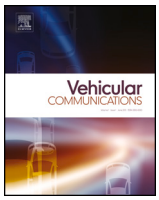
Vehicular Communications 47 (2024) 100784

Contents lists available at ScienceDirect

Vehicular Communications

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



# How secure are our roads? An in-depth review of authentication in vehicular communications

Mahmoud A. Shawky [a,*], Syed Tariq Shah [b,*], Mohammed Abdrabou [c], Muhammad Usman [d], Qammer H. Abbasi [a], David Flynn [a], Muhammad Ali Imran [a], Shuja Ansari [a,*], Ahmad Taha [a,*]

[a] James Watt School of Engineering, University of Glasgow, G12 8QQ, Glasgow, UK
[b] School of Computer Science and Electronic Engineering, University of Essex, Colchester, CO4 3SQ, UK
[c] Department of Electrical and Computer Engineering, University of Victoria, Victoria, Canada
[d] School of Computing, Engineering and Built Environment, Glasgow Caledonian University, G4 0BA, Glasgow, UK

ARTICLE INFO

*Keywords:*
Conditional privacy preservation
Cross-layer authentication
PHY-layer authentication
Reconfigurable intelligent surfaces
Vehicular ad hoc networks
6G technologies

ABSTRACT

Intelligent transportation systems are pivotal in enhancing road safety by enabling intra-vehicle communication. Due to the nature of the wireless communication link, several potential risks of attacks exist, including impersonation, modification, and replay. To ensure the security of vehicular ad hoc networks (VANETs) against malicious activities, secure data exchange between inter-communicating terminals, specifically vehicle-to-everything (V2X) communication, becomes a critical technological challenge that requires attention. Existing authentication methods for VANET applications mainly rely on crypto-based techniques. The emergence of physical (PHY)-layer authentication has gained prominence, leveraging the inherent characteristics of wireless channels and hardware imperfections to distinguish between wireless devices. The PHY-layer-based authentication is not a standalone alternative to cryptographic methods, but it shows potential as a supplementary approach for re-authentication in VANETs, referred to as "cross-layer authentication". This comprehensive survey thoroughly evaluates the state-of-the-art of crypto-based, PHY-layer-based, and cross-layer-based authentication methods in VANETs. Furthermore, this survey delves into integrating different sixth-generation (6G) and beyond technologies, such as reconfigurable intelligent surfaces (RIS) and federated learning, for enhancing PHY-layer authentication performance in the presence of active attackers. Furthermore, in-depth insights into the advantages of cross-layer authentication methods are presented, along with exploring various state-of-the-art VANET security techniques. A detailed technical discussion is provided on these advanced approaches, and it is concluded that they can significantly enhance the security of intelligent transportation systems, ensuring safer and more efficient vehicular communications.

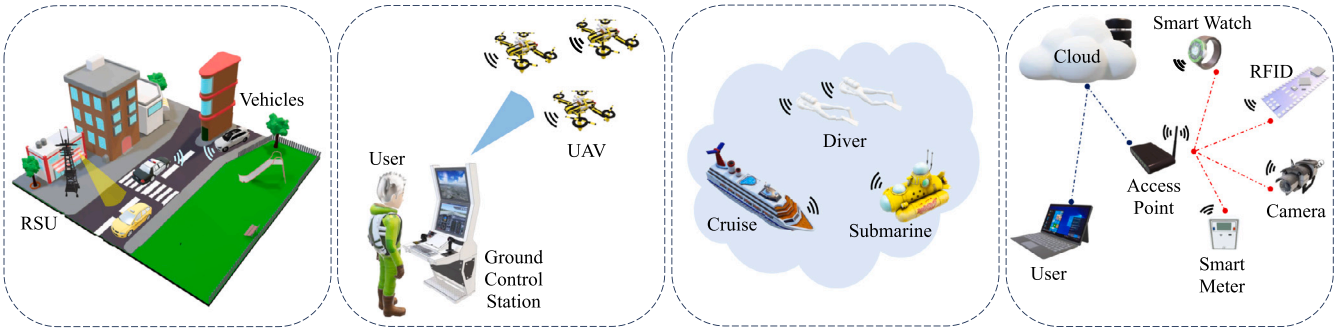
## 1. Introduction

On a global scale, the occurrence of road traffic incidents and mortalities amounts to approximately 1.3 million each year and is projected to ascend as the fifth primary cause of death by the year 2030, as indicated by the authoritative "Second Global Status Report on Road Safety" [1]. The European Commission (EC) disclosed a noteworthy reduction of around 23% in fatal road collisions in the year 2020, compared to the statistics from 2010 [2]. Furthermore, the EC has established the ambitious objective of attaining zero fatalities by 2050. A comprehensive safety framework plan has been published to foster safety and efficiency in transportation, focusing on leveraging technology to conceptualise and deploy intelligent transportation systems [3]. To construct these advanced systems, state-of-the-art sensor data is utilised within vehicular ad hoc networks (VANETs) [4].

The term "ad hoc networks", also known as mobile ad hoc networks (MANETs), refers to the decentralised networks that allow devices, such as laptops, smartphones, or internet-of-things (IoT) devices, to communicate directly with each other, acting as both hosts and routers [5]. This peer-to-peer communication enables data transmission and net-

* Corresponding authors.
*E-mail addresses:* m.shawky.1@research.gla.ac.uk (M.A. Shawky), syed.shah@essex.ac.uk (S.T. Shah), abdrabou@outlook.com, abdrabou@uvic.ca (M. Abdrabou), muhammad.usman@gcu.ac.uk (M. Usman), Qammer.Abbasi@gla.ac.uk (Q.H. Abbasi), David.Flynn@gla.ac.uk (D. Flynn), Muhammad.Imran@gla.ac.uk (M.A. Imran), Shuja.Ansari@gla.ac.uk (S. Ansari), Ahmad.Taha@gla.ac.uk (A. Taha).

https://doi.org/10.1016/j.vehcom.2024.100784
Received 19 October 2023; Received in revised form 31 December 2023; Accepted 21 April 2024
Available online 26 April 2024




(a) Vehicular ad hoc networks. (b) Flying ad hoc networks. (c) Acoustic communication. (d) Wireless sensor networks.

**Fig. 1.** Various applications of wireless ad hoc networks.

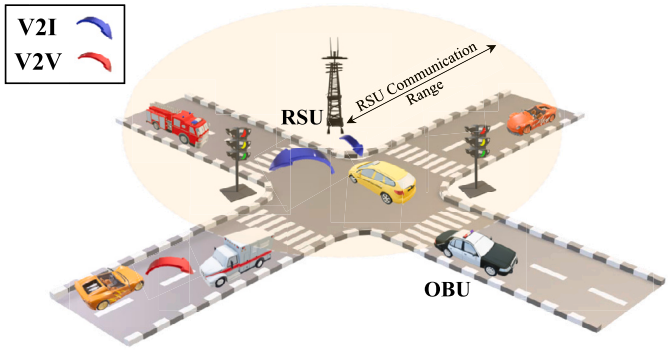



**Fig. 2.** System architecture.

work connectivity even in the absence of a fixed infrastructure, such as Wi-Fi access points or cellular towers. Ad hoc networks are characterised by their ability to self-organise and self-configure, allowing devices to establish communication links and form a network on the fly [6]. Fig. 1 illustrates various applications of ad hoc networks, including VANETs, flying ad hoc networks (FANETs), acoustic communications, and wireless sensor networks (WSN) [5,6]. VANETs facilitate direct vehicle-to-everything (V2X) communication [7], encompassing vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) interactions, see Fig. 2.

Using the dedicated short-range communication protocol (DSRC) protocol [8], each vehicle within the VANET environment autonomously generates and disseminates safety-related messages at a frequency typically ranging from 5.85 to 5.925 GHz [9], every 100 to 300 milliseconds [10]. These messages contain vital data such as the vehicle's current position, speed, acceleration, direction, and other relevant information. By broadcasting these messages periodically, vehicles can effectively communicate their status to other vehicles and infrastructure units in their proximity [11].

VANETs play a crucial role in enhancing the performance of various traffic-related applications, including safety, mobility, and autonomy, while also contributing to reducing carbon emissions and promoting environmentally friendly transportation. By enabling vehicles to optimise their routes and avoid traffic congestion en route to their destinations, VANETs enable efficient and sustainable transportation. Typically, VANETs consist of three primary terminals: a trusted authority (TA), roadside units (RSUs), and onboard units (OBUs) located within vehicles. Each terminal within the network has specific roles described as follows [12].

1. *The trusted authority*: The TA is a trusted terminal for all vehicles and RSUs in the network. The TA plays a critical role in facilitating secure and trustworthy communication between network participants, ensuring that messages transmitted between vehicles are authentic and have not been tampered with. Beyond its role in maintaining secure communication, the TA is also responsible for managing the network's membership by registering vehicles and RSUs before they can participate in network activities. In addition, the TA is responsible for revoking vehicles engaging in malicious activity, such as launching an attack or violating traffic laws.
2. *Roadside units*: RSUs are stationary wireless devices deployed along the roadside infrastructure to offer support for vehicular communication. The primary role of RSUs in VANETs is to enhance the reliability and efficiency of communication between vehicles and between vehicles and the TA. In addition to providing communication support, RSUs can be used for various other applications. These include providing information about traffic conditions, road hazards, and emergency situations to vehicles in the network. They can also be used for collecting traffic data and performing traffic management tasks, such as traffic flow optimisation and congestion control.
3. *Vehicles' OBUs*: OBUs are electronic wireless devices installed on vehicles that enable communication with other vehicles and RSUs. The primary role of OBUs in VANETs is to support the exchange of information among vehicles and between vehicles and the network infrastructure.

Unfortunately, the widespread availability of off-the-shelf wireless cards and the open accessibility of wireless communication have made VANETs vulnerable to various attacks, including interception, modification, and impersonation [13]. For instance, an adversary can fabricate a false emergency to manipulate other drivers into reducing speed or abruptly applying brakes. Moreover, an attacker can impersonate the identity of a legitimate vehicle or generate numerous malicious messages, leading to a fabricated traffic scenario that deviates from reality. The potential ramifications of such malicious attacks include disruptions in traffic flow, congestion, and even accidents. Consequently, it becomes crucial to establish robust mechanisms for message authentication capable of verifying the authenticity of the sender's identity [14].

In VANETs, conventional authentication mechanisms depend on the computational complexity of solving complex cryptographic mathematical problems such as the factorization problem [15] and discrete logarithm problem (DLP) [16]. These mechanisms ensure the integrity and authenticity of transmitted messages. However, generating a cryptographic signature for each message incurs a significant computation cost. Furthermore, the inclusion of these signatures with each message introduces additional communication overhead, consuming approximately 30% of the available bandwidth [17]. Generally, these complex crypto-based operations are typically performed at the upper layers of the protocol stack [18]. These include the application and link layers, see Fig. 3 [19,20].

