the Communications, Sensing and Imaging research group at the University of Glasgow as a Research Associate in 2019 working on energy efficient 5G mobile networks. He is currently the Wave-1 Urban 5G use case implementation lead at Glasgow 5G Testbed funded by the Scotland 5G Centre of the Scottish Government working on a variety of 5G applications in partnership with several industrial and academic partners. His research interests include Wireless Communications, Internet of Things, Cooperative Intelligent Transport Systems, Autonomous Systems, Terrestrial/Airborne Mobile Networks, and Healthcare technologies.

Dr. Ahmad Taha (MIEEE) is a Lecturer in the Glasgow College UESTC at the University of Glasgow, UK. He is Endorsed by the Royal Academy of Engineering as an Exceptional Promise under the Global Talent scheme, a Fellow of Advanced Higher Education (FHEA), and a UKCGE recognised Associate Supervisor. He first joined the University of Glasgow as a Postdoctoral Research Associate working on the 5G New Thinking project (funded by the Department for Digital, Culture, Media and Sport DCMS), in collaboration with several industrial and academic partners including Cisco and the University of Strathclyde, He was nominated for the Energy Institute award in 2019 due to contributions in technology-based energy-saving systems in the NHS. His research interests include smart energy systems, energy conscious networks and healthcare technology. He holds a Ph.D. Degree on (topic) from (institute) which was partially funded and in collaboration with the Medway NHS Foundation Trust in Kent, UK.