To address the challenges posed by upper-layer cryptographic approaches' computation and communication overheads, researchers have explored PHY-layer authentication techniques as a promising solution [21]. These techniques leverage the distinctive characteristics of

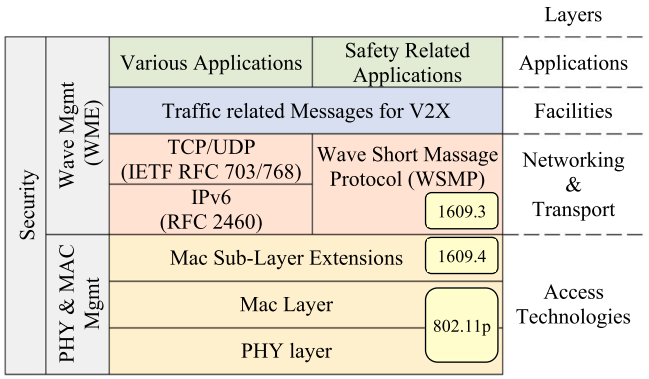



**Fig. 3.** Layered DSRC protocol architecture [19,20].

wireless channels, including channel fading coefficients and phase responses, as well as hardware impairments such as the front-end communication circuit imperfections and the carrier frequency offset (CFO) [22]. By exploiting these inherent properties, PHY-layer authentication can differentiate between terminals without completely relying on computationally intensive cryptographic operations. However, it is important to note that PHY-layer authentication alone cannot be a comprehensive authentication solution [23]. While PHY-layer techniques provide a means to authenticate terminals based on unique channel characteristics, they still require initial identity verification using upper-layer-based authentication mechanisms [24]. This implies that an additional layer of authentication is necessary to verify the identity of the communicating vehicle.

In practice, combining PHY-layer authentication with upper-layer authentication can offer a more robust and efficient authentication framework. This integration can be referred to as "cross-layer authentication" [25]. Upper-layer authentication (i.e., cryptographic approaches) can serve as a preliminary step to quickly establish the authenticity of terminals. Once a terminal's identity is preliminarily verified, PHY-layer authentication mechanisms can be employed to perform a more thorough and reliable verification based on physical properties [23–25]. By integrating PHY-layer and upper-layer authentication techniques, VANETs can benefit from a hybrid approach combining both methods' advantages. This hybrid authentication scheme provides a balance between efficiency and security, leveraging the unique properties of the wireless channel while maintaining the robustness and trustworthiness offered by upper-layer cryptographic approaches.

Cross-layer authentication in vehicular communication draws inspiration from human communication patterns, where individuals are often recognised through initial introductions and subsequent memorisation of their physical features, such as facial characteristics, body shape, voice, and other distinguishing attributes. By applying a similar concept, reliable and secure communication in vehicular networks can be established through an initial handshaking step that utilises crypto-based authentication. This step plays a crucial role in verifying the legitimacy of communicating vehicles and extracting unique wireless device features that can be used for subsequent re-authentication in future transmissions. However, choosing an appropriate PHY-layer re-authentication technique depends on various application characteristics factors, including channel variations, communication range, broadcasting rate, dynamicity, and other relevant parameters [26].

This survey distinguishes itself from previous surveys, such as those mentioned in references [27–29], which focus on reviewing the state-of-the-art of crypto-based authentication methods, as well as surveys [22,30] that solely concentrate on PHY-layer-based authentication methods, see Table 1. In contrast, our survey comprehensively reviews both approaches within the context of VANETs. Furthermore, this survey goes beyond the existing literature by examining current cross-layer authentication methods in VANETs and offering insights into future research directions. In addition, it examines the strengths and weaknesses of each approach and discusses their applicability in different scenarios. This analysis allows for a more holistic understanding of the authentication landscape in VANETs. Moreover, this survey explores the emerging area of cross-layer authentication in VANETs. The contributions of this survey can be summarised as follows:

**Table 1**
A comprehensive taxonomic analysis of survey papers on ad hoc network authentication.

| Ref. | Crypto-based | PHY-layer-based | Cross-layer-based |
|---|---|---|---|
| [27] | √ | - | - |
| [28] | √ | - | - |
| [29] | √ | - | - |
| [30] | - | √ | - |
| [22] | - | √ | - |
| Ours | √ | √ | √ |

1. This paper presents a comprehensive classification of authentication schemes utilised in ad hoc networks, categorising them into crypto-based, PHY-layer-based, and cross-layer-based methods.
2. Moreover, the strengths and weaknesses of each scheme are thoroughly examined, providing valuable insights into their respective suitability for various applications.
3. Finally, we emphasise the significance of integrating cutting-edge sixth-generation (6G) technology, specifically reconfigurable intelligent surface (RIS) and federated learning, to enhance the performance of PHY-layer authentication.

The rest of this paper is structured as follows: Section 2 discusses the metrics employed for evaluating authentication schemes. Sections 3, 4, and 5 offer a comprehensive review of the crypto-based, PHY-layer-based, and cross-layer-based authentication, respectively. Section 6 explores the prospective developments and insights about 6G authentication in VANETs. Finally, Section 7 presents the concluding remarks of this survey.

## 2. Performance evaluation metrics

To ensure the robustness of an authentication scheme, it must adhere to predefined security and privacy metrics. Likewise, evaluating the scalability of a scheme in VANETs primarily hinges upon its ability to meet the computation and communication overhead metric [31,32]. A detailed discussion of the performance evaluation metrics presented in Fig. 4 is as follows.

### 2.1. Security and privacy requirements

Following are the security and privacy requirements for VANET applications.

1. *Privacy preservation*: Privacy preservation refers to protecting users' personally identifiable information (PII) from unauthorised access or disclosure. In VANETs, privacy preservation aims to safeguard the identity, location, and travel pattern information of vehicles and their passengers from being revealed to unauthorised entities or attackers. The objective is to prevent the misuse of this information, such as for surveillance, tracking, or profiling purposes.
2. *Unlinkability*: Unlinkability ensures that adversaries cannot track the transmitter behaviours by identifying the transmission source of two different messages. It can be achieved through the use of techniques such as dynamically updated pseudonyms, which allow vehicles to hide their real identities while still being able to communicate without linking between different messages. By ensuring unlinkability, VANETs can protect the users' privacy and prevent attackers from tracking and profiling users' activities.

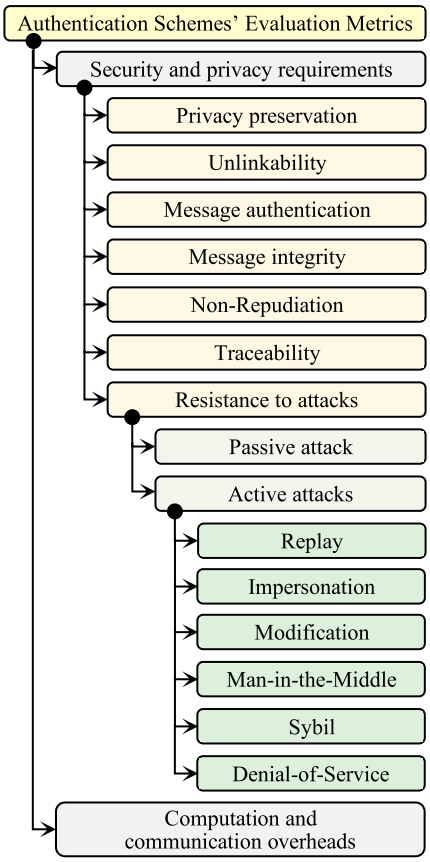



**Fig. 4.** Performance evaluation metrics of different authentication schemes.

3. *Message authentication*: Receiver's ability to authenticate every safety-related message sent from a specific terminal. The primary objective of message authentication is to prevent malicious entities from injecting false or modified messages into the network, which can compromise the safety and efficiency of vehicular communication.
4. *Message integrity*: Receiver can detect modification attempts on messages exchanged between vehicles. This can be ensured through cryptographic techniques such as message authentication codes and digital signatures.
5. *Non-Repudiation*: Non-repudiation ensures that a sender cannot deny sending a message/data to a receiver. It is a security requirement that provides proof of the origin of a message, its delivery to the intended recipient, and its contents. Non-repudiation helps to prevent disputes and false accusations arising from malicious attacks or errors. It is achieved through digital signatures and certificates, which provide a unique and verifiable identification of the sender and ensure the transmitted information's authenticity, integrity, and confidentiality.
6. *Traceability*: Traceability ensures the ability to track and identify the real identity of vehicles in the network, which can be used for various purposes, such as traffic management, accident investigation, and law enforcement. However, traceability can also threaten privacy as it may reveal sensitive information about the driver, such as their identity and travel patterns. Therefore, it is important to implement traceability to balance the need for information with the users' privacy concerns. This can be achieved through anonymous identifiers, encryption, and access controls, which ensure that the data is only accessible to authorised parties and is protected from unauthorised disclosure or misuse.
7. *Resistance to attacks*: The primary objective of an attacker is to disrupt the network by implementing the following attacks [33].

- *Passive attack*: A passive attack involves eavesdropping on the communication between vehicles without altering or modifying the content of the messages. In this attack, the attacker monitors messages exchanged between vehicles to gain sensitive information, such as the vehicle's location, heading, and speed, without being detected or raising suspicions. This attack can be carried out using various techniques such as radio frequency scanning, packet sniffing, or traffic analysis. Passive attacks are difficult to detect as the attackers do not alter the original messages or cause any disruption in message contents. Therefore, it is important to implement security solutions such as encryption, authentication, and access control, which can prevent passive attacks by ensuring the confidentiality and integrity of messages' contents.
- *Active attacks*: An active attack involves modifying or manipulating the content of the messages exchanged between vehicles or between a vehicle and infrastructure. In this attack, the attacker aims to disrupt vehicular communication by performing impersonation, message replay, and modification. This can have severe consequences, causing accidents, traffic congestion, or misleading vehicles to the wrong destination. Active attacks can be carried out by malicious vehicles or infrastructure or by exploiting vulnerabilities in VANET protocols or applications. The following are the common types of active attacks [34,35].
  (a) *Replay attack*: A replay attack involves retransmitting previously captured messages to cause confusion or carry out unauthorised actions. Cryptographic techniques such as timestamps or sequence numbers ensure message freshness and uniqueness to avoid this attack. While digital signatures, authentication codes, and secure communication channels guarantee message authenticity.
  (b) *Impersonation attack*: An impersonation attack involves a malicious entity acting as a legitimate entity to gain unauthorised access or control over the network. In this attack, the attacker pretends to be a trusted entity such as a vehicle, a traffic sign, or a roadside unit to either gain access to sensitive information, disrupt communication, or carry out unauthorised actions.
  (c) *Modification attack*: In this attack, the attacker tries to modify the data transmitted over the network to cause malicious effects or intercepts the transmitted data and alters it in some way before forwarding it to the intended recipient. This modification can be done in various ways, such as changing the content of the message, the source or destination, or the timing of the message. Some techniques that can be used to prevent such attacks include message authentication, encryption, and digital signatures.
  (d) *Man-in-the-Middle attack*: In this attack, the attacker controls the messaging process by manipulating and redirecting the communication flow between different terminals in the network.
  (e) *Sybil attack*: The attacker employs a strategy involving the generation of multiple fabricated identities, intending to masquerade as numerous legitimate users. This malicious action is aimed at disrupting the network functionality. To prevent such attacks, authentication and verification mechanisms are essential to ensure only legitimate vehicles can join the network or reputation-based systems that can detect anomalies in vehicles' behaviours.
  (f) *Denial-of-Service (DoS) attack*: In this attack, the attacker uses several techniques, such as flooding the network with messages, sending fake requests, or consuming network resources to disrupt the network's functionality.

**Table 2**
Overhead categories for computation and communication [28].

| Classification Category | Computation overhead (*msec*) | Communication overhead (*bytes*) |
|---|---|---|
| Low | 1 : 3 | 1 : 50 |
| Medium | 3.1 : 6 | 51 : 100 |
| High | 6.1 : 10 | 101 : 140 |

### 2.2. Computation and communication overheads

In VANET applications, it is vital to consider the computation and communication overheads as they significantly impact the overall system performance. The term "computation overhead" pertains to the computational power and processing requirements necessary to execute intricate algorithms and protocols within the VANET environment. This overhead is influenced by the complexity of the algorithms used for tasks such as route planning, data fusion, collision avoidance, and other intelligent decision-making processes. On the other hand, the term "communication overhead" refers to utilising channel bandwidth and network resources that are essential for exchanging information among vehicles and infrastructure components [27]. In VANETs, vehicles are limited in processing power and memory, and running complex algorithms can drain their battery quickly. This can be challenging for safety-critical applications, such as collision avoidance, which require real-time processing and low latency. As the number of vehicles on the network increases, computation and communication overheads increase, leading to congestion and message delivery delays. In the realm of authentication, ensuring reliability necessitates finding the ideal trade-off between minimal computational complexity and communication costs, thereby guaranteeing optimal network scalability. Table 2 categorises the associated overheads necessary for transmitting and verifying a single authentication request in VANETs based on low, medium, and high categories [36]. The low, medium, and high categories for communication overhead are 1 to 50 *bytes*, 51 to 100 *bytes*, and 101 to 140 *bytes*, respectively, while those for computation overhead are 1 to 3 *msec*, 3.1 to 6 *msec*, and 6.1 to 10 *msec*, respectively.

## 3. Crypto-based authentication

The classification depicted in Fig. 5 provides a comprehensive taxonomy of the existing authentication methods employed in ad hoc networks. The current state-of-the-art authentication in VANETs has been enriched by numerous contributions from researchers who have employed various cryptographic techniques, including the elliptic curve cryptosystem (ECC), bilinear pairing (BP), and hash functions. Generally, there are three commonly used crypto-based authentication methods denoted by public key infrastructure (PKI)-based, identity (ID)-based, and group signature (GS)-based authentication. This section comprehensively discusses recently published approaches based on PKI, ID, and GS authentication.

### 3.1. PKI-based authentication

This type of authentication relies on a trusted third party known as the certificate authority (CA) to issue digital certificates to communicating entities. These digital certificates contain the entity's public key, which other entities use to authenticate the entity's identity. Generally, PKI-based authentication involves the following steps:

1. The entity generates a key pair consisting of private and public keys for authentication.
2. The entity sends a certificate signing request (CSR) to the CA, which includes the entity's public key and identifying information.
3. The CA verifies the entity's identity and issues a digital certificate containing the entity's public key and identifying information.
4. The entity uses its private key to sign a message or generate a digital signature, which can be verified by other entities using the entity's public key.

Suppose an entity $A$ wants to authenticate its identity to entity $B$ using PKI-based authentication. Then, $A$ generates a key pair $\{A_{priv}, A_{pub}\}$, where $A_{priv}$ and $A_{pub}$ are the private and public keys, respectively.

1. $A$ sends a CSR to the CA, which includes its public key and identifying information: $CSR_A = \langle A_{pub}, ID_A \rangle$.
2. The CA verifies $A$'s identity and issues a digital certificate containing the entity's public key and identifying information: $Cert_A = \langle CSR_A, \sigma_{CA} \rangle$, where the CA's signature on the CSR is $\sigma_{CA} = Sign_{CA_{priv}}(CSR_A)$ and $CA_{priv}$ is the CA's private key.
3. Next, $A$ signs the packet payload $(m \| Cert_A)$ using its private key to generate $\sigma_A = Sign_{A_{priv}}(m \| Cert_A)$. Then, $A$ sends the tuple $\langle m, Cert_A, \sigma_A \rangle$ to $B$.
4. Finally, $B$ checks $\sigma_{CA} \in Cert_A$ and verifies the received signature $(\sigma_A)$ using $A$'s public key as $Verify_{A_{pub}}(\sigma_A)$.

Fig. 6 shows the description of PKI-based authentication. A selective list of articles in Fig. 5 is provided to comprehensively compare various methodologies and their limitations in PKI-based authentication. These articles offer a detailed overview of the various approaches to PKI-based authentication and their respective advantages and limitations.

In [37], Raya et al. introduced an enhanced PKI-based approach that involves preloading a substantial number of anonymous certificates and corresponding private keys. The CA signs these certificates and contains the vehicle's pseudo identities. In this way, users remain anonymous. To ensure long-term security and privacy, it is necessary to preload a sufficient number of certificates (approximately 43,800 [27]) onto each vehicle's OBU, typically enough to last for a certain period. These certificates can be updated during the annual registration process. When a safety-related message needs to be signed, an anonymous certificate and its associated private key are randomly selected. The private key generates the signature, while the public key attached to the certificate is used for verification by the recipient. Only the CA has access to information linking the real identities of vehicles to their anonymous certificates. This mechanism allows the CA to trace misbehaviour and identify users if necessary. However, revocation is a primary limitation of PKI-based authentication in vehicular networks, requiring the management of many certificates in the certificate revocation list (CRL). In practical terms, revoking a single vehicle requires adding all of its issued certificates to the CRL. With more revoked vehicles, the CRL size increases. This adversely affects the signature verification as the recipient checks the CRL for each received signature, posing a challenge. Hence, carefully considering the CRL size and verification time is crucial for efficient and secure management of revoked certificates.

In high-speed dynamic conditions, centralising certification services on the servers could compromise access availability. To address this problem, the research conducted by Oulhaci et al. [38] discusses designing and implementing a distributed certification system architecture that centralises the certification services on the region certification authority (RCA) instead of the CA. The authors emphasised the need for security in VANETs and proposed a distributed approach that allows for effective management of public key certificates (PKCs) using the RCA and sub-ordinate RSUs to issue and sign PKCs to the corresponding vehicles in the same region while improving the resistance to attacks with compromised RSUs. However, this approach still relies on centralising certification services to the RCA, potentially posing a single point of failure and scalability challenges in a large-scale network. Wang et al. [39] proposed the local identity-based anonymous message authentication protocol (LIAP) for VANETs. The LIAP scheme uses a hybrid digital signature approach, where registered vehicles are issued long-term certificates for mutual authentication between RSUs and vehicles in the

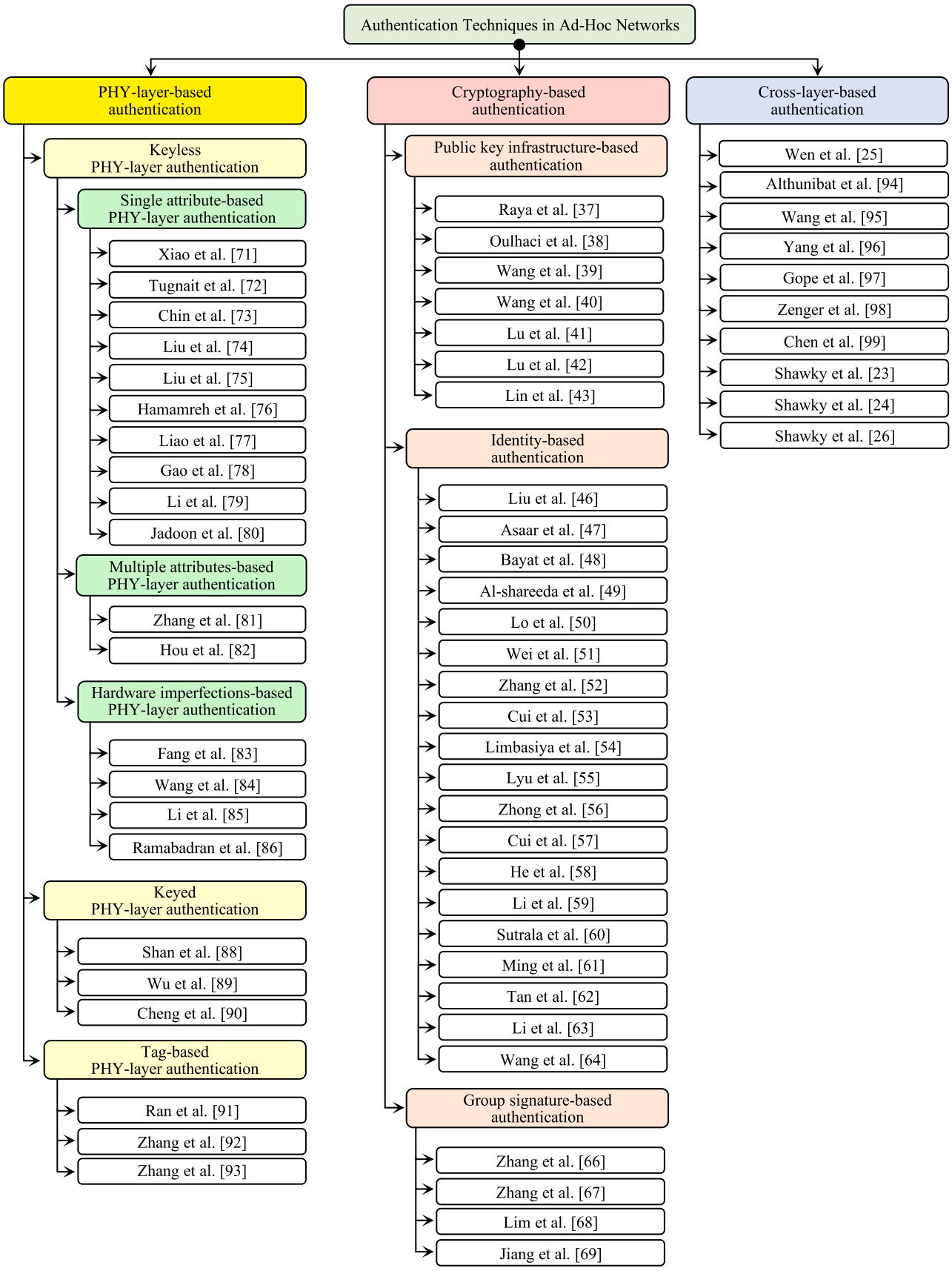



**Fig. 5.** Classification of authentication schemes in wireless communications.

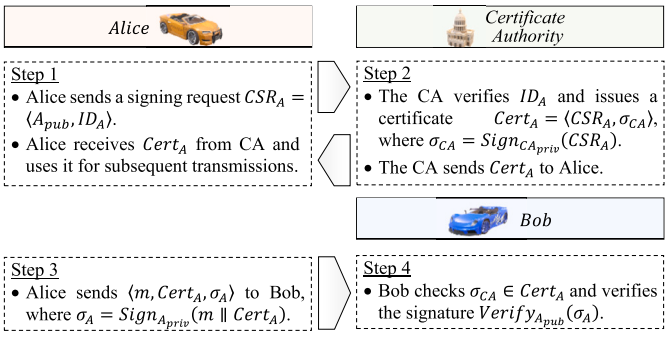



**Fig. 6.** High-level description of PKI-based authentication.

same geographic area. To verify the certificates, the validity of the vehicle's certificate is checked against the vehicle's CRL, while the RSU's certificate is checked against the RSU's CRL. After mutual authentication, the RSU issues a local master key, transmitted encrypted to the corresponding vehicle. By using the received local master key, the vehicle then generates its anonymous IDs and private keys, which are used for signing messages. To ensure secure communication, the local master key is periodically updated. When communicating with adjacent vehicles in another region with a different RSU, each signature must include the local public key of the regional RSU. Vehicles, in turn, identify the source region of messages by checking the received local public key and then verifying the signatures. However, its reliance on the computationally costly bilinear pairing and map-to-point ($M \rightarrow P$) hash function may introduce scalability and performance limitation issues.

To reduce the high computational cost of checking the CRL, Wang et al. [40] proposed a hybrid authentication scheme that combines PKI-based with anonymous ID-based authentication. After registration with the CA, each vehicle is issued a unique long-term certificate. To obtain an anonymous ID, the vehicle sends a message request to the corresponding RSU, which checks the validity of the vehicle's certificate and the freshness of the request at a certain timestamp. If the request is valid, the RSU sends the vehicle's request to the CA, which issues the corresponding pseudo ID and sends it to the vehicle via the RSU as an encrypted message. The vehicle decrypts the message and obtains its anonymous ID, which is subsequently utilised during the message signing phase. Nevertheless, this method may introduce additional latency in the authentication process due to the involvement of multiple entities (RSU and CA) in the anonymous ID issuance, potentially impacting the real-time communication requirements of VANETs.

This part provides an overview of prominent blockchain-based authentication techniques to address certain limitations associated with PKI-based authentication in VANETs. In reference [41], a novel blockchain-based methodology was introduced by Lu et al., featuring proof of presence and absence mechanisms for certificate issuance and revocation. This innovative approach incorporated a conditional identity anonymity feature to enhance user privacy. Notably, this system also integrated a reputation scoring system to gauge the trustworthiness of message senders during transmissions. However, one notable limitation in their scheme is the absence of unlinkability. The system's gradual updating of reputation scores introduces a potential vulnerability, wherein adversaries could exploit this feature to trace broadcasted messages and subsequently execute location-tracking attacks, undermining the security and privacy of the communication process. Another approach by Lu et al. [42] combines the Merkle Patricia Tree with blockchain technology to facilitate monitoring of the authority's activities, thereby promoting transparency. Nonetheless, generating anonymous certificates in this method necessitates frequent interactions between vehicles and the CA.

In an effort to enhance the certificate distribution and revocation process, Lin et al. [43] innovatively integrated the public blockchain network "Ethereum" into the PKI-based framework. Within this novel

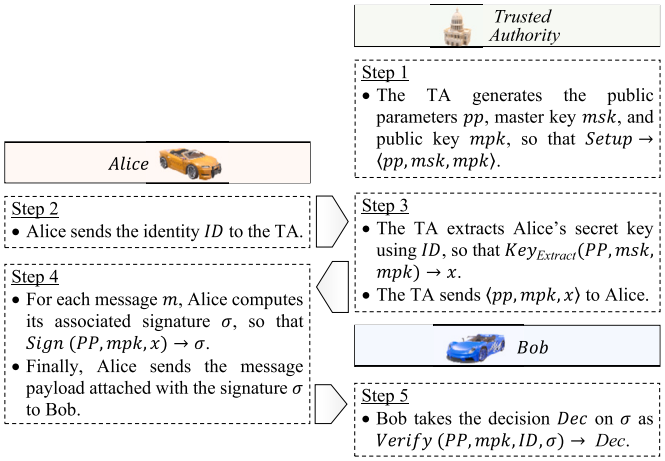



**Fig. 7.** High-level description of ID-based authentication.

approach, the CA actively updates the blockchain with distinct blocks containing users' digital certificates in the form of transactions. Consequently, network terminals gain the ability to verify the legitimacy of received signatures by corroborating them with transaction addresses, thus ensuring the integrity and security of the entire process. However, blockchain-based solutions' practical feasibility and scalability in high-speed and resource-constrained environments need further investigation to assess their suitability for real-world deployment [44].

### 3.2. ID-based authentication

An ID-based authentication is a cryptographic approach where a user's identity information is utilised to derive the corresponding public key, while the private key is generated and distributed by the TA based on the provided identity information [45]. This process enables the receiver to verify incoming messages using the sender's public key and the sender to sign messages using its private key. The typical steps involved in ID-based authentication are as follows:

1. *Setup*: This step involves generating the system public parameters ($PP$), the master key ($msk$), and its associated public key ($mpk$), s.t. $Setup \rightarrow \langle PP, msk, mpk \rangle$, where the master secret key ($msk$) is kept secret.
2. *Key Extraction*: Given an identity ($ID$) for a specific terminal, the TA extracts the $ID$'s relevant secret key ($x$) based on $\langle PP, msk, mpk \rangle$, s.t. $Key_{Extract}(PP, msk, mpk) \rightarrow x$.
3. *Signing*: In this step, the communicating terminal computes the signature ($\sigma$) based on $\langle PP, mpk, x \rangle$, s.t. $Sign(PP, mpk, x) \rightarrow \sigma$.
4. *Verifying*: In this step, the recipient decides on the received signature $Dec = \{accepted, rejected\}$ based on $\langle PP, mpk, ID, \sigma \rangle$, s.t. $Verify(PP, mpk, ID, \sigma) \rightarrow Dec$.

Fig. 7 shows the description of ID-based authentication. However, ID-based authentication encounters significant computation complexity due to the complex design of this authentication approach. This limitation hinders the system's ability to achieve both high scalability and low latency. Achieving scalability is a main objective of various research studies [32–43,45–51], where the network is able to incorporate additional terminals without compromising performance. Liu et al. [46] introduced the first proxy-based authentication scheme, where proxy vehicles utilise their computation capabilities to verify signatures on behalf of the RSUs and broadcast the verification results. Nonetheless, it is important to note that their approach was primarily tailored to V2I communication and did not encompass the crucial domain of V2V communication scenarios. Subsequently, Asaar et al. [47] identified vulnerabilities in the scheme proposed by Liu et al. [46], particularly with impersonation and modification attacks. They developed an

enhanced proxy-based scheme that exhibited improved computational performance. The enhanced scheme distributed the $n$ received signatures among $\lceil \frac{n}{d} \rceil$ proxy vehicles for the signature verification process, with $d \simeq 0.1n$. However, a significant security concern emerged about this approach due to the preloading of the TA master key into vehicles' tamper-proof devices (TPDs), making them vulnerable to potential side-channel attacks. To address this issue, Bayat et al. [48] proposed an alternative method by leveraging the secure communication link between the TA and RSUs to dynamically update the master key stored in the RSUs' TPDs. Their approach utilised bilinear pairing properties and the $M \rightarrow P$ hashing function to develop an ID-based scheme that supported batch verification. Despite its advantages, this scheme exhibited significant computation complexity.

In this challenging scenario, Al-shareeda et al. [49] developed a novel free pairing conditional privacy-preserving authentication scheme. Their approach utilised an online mode for updating the secret parameters of TPDs, effectively mitigating potential side-channel attacks. However, this scheme incurred a high communication cost. Lo et al. [50] presented an alternative solution to address the computational overhead arising from bilinear pairing operations. They leveraged the computational Diffie-Hellman problem of the ECC for singular verification, offering a more efficient approach. Furthermore, in a lightweight ID-based solution, Wei et al. [51] utilised the factorization problem of the RSA cryptosystem for identity verification, aiming to achieve a resource-efficient authentication process.

In a recent study, reference [52] highlighted a vulnerability in the proposed scheme presented in [51], wherein the common modulus attack could potentially expose the secret parameters of vehicles. To address the computational load on the vehicles, [53] suggested an edge computing technique where RSUs verify messages from neighbouring vehicles and subsequently broadcast verification results to the surrounding vehicles. However, subsequent research conducted by Limbasiya et al. in [54] revealed security weaknesses in [53]'s approach, specifically concerning susceptibility to impersonation attacks. Limbasiya et al. introduced a message authentication method based on symmetric key cryptography to address these concerns. Lyu et al. [55] proposed a novel approach where they integrated the timed efficient stream loss-tolerant authentication (TESLA) method with elliptic curve-based digital signatures. This innovative combination resulted in developing a scheme capable of predicting a vehicle's future position to enable instantaneous message authentication. However, the high communication cost associated with the Merkle Hash Tree's added leaf values remained a challenging issue. To tackle the communication cost and privacy concerns, [56] proposed a certificateless aggregation signature scheme that reduces the signature size. However, they did not consider the implications for V2V applications, which is crucial as vehicles have lower processing power than RSUs. In [57], Cui et al. introduced an ECC-based content-sharing scheme specifically tailored for fifth-generation (5G)-enabled vehicular networks. Their approach allows vehicles with content downloading requests to efficiently filter nearby vehicles and select competent proxy vehicles to provide content services.

Many studies have made significant contributions towards addressing the critical security and privacy concerns associated with VANETs. In references [58–61], researchers introduced conditional privacy-preserving authentication (CPPA) schemes, which utilise ECC-based scalar multiplication and addition operations for signature generation and verification. One of the proposed schemes, as outlined in reference [59], employs a pseudo-ID-based approach, where pseudo-identities are exchanged between terminals to provide conditional privacy. Additionally, other researchers [62–64] designed certificate-less authentication schemes, aimed at reducing authentication overheads and enhancing privacy. These schemes allow vehicles to forgo storing certificates for authentication purposes, relieving the TA from the burden of extracting the real identities of malicious vehicles from certificates.

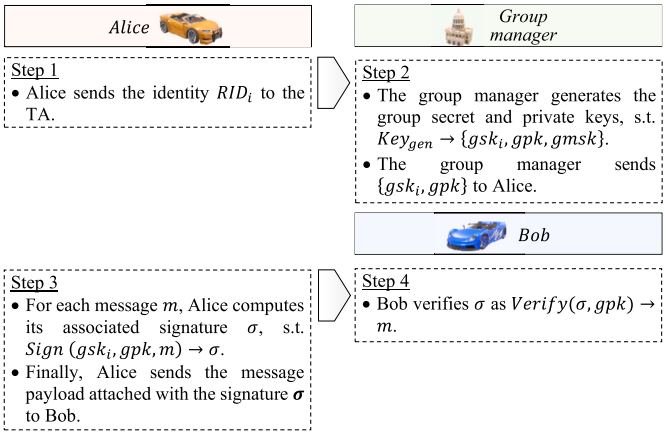



**Fig. 8.** High-level description of GS-based authentication.

### 3.3. GS-based authentication

In the context of GS-based authentication, a group consists of a manager and its members. When a message ($m$) needs to be signed by any group member ($V_i$), $V_i$ generates its corresponding signature ($\sigma$), utilising their respective secret key ($gsk_i$). This way ensures privacy preservation during the signature generation as $V_i$ signs messages on behalf of the group members [65]. Subsequently, the message recipient verifies the $\sigma$ using the group's public key ($gpk$). GS-based authentication typically involves four following steps [29]:

1. $Key_{gen}$: This phase is executed to generate the essential secret and private keys, s.t. $Key_{gen} \rightarrow \{gsk_i, gpk, gmsk\}$ and other parameters, where $gmsk$ is the group manager's secret key.
2. $Sign\ (m, gsk_i, gpk)$: This phase is run by $V_i$ to sign $m$ using $gsk_i$ related to $gpk$, s.t. $Sign(gsk_i, gpk, m) \rightarrow \sigma$.
3. $Verify(\sigma, gpk)$: The recipient checks the validity of $\sigma$ using $gpk$ without disclosing $V_i$'s real identity ($RID_i$), s.t. $Verify(\sigma, gpk) \rightarrow m$.
4. $Open(\sigma, gpk, gmsk)$: The group manager can reveal $RID_i$ using $gmsk$, s.t. $Open(\sigma, gpk, gmsk) \rightarrow RID_i$ in case of misbehaving.

Fig. 8 shows the description of GS-based authentication. Nevertheless, a significant drawback of this approach is the necessity to update and distribute the group key through the TA each time a vehicle joins or leaves the group region. This requirement poses challenges in supporting both forward and backward secrecy, particularly for high-speed group members. As highlighted in [66], a potential enhancement involves assigning RSUs as group managers to reduce communication and computation overheads. However, if an RSU becomes compromised, it puts the private information of vehicles at risk of exposure. Zhang et al. [67] proposed a group key distribution algorithm for GS-based batch verification. This algorithm uses a bivariate polynomial-based mechanism to ensure that only unrevoked vehicles can access the group session key. Reference [68] decreases the insignificant overhead on the TA by dividing the RSUs/domain into leader RSU (L-RSU) and member RSUs (M-RSUs). The L-RSU is responsible for generating group keys and tracing the real identities of misbehaving vehicles with the help of the TA. Increasing the number of M-RSUs/domain enhances the system's performance because the vehicle remains in the same domain for a longer period, decreasing the number of domains/region. However, managing the complexities associated with increasing M-RSUs requires careful consideration in practical scenarios. Using a region trust authority, reference [69] provides vehicles with authentication services and reduces the overhead on RSUs and the TA.

**Table 3**
Ensuring security and privacy: A comprehensive analysis of crypto-based authentication schemes (Part I).

| Ref. | PKI-based | | | | | | | ID-based | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | [37] | [38] | [39] | [40] | [41] | [42] | [43] | [46] | [47] | [48] | [49] | [50] | [51] | [52] | [53] |
| Privacy Preservation | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Unlinkability | ✓ | ✓ | × | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Message Authentication | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Message Integrity | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Non-Repudiation | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Traceability | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Resistance to Replay | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | × | ✓ | ✓ | ✓ | × | ✓ | × |
| Resistance to Impersonation | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | × | ✓ | ✓ | ✓ | × | ✓ | × |
| Resistance to Modification | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | × | ✓ | ✓ | ✓ | × | ✓ | × |
| Resistance to DoS | × | × | × | × | × | × | × | × | × | × | × | × | × | × | × |
| Computation Cost | Low | Low | High | Med. | Med. | Med. | Low | High | Low | Med. | Low | Med. | Low | High | Med. |
| Communication Cost | Med. | Med. | Med. | Med. | High | High | High | Med. | High | Med. | High | High | High | High | Med. |

**Table 4**
Ensuring security and privacy: A comprehensive analysis of crypto-based authentication schemes (Part II).

| Ref. | ID-based | | | | | | | | | | | GS-based | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | [54] | [55] | [56] | [57] | [58] | [59] | [60] | [61] | [62] | [63] | [64] | [66] | [67] | [68] | [69] |
| Privacy Preservation | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Unlinkability | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Message Authentication | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Message Integrity | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Non-Repudiation | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Traceability | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Resistance to Replay | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Resistance to Impersonation | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Resistance to Modification | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Resistance to DoS | × | × | × | × | × | × | × | × | × | × | × | × | × | × | × |
| Computation Cost | Low | Low | High | Med. | Med. | Med. | High | Med. | High | High | High | High | High | High | High |
| Communication Cost | High | High | High | High | High | High | High | High | High | High | High | High | High | High | High |

### 3.4. Challenges of crypto-based authentication

For a comprehensive evaluation, Tables 3 and 4 present an in-depth analysis of crypto-based authentication methods concerning their fulfilment of VANET security and privacy requirements. The evaluation reveals that certain approaches cannot support resistance against active attacks, a security flaw supported by findings in the literature. Moreover, considering the flooding type of the DoS attack in which the attacker tries to deteriorate the network's performance by overwhelming the targeted terminal with fake signatures $\sum \sigma_i$. The current state-of-the-art suggests using channel switching and beamforming techniques to avoid such attacks. However, an effective authentication scheme should consider a low-time cost verification process of $\sigma_i$ allows for mitigating the impact of such an attack on the network, which is hard to achieve due to the high computation cost of cryptographic operations, as summarised in Tables 3 and 4.

Furthermore, it can be noted that there is a trade-off relationship between the computation and communication overheads. While some schemes prioritise minimal computational overhead for enhanced performance, they may neglect the importance of managing communication overheads. An effective authentication framework should consider both metrics. At last, Fig. 9 summarises the performance limitations associated with different types of crypto-based authentication in VANETs.

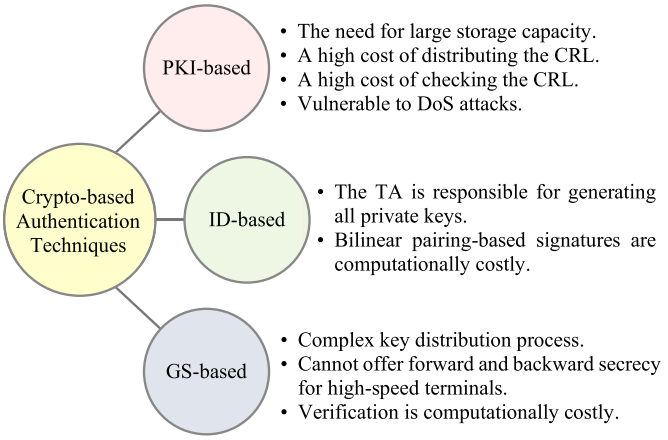



**Fig. 9.** Challenges of crypto-based authentication methods.

## 4. PHY-layer authentication

PHY-layer authentication is a security mechanism that aims to establish the authenticity of wireless communication devices by exploiting the unique physical characteristics of their wireless transmissions. This authentication process is performed at the physical layer of the protocol stack and is effective in preventing various types of attacks, including spoofing and impersonation. In this context, existing PHY-layer authentication methods can be classified into three main categories: keyless, keyed, and tag-based (see Fig. 5), which are presented in Subsections 4.1, 4.2, and 4.3, respectively. These subsections review articles discussing different PHY-layer authentication methods in wireless communication. Finally, the challenges of implementing each method in vehicular communication networks are outlined.

### 4.1. Keyless PHY-layer-authentication

Keyless PHY-layer authentication is a technique used to verify wireless communication devices' authenticity without relying on pre-shared keys or secret information. Instead, this approach exploits the inherent properties of the hardware manufacturing process of different wireless

**Table 5**
Classification of keyless PHY-layer-authentication.

| Ref. | Authors | Year | Authentication feature |
|---|---|---|---|
| *Single attribute-based PHY-layer authentication* | | | |
| [71] | Xiao et al. | 2008 | CFR |
| [72] | Tugnait et al. | 2013 | PSD |
| [73] | Chin et al. | 2015 | PDP |
| [74] | Liu et al. | 2016 | CIR |
| [75] | Liu et al. | 2017 | CIR |
| [76] | Hamamreh et al. | 2018 | CSI |
| [77] | Liao et al. | 2019 | CSI |
| [78] | Gao et al. | 2019 | RSS |
| [79] | Li et al. | 2020 | RSS |
| [80] | Jadoon et al. | 2021 | RSS |
| *Hardware imperfections-based PHY-layer authentication* | | | |
| [81] | Zhang et al. | 2019 | AFE imperfections |
| [82] | Hou et al. | 2014 | CFO |
| *Multiple attributes-based PHY-layer authentication* | | | |
| [83] | Fang et al. | 2018 | CFO & CIR & RSS |
| [84] | Wang et al. | 2016 | RSS & (I/Q imbalance) |
| [85] | Li et al. | 2019 | CSI & RSS & CFO |
| [86] | Ramabadran et al. | 2020 | CIR & AFE imperfections |

devices, such as the carrier frequency offset (CFO) and analogue front-end (AFE) imperfections, and the unique attributes of wireless communication channels, such as the channel state information (CSI), received signal strength (RSS), power delay profile (PDP), channel frequency response (CFR), channel impulse response (CIR) and power spectral density (PSD), to discriminate between different wireless devices. Keyless authentication methods typically use statistical analysis to compare the characteristics of the received signal with those of a known reference signal to determine whether the sender is authentic or not. This approach is particularly useful when pre-shared keys are unavailable or impractical. Keyless authentication can generally be classified into three categories: single attribute-based, multiple attributes-based, and hardware imperfections-based methods. Table 5 categorises the literature on keyless authentication according to the distinctive discrimination features employed in the selected studies.

#### 4.1.1. Single attribute-based PHY-layer authentication

The channel attributes-based method is founded on the principle of leveraging the short-term spatial and temporal correlations in channel characteristics between two wireless communication devices. These correlations can be effectively described by a zero-order Bessel function, with the first zero point occurring at a distance of half the wavelength ($\lambda/2$) between the legitimate user and the adversary [70], as depicted in Fig. 10. Thus allowing for location decorrelation between legitimate and wiretapped channel responses. This approach involves utilising a range of channel features including the CFR [71], PSD [72], PDP [73], CIR [74,75], CSI [76,77], and RSS [78–80]. By tracking these features, this method ensures that the received signals, $R_X(t)$ and $R_X(t+\Delta t)$, originate from the same source, where the receiving time interval $\Delta t$ is less than or equal to the coherence time $T_c$. This approach is commonly known as the "feature tracking" mechanism.

In [71], Xiao et al. proposed an authentication method that enables a receiver ($B$) to authenticate a legitimate terminal ($A$) based on the channel frequency response in a time-variant environment. The proposed method involves comparing the estimated channel response $H_{A\to B}(K)$ with previously recorded responses $H_t(K)$. If the channel responses are highly correlated over time, the terminal is considered trustworthy. On the other hand, if the channel responses are not correlated, the terminal is deemed untrustworthy, depending on the threshold value ($\tau$). The decision to trust or not trust the terminal is made based on a binary hypothesis testing problem. Specifically, the null hypothesis is defined as $H_0 : H_t(K) = H_{A\to B}(K)$, while the alternative hypothesis is defined as $H_1 : H_t(K) \neq H_{A\to B}(K)$. Tugnait et al. [72]

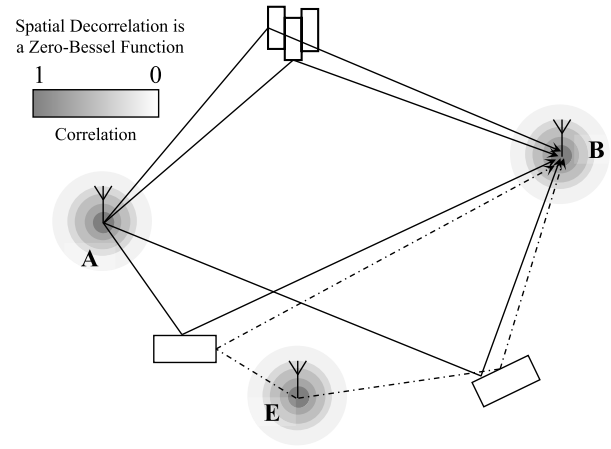



**Fig. 10.** Spatial decorrelation representation between legitimate and wiretap channel.

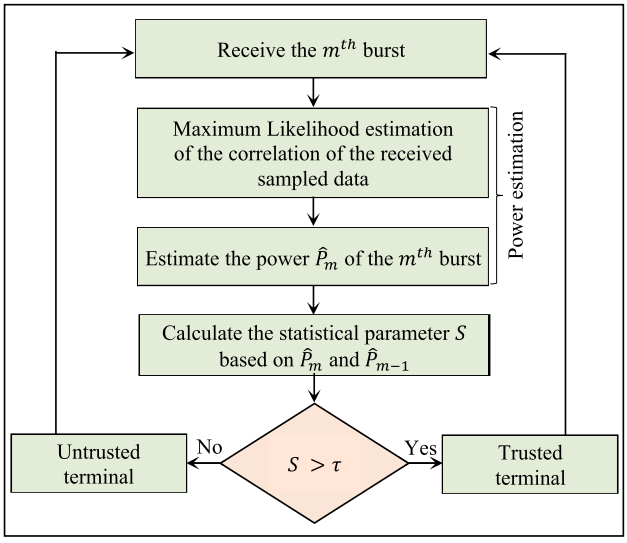



**Fig. 11.** Flowchart of the power delay profile-based implementation of the PHY-layer authentication method in [73].

introduced an authentication technique that leverages the correlation among power spectral density estimates, $S(f)$, obtained from a particular terminal at different time series. The method involves a binary hypothesis testing process represented by $H_0 : S_t(f) = S_{A\to B}(f)$ and $H_1 : S_t(f) \neq S_{A\to B}(f)$. The authors estimated the power spectral density using the Daniell method [87] and optimised the threshold value and the probability of false alarm ($P_{fA}$) for a generalized likelihood ratio test (GLRT), where $P_{fA}$ is the probability that a third party is authenticated as an authorised terminal. Chin et al. [73] have utilised the concept of employing the power delay profile as a proficient PHY-layer authentication mechanism to differentiate between two consecutive bursts $\{m-1, m\}$ in mobile orthogonal frequency division multiplexing (OFDM) system. The study formulates the PDP $\{\hat{P}_{m-1}, \hat{P}_m\}$ of different bursts based on the cyclic prefix (CP) length and the number of subcarriers ($N$). Fig. 11 depicts the flowchart of the method proposed in [73], which employs the statistical parameter $S$ to make a trustworthy decision. The parameter $S$ is determined by calculating $\{\hat{P}_{m-1}, \hat{P}_m\}$, and then compared to $\tau$. The results indicated that as the value of $\tau$ increases, the false alarm probability decreases and vice versa.

For improved performance, Liu et al. [74] presented a novel two-dimensional (2D) quantisation method $\{Q_h, Q_d\}$ that employs the channel amplitude ($\hat{h}_l(n)$) and path delay ($\hat{d}_l(n)$) estimates of the $l^{th}$ multipath component to distinguish between trusted and untrusted terminals

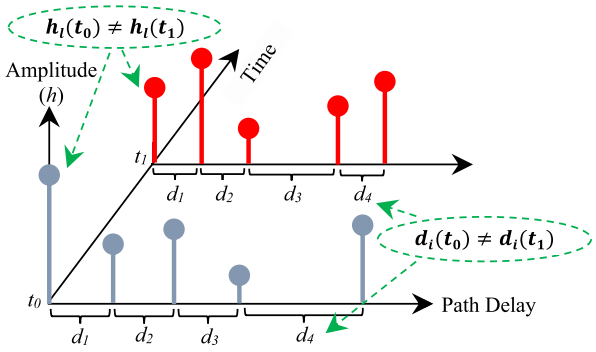



**Fig. 12.** Channel variations (amplitude & phase) over time [74].

based on the spatial and temporal variations in transmission across different time intervals $\{n, n+1\}$. Fig. 12 illustrates the changes in the $\hat{h}_l(n)$ and $\hat{d}_l(n)$ components across various time slots. The decision rule is determined based on the following hypothesis:

$$\begin{aligned} H_0 &: S = S_h + S_d \leq \tau, \\ H_1 &: S = S_h + S_d > \tau \end{aligned} \tag{1}$$

where $S_h$ and $S_d$ are given by

$$\begin{aligned} S_h &= \sum_{l=0}^{L-1} Q_h \left[ \left| \hat{h}_{X,l}(n+1) - \hat{h}_{A,l}(n) \right|^2 \right], \\ S_d &= \sum_{l=1}^{L-1} Q_d \left[ \left| \hat{d}_{X,l}(n+1) - \hat{d}_{A,l}(n) \right| \right] \end{aligned} \tag{2}$$

where $L$ is the total number of channel paths, and $\{\hat{h}_X, \hat{d}_X\}$ are the channel amplitude and path delay estimates from a specific terminal $(X)$ at time $(n+1)$ while $\{\hat{h}_A, \hat{d}_A\}$ are that of a pre-authenticated terminal $(A)$ at time $n$. The null hypothesis $H_0$ means $X = A$ while $H_1$ means $X \neq A$.

In [75], Liu et al. proposed an amplify-and-forward cooperative relaying technique for end-to-end (E2E) transmission aimed at enhancing the wireless communication range, as shown in Fig. 13. The proposed method optimises the selection of the best cooperative relay $(R_i)$ from a set of $M$ relays, by maximising the signal-to-noise (SNR) for E2E communication $(Alice \rightarrow R_i \rightarrow Bob)$ through each of the relays $\forall R_i \in \{R_1, \ldots, R_M\}$. Furthermore, the authors presented a PHY-layer authentication mechanism that utilises the short-term channel correlation between consecutive E2E transmissions that pass through the selected best relay.

In the context where a source node (Alice) communicates with a legitimate user (Bob) in the presence of passive eavesdropping (Eve), a technique known as cyclic redundancy check (CRC) is employed to encode information data bits. Upon transmission of the encoded data to Bob, the latter carries out a CRC decoding process and sends a retransmission request indicating whether the decoding was successful or not. Alice may repeat the transmission process until Bob exhausts the maximum number of retransmissions $(L)$ or receives the transmitted packet successfully. This technique is commonly referred to as automatic repeat request (ARQ). To enhance the security of this method, Hamamreh et al. presented a technique in [76] that combines the artificial noise (AN) cancellation process with the use of maximal ratio combining (MRC) at the receiver terminal. The MRC process merges two consecutive retransmitted data packets (i.e., $L = 2$) to eliminate the effect of the AN on the intended receiver's side. The security strength of this approach relies on the complexity involved in Eve's ability to eliminate the added AN. This is because the AN is produced at the transmitter's side based on the channel reciprocity between legitimate terminals (i.e., $Alice \leftrightarrow Bob$).

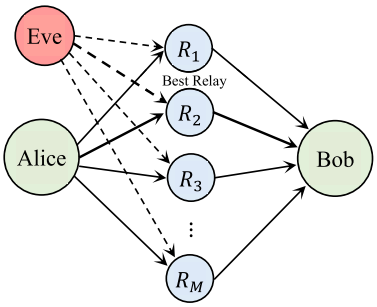



**Fig. 13.** Relay selection for cooperative relaying using amplify and forward method [75].

In [77], Liao et al. proposed a deep learning (DL)-based authentication method for industrial wireless sensor nodes that adopts three alternative algorithms, deep neural network (DNN), convolution neural network (CNN), and improved convolution pre-processing neural network (CPNN). Fig. 14 presents the flowchart of this technique comprising three phases, initialisation, authentication, and retraining. During the initialisation phase, the kernels are trained using CSI data obtained from different nodes. In the subsequent authentication phase, the upcoming CSI is verified, and the dataset is retrained for the next iteration.

The WSN is vulnerable to intelligent attackers who can imitate legitimate channel information through beamforming techniques. These attackers leverage machine learning, such as Q-learning, to select attack actions based on the communication channel and maximise long-term cumulative rewards. To mitigate such attacks on a network comprising $M$ nodes, $\{n_1, \cdots, n_M\}$, Gao et al. [78] proposed a cooperative PHY-layer authentication approach. In this method, an intelligent attacker attempts to mimic the channel and transmit a signal to a sensor $n_i \in \{n_1, \cdots, n_M\}$. Each sensor in the network measures the power of the received signal $\psi(y_i)$, for $i = \{1, \cdots, M\}$. In the presence of an attack, both the attacker and the sink node coexist, resulting in a larger received power than usual. Notably, the higher the power of the deceptive signal, the greater the risk of the attack being detected. Therefore, there exists a tradeoff between transmit power and the detection probability of local observation. Finally, each sensor transmits messages to its neighbours based on $\psi(y_i)$, updates the final message (belief), and tests whether it exceeds the threshold value (belief threshold). The flowchart illustrating this method is presented in Fig. 15.

Li et al. [79] introduced a PHY-layer authentication framework that employs an area-based approach for detecting spoofing attacks. The proposed framework classifies the area surrounding the destination terminal, represented by the symbol ★ in Fig. 16. The legitimate area is defined as the region bounded by distances $[d_i, d_0]$, where the legitimate terminal (•) is positioned far from the destination point with distance $d_{LR}$, and the spoofing attacker (■) is located at a distance $d_{AR}$. This method involves the definition of a silent probability. Specifically, when the spoofer is located far away from ★ or the spoofing power is small, the attacker is more likely to keep silent. Hence, the surrounding area of ★ is categorised into three areas:

1. The clear area, where the spoofer has no opportunity to construct an attack due to the high probability of detection (i.e., the silent probability is larger than a threshold $\epsilon_1$; e.g. 90%).
2. The danger area consists of locations where the spoofer can achieve a relatively higher successful spoofing probability larger than a threshold $\epsilon_A$ (e.g., 10%).
3. The warning area is the region where a legitimate terminal should not be located, as it can be classified as a spoofer (i.e., high probability of false alarm).

The boundaries of each region are allocated based on the RSS while the threshold values are chosen to meet practical specifications and de-

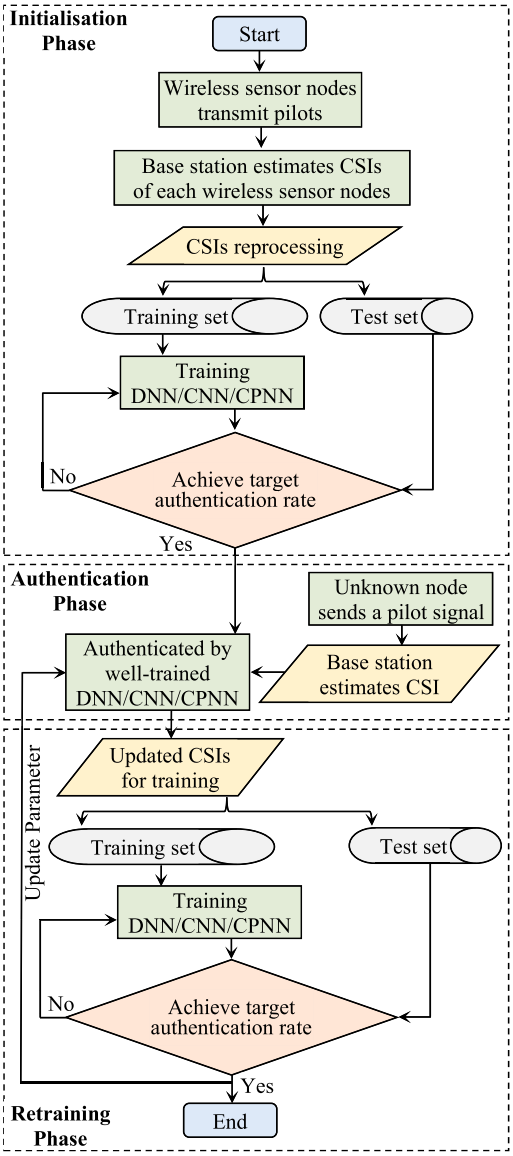



**Fig. 14.** Flowchart of the deep learning-based authentication [77].

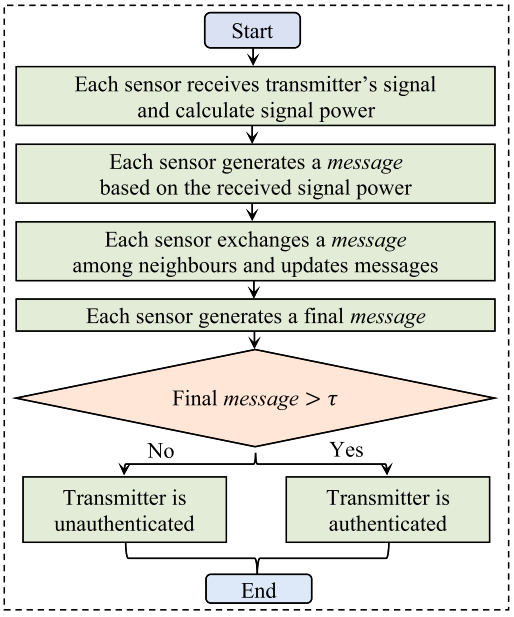



**Fig. 15.** Flowchart of the cooperative PHY-layer authentication [78].

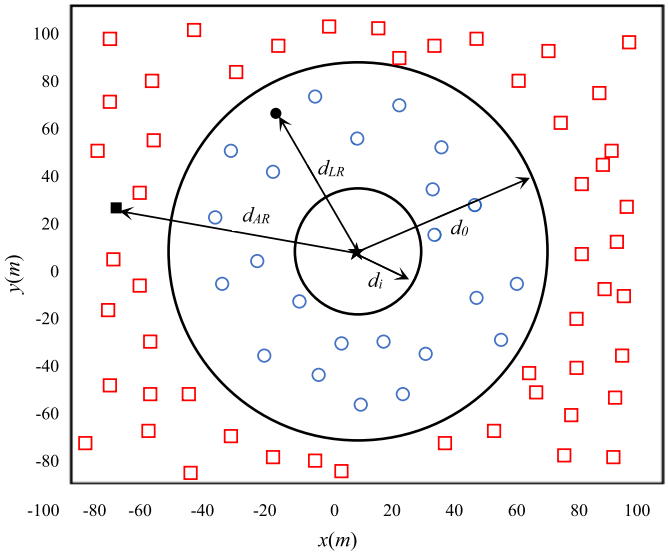



**Fig. 16.** Area authentication model [79].

mands. The probability of a successful attack increases as the legitimate user approaches the inner and outer boundaries. This framework offers an effective solution for detecting spoofing attacks and enhances network security.

The channel randomness and the short-term reciprocal features can be exploited to extract a high entropy secret key. By exchanging probing packets and quantising the resulting channel estimates, two communicating terminals can establish a symmetric shared key. However, the imperfect channel reciprocity can introduce discrepancies in the extracted key, requiring subsequent information reconciliation and privacy amplification stages. Jadoon et al. [80] proposed a Hopper-Blum-based PHY-layer (HB-PL) authentication scheme that excludes the information reconciliation and privacy amplification stages. The extracted information is used as an input secret key for the HB protocol used for authentication. The authors estimated the percentage of successful authentication for varying numbers of exchange probing packets and compared the results with the traditional cascade scheme using MATLAB simulations. The simulations showed that the HB-PL scheme achieves a 95% authentication rate with 55 exchange probing packets, while the cascade scheme required 65 exchange probing packets to achieve a 90% authentication rate. The proposed HB-PL scheme offers a more efficient and simplified approach for PHY-layer authentication in wireless communication systems.

#### 4.1.2. *Hardware imperfections-based PHY-layer authentication*

Hardware imperfections-based authentication is an innovative technique for enhancing wireless communication security. This approach leverages the intrinsic imperfections inherited in the hardware components of wireless devices for authentication purposes. These imperfections can be a result of manufacturing variations, such as the CFO [81] and AFE imperfections [82]. This method involves the measurement and characterisation of these imperfections using signal processing techniques and machine learning algorithms to establish unique hardware signatures, which can then be used to authenticate legitimate users and devices. In the work introduced by Zhang et al. [81], radio frequency fingerprinting (RFF) is employed to differentiate between various terminals in IoT devices. The received signal is partitioned into samples, and the primary features can be extracted as follows:

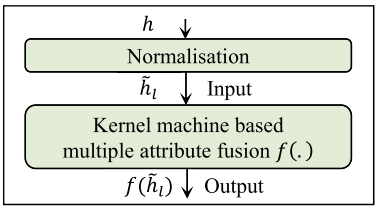



**Fig. 17.** Kernel machine-based multiple PHY-layer channel attributes [83].

1. *Transient part*: The turn-on transient part of the signal can be identified by the authenticator during frequency synthesis when the frequency synthesizer synchronises with the user's assigned transmission frequency.
2. *Near transient part*: This feature includes both the turning on transient and stable segments of the signal.
3. *Preamble part*: The unique hardware features can be extracted from the preamble segment of the signal by calculating its power spectral density and analysing its frequency and phase attributes to generate the RFF.
4. *The entire signal*: The frequency, phase, amplitude, and in-phase/quadrature (I/Q) samples can be analysed across the entire signal to extract RFF features.
5. *RF burst*: RF identification-based systems can use the out-of-band emissions from a sinusoidal carrier outside its centralised frequency to obtain a distinct hardware fingerprint.

The feature vector of $N$ devices is represented by $V = \{v_1, v_2, \ldots, v_N\}$. The classifier is trained to obtain the function $(\phi)$, which represents the feature space of $N$ users, such that $C = \phi(V)$, where $C = \{c_1, c_2, \ldots, c_N\}$ is the class space. The decision rule is taken based on the scoring function $s : V \times C$. If the scoring value of $(v_i, c_i)$ is greater than $\tau$, then the person is considered an authorised terminal. Otherwise, the terminal is unauthorised.

The CFO is another distinctive PHY-layer attribute, in which, radio frequency (RF) oscillators of each pair of communication terminals can be relatively biased to the central oscillating frequency in addition to the Doppler shift induced by the mobility terminals. In a study conducted by Hou et al. [82], a Kalman filter is employed to predict the current CFO value using previous CFO variations and a training sequence. The decision rule involves a binary hypothesis testing problem, where the current CFO estimate is compared to the predicted Kalman CFO.

#### 4.1.3. Multiple attributes-based PHY-layer authentication

For improved authentication performance, a combination of multiple PHY-layer features can be used for discriminating between different geographically located terminals. Fang et al. [83] proposed an authentication technique that leverages machine learning and $N$ number of multiple channel attributes. This technique utilises different attributes, such as the RSS, CFO, and CSI, among others. The normalisation process for each channel attribute is done using the maximum and minimum range of each attribute's observations. A training set of observations is utilised to train the authentication step. The Gaussian kernel function $f(.)$ is employed to model the authentication process, as illustrated in Fig. 17. The authors measure the mean square error (MSE) versus the iteration index for different combinations of attributes {CFO, CIR, RSS, CFO & CIR, CFO & RSS, CIR & RSS, CFO & CIR & RSS}. The results show that the best authentication performance is achieved using all three attributes (CFO & CIR & RSS). Moreover, the evaluation of the MSE with respect to different numbers of attributes $(N = 1, 2, 3)$ indicates that increasing the number of attributes leads to a decrease in the error rate. The security strength of this technique lies in the difficulty of an adversary to forge the correct observations of all three attributes, which enhances the security of the authentication process.

Wang et al. [84] proposed a multi-attributes multi-observation (MAMO) authentication mechanism that combines the RSS estimation and I/Q amplitude and phase shift imbalance (IQI) for both stationary and mobile device scenarios. The proposed method employs three antennas to obtain multiple observations, which enhances the reliability of the authentication mechanism by estimating the MRC for multiple channels. To evaluate the performance of the authentication techniques, the receiver operating characteristics (ROC) curves (probability of detection $P_d$ versus probability of false alarm $P_{fa}$) are evaluated using MATLAB simulations for three methods, namely, IQI&RSS-MRC, IQI-MRC, and IQI-Non-MRC. The results indicated that the MAMO technique achieves superior performance, 50.48% and 9.28%, compared to the IQI-Non-MRC and IQI-MRC, respectively.

Li et al. [85] developed a software-defined radio (SDR) platform-based PHY-layer authentication mechanism for 802.11 a/g networks. The channel characteristics are extracted from the 802.11 frames using the following methods:

1. The CSI is calculated from the long training sequence (LTS). A vector of 52 samples is generated to estimate the CSI of the current frame, and changes are estimated by comparing the pre-stored and received values of the LTS.
2. The RSS is obtained from the power values of the short training sequence (STS) as it is considered to be fixed across different frames.
3. The frequency offset is measured from the last 64 samples in the STS, and the previous samples are discarded to avoid the effect of automatic gain control (AGC) adjustment.
4. The timestamp is estimated using a 64-bit counter that is incremented every clock cycle.

The TickSEC platform, which includes an embedded MicroBlaze processor is used to evaluate the detection rates of Wi-Fi devices using different machine learning models, such as linear regression, decision tree, and support vector machines. The detection rates ranged from 96.8% to 98.48%.

Ramabadran et al. [86] propose a scheme to generate a shared key between two nodes $(1, 2)$ for phase encryption of modulated signals, taking into account circuit impairments. The key generation process is based on the CIR and is explained as follows.

1. *Step 1*: Node-1 sends a predefined probe signal $y(n)$ to Node-2, and the received signal $r_2(n)$ combines the hardware frequency response $h_{11}(n)$ of Node-1 with the CIR $h_{12}(n)$. The received signal in the frequency domain is given by

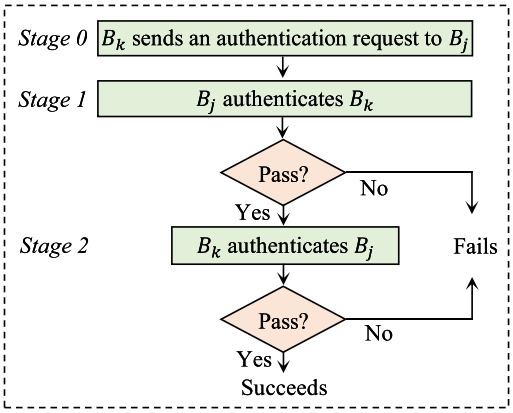
$$R_2(j\omega) = Y(j\omega)H_{11}(j\omega)H_{12}(j\omega) \tag{3}$$

   The obtained $R_2(j\omega)$ is then multiplied by its hardware frequency response $h_{22}(n)$, resulting in the final estimate $E_2(j\omega)$, denoted by

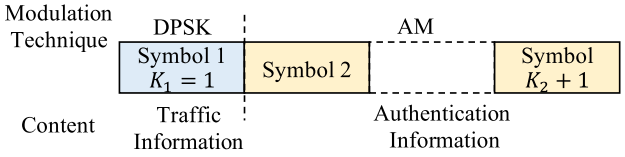
$$E_2(j\omega) = \frac{R_2(j\omega)}{Y(j\omega)} H_{22}(j\omega) = H_{11}(j\omega)H_{12}(j\omega)H_{22}(j\omega) \tag{4}$$

   This process is repeated to estimate $E_1(j\omega)$ of Node-1 within $T_c$, such that $H_{12}(j\omega) \simeq H_{21}(j\omega)$. Despite the added noise and hardware performance variations, the estimated $E_1(j\omega)$ is highly correlated with $E_2(j\omega)$, which is quantised to extract the shared key.
2. *Step 2*: The transmission of modulated signals involves the encryption of the phase component at the transmitter side and its subsequent decryption at the receiver side. The encryption and decryption processes rely on the use of a non-linear function, which is predetermined and applied on both sides. The non-linear function is a critical component to generate the encryption and decryption phase values, given by

$$y = x^3 + f_1 x + f_2 \bmod f_3 \tag{5}$$




(a) Flowchart of the mutual authentication.




(b) Frame structure of the authentication process.

**Fig. 18.** The flowchart and frame structure of the keyed PHY-layer authentication method in [88].

where the prime coefficients $(f_1, f_2, f_3)$ of the non-linear function are selected randomly from the extracted shared key, which is periodically updated to avoid brute force attacks. Finally, the encryption phase values are added to the modulated signals' phases.

The extracted key is tested for symmetry. In addition, the proposed scheme is evaluated through experiments on an SDR testbed. The results demonstrate the effectiveness of the proposed scheme in detecting unauthorised devices.

### 4.2. Keyed PHY-layer-authentication

This authentication method works by using a secret key that is shared between the communicating wireless devices and the physical characteristics of the wireless channel. The key is used to authenticate the identity of the wireless device during the initial connection setup. Shan et al. [88] proposed a physical layer challenge-response authentication mechanism (PHY-CRAM) for wireless networks, which is a one-way or mutual authentication scheme for an OFDM system with $N$ subcarriers. The scheme utilises either stage 1 alone or stages 1 and 2 in combination, as illustrated in the flowchart presented in Fig. 18(a). The frame structure consists of $k_1$ and $k_2$ symbols, as shown in Fig. 18(b). The first $k_1$ symbols contain traffic information, which is modulated using differential phase shift keying (DPSK), while the following $k_2$ symbols are used for authentication based on the symmetric key pair $\{X_j, X_k\}$ and the random values $D_n$. The authentication process is carried out between two legitimate terminals, $B_j$ and $B_k$, and can be summarised as follows.

1. *Stage 0*: To maintain the secrecy of the CSI, $B_k$ sends an authentication request to $B_j$ using random amplitude subcarriers.
2. *Stage 1*: $B_j$ generates random values $D_n$ within the range of $[k_3, k_4]$, where $0 < k_3 < 1 < k_4$. These random values are used to amplitude modulate the last $k_2$ symbols, which are then sent to $B_k$. Based on the received signal $R^{(1)} = D_n H_{jk} + W_n^{(1)}$, $B_k$ calculates and sends $T^{(1)} = \frac{\mathcal{M}(X_k)}{D_n H_{jk} + W_n^{(1)}}$ to $B_j$, where $\mathcal{M}(.)$ represents the mapping function, $H_{jk}$ is the wireless channel response from $B_j$ to $B_k$, and $W_n^{(1)}$ is the added noise at the receiver side.
3. *Stage 2*: $B_j$ receives $R^{(2)} = \frac{\mathcal{M}(X_k) H_{kj}}{D_n H_{jk} + W_n^{(1)}} + W_n^{(2)}$, where $H_{kj}$ represents the wireless channel response from $B_k$ to $B_j$. Due to channel reciprocity ($H_{kj} \approx H_{jk}$) within $T_c$ and neglecting the noise, it follows that $R^{(2)} = \frac{\mathcal{M}(X_k)}{D_n}$. Finally, $B_j$ performs binary hypothesis testing based on the pre-agreed shared key $X_k$ and $D_n$ to authenticate $B_k$.

This mechanism has been implemented and evaluated using a field-programmable gate array (FPGA) in both urban and rural channels. The ROC has been measured for various values of SNRs including 10, 15, and 20 dB, and key lengths of 40 and 60 bits. The evaluations have been carried out for line-of-sight (LoS) scenarios at different distances of 3, 6, and 28 meters, as well as for non-line-of-sight (NLoS) scenarios at a distance of 6 meters. The results show that increasing the key length and SNR leads to better ROC values. The worst performance is observed at an SNR of 10 dB for the NLoS scenario and LoS with a distance of 28 meters.

In [89], a novel PHY-layer challenge-response authentication scheme (PHY-PCRAS) is proposed for a multi-carrier communication system with $N$ subcarriers. The scheme utilises the short-term reciprocal features of the channel phase response to generate the response signal corresponding to the received challenge. This scheme facilitates mutual authentication between two parties, Alice and Bob, who have previously agreed upon a shared key denoted by $(k_A, k_B)$. For a one-way authentication, Alice sends an initial challenge-modulated sinusoidal signal to Bob. Subsequently, Bob computes the phase difference estimate of the $i^{th}$ subcarrier denoted by $\Delta\theta_{i1} = \theta_i - \theta_1$, $\forall i \in \{1, \cdots, N\}$, where $\theta_i$ represents the estimated channel phase response of the $i^{th}$ subcarrier. Then, Bob replies to Alice's challenge by encapsulating the mapped key $k_B$ into the phase of the response signal, masked by the computed $\Delta\theta_{i1}$. Leveraging the channel reciprocity, the response signal is equalised at the side of Alice. Subsequently, Alice verifies the received signal by performing binary hypothesis testing, using the shared key $k_B$ as a reference for authentication.

In a similar way, Cheng et al. [90] introduced a secret key extraction mechanism at the physical layer. This mechanism involves extracting a preliminary key, which is subsequently employed for authentication purposes based on the reciprocal features of the channel phase response. The study evaluates the ROC under varying numbers of subcarriers $N = \{16, 32, 64, 128\}$ at a SNR of 5 dB. The results demonstrate a positive correlation between ROC performance and $N$, with near-ideal performance observed when $N = 32$ subcarriers and SNR = 5 dB. Furthermore, the scheme introduced in [90] demonstrates better performance than PHY-CRAM [88] and similar performance to PHY-PCRAS [89].

### 4.3. Tag-based PHY-layer-authentication

The principle behind tag-based PHY-layer authentication involves superimposing a secret modulated signal into the transmitted signal, which acts as a signal watermark. The study conducted by Ran et al. [91] proposes a method for implementing tag-based PHY-layer authentication by inserting a tag signal $(t_i)$ into the transmitted signal $(x_i)$. The tag is generated using a hash function $g(.)$, which takes into account both the channel gain $(H_i)$ and the message contents $(s_i)$ as inputs, resulting in $t_i = g(s_i, H_i)$. The tag is then combined with the transmitted message by padding it, such that $x_i = \rho_s s_i + \rho_t t_i$, where $\rho_s$ and $\rho_t$ represent the allocated energy to the message and tag, respectively. Additionally, $\rho_s^2 + \rho_t^2 = 1$, and $0 < \rho_s, \rho_t < 1$. At the receiver end, the estimated channel gain $(H_i')$ is used to compute the receiver's tag value $(t_i')$, which is then compared with the transmitted tag using the cost function $f_c(t_i, t_i')$ to make a decision. Simulation results showed that increasing the SNR value led to a decrease in the bit error rate (BER)

and an increase in the authentication rate, and vice versa. The simulation is conducted with varying SNR values (ranging from 0 to 12 dB) and with 40% of the transmitted signal being tagged. The results also showed that increasing the energy allocation of the tag led to a decrease in the BER.

The tag-based authentication method proposed by Zhang et al. [92] involves embedding an encrypted tag signal into the message signal using an asymmetric encryption scheme. The reference tag signal of each terminal is shared with the access point (Bob) through a secured channel. Public and private keys with low key space are computed for network terminals, after which the reference tag is encrypted using a hash function and Alice's private key to generate the cover tag. The cover tag is then embedded into the 16-QAM modulated signal. In the tag verification process, the estimated tagged signal is decrypted, allowing Bob to authenticate the sender under binary hypothesis testing.

Zhang et al. [93] proposed a novel Gaussian tag-embedded authentication (GTEA) scheme utilising the weighted fractional Fourier transform (WFRFT) to generate the tag signal. The Gaussian distribution of the embedded tag signal provides an additional layer of security as it appears as random noise to unauthorised terminals. The effectiveness of the GTEA scheme is evaluated through simulations where both the message bit error rate (MBER) and tag bit error rate (TBER) are measured across varying SNR values ($0 \rightarrow 40$) dB and signal-to-tag power allocation ratio (STR) values ($0 \rightarrow 40$). Results show that increasing the STR leads to a decrease in MBER and an increase in TBER for a fixed SNR value. Similarly, for a fixed STR, an increase in SNR value leads to a decrease in MBER and TBER, ultimately improving the authentication performance.

### 4.4. Challenges of PHY-layer authentication

This section discusses performance limitations associated with each type of PHY-layer authentication. The challenges related to single attribute-based authentication can be summarised as follows: Firstly, this technique is hindered by a low probability of detection when there are significant channel variations and low SNRs. As a result, it may not be practical for applications that have limited resources or are required to cover long distances. Secondly, observing the wireless channel attributes of all the relevant terminals within a limited time period $T_c$ is a challenging task, especially for applications that are highly dynamic or densely populated. Finally, initial identity verification of the corresponding terminal is still necessary based on existing cryptographic protocols to identify its legitimacy and extract its unique features. Authentication based on hardware imperfections suffers from a notable weakness wherein the extracted features from different devices exhibit slight variations, potentially resulting in false decision-making. Moreover, these features are susceptible to instabilities caused by factors such as voltage supply fluctuations, temperature variations, and electromagnetic interference. As a consequence, the reliability and accuracy of such authentication methods can be compromised, necessitating robust techniques to address these challenges effectively.

Multiple attributes-based authentication poses several challenges that require careful consideration. Firstly, machine and deep learning-based techniques encounter significant performance limitations due to the inherent complexity of these techniques. Specifically, the training of kernels and neurons requires the use of large datasets, which is not feasible in VANET applications. Secondly, each terminal in the network must be pre-registered to extract its distinctive features for supervised authentication approaches. Keyed authentication requires the presence of a pre-agreed shared key between the communicating terminals. Furthermore, the establishment of this shared key requires an initial identity verification of the corresponding terminal, which is accomplished through existing cryptography-based authentication schemes. Tag-based authentication introduces a significant tradeoff between decoding performance and security, particularly under varying signal-to-tag power allocation ratios. Moreover, to ensure the legitimacy of the communicating terminal and agree on a secret tag, initial identity verification is still necessary, which is performed through existing cryptographic protocols.

Table 6 presents a concise summary of the problem statement and limitations associated with various types of PHY-layer authentication. In summary, PHY-layer-based authentication cannot provide a comprehensive alternative solution, as initial identity verification of the corresponding terminal is still necessary to authenticate the legitimacy of the terminal and extract its unique features or establish a symmetric shared key using existing cryptographic protocols. However, these methods can serve as an integral component in the broader context of cross-layer authentication, as discussed in the subsequent section.

## 5. Cross-layer authentication

This method involves an initial mutual authentication between authorised parties using crypto-based authentication methods described in Section 3. Subsequently, the re-authentication process is conducted at the physical layer, utilising the authentication techniques outlined in Section 4. It is crucial to note that the initial legitimacy verification is a crucial step in extracting secret features or establishing a symmetric key for the PHY-layer re-authentication process.

Wen et al. [25] patented a novel cross-layer authentication technique. This method involved employing PKI-based authentication during handshaking, alongside the generation of a radio frequency fingerprint for subsequent re-authentication. Another approach was proposed by Althunibat et al. [94], which presented an integration method for mobile multiple-input multiple-output (MIMO) systems. In their method, they initially utilised PKI-based authentication and then the feature tracking method for re-authentication. For improved performance, Wang et al. introduced a solution in [95] that incorporated the adaptive Kalman filter. This filter was employed to predict upcoming CSI and RSS based on previous estimations and then compared them with real-time observations in a 2D hypothesis testing problem. Alternatively, Yang et al. [96] proposed a cross-layer approach for mobile communications. Their work involved masking the PHY response by leveraging the channel frequency response between the user terminal and the base station. This was achieved using a fault-tolerant hashing technique. However, the authors did not calculate the computation time needed for the response signal generation and compare it to the minimum coherence time of the maximum speed limit of the communicating vehicle, which is essential to ensure short-term channel reciprocity between communicating terminals. Gope et al. [97] proposed an approach for incorporating the integrated circuits (ICs) physically unclonable function (PUF) into a pseudo-ID-based authentication. Based on the ICs' physical variation ($P$), the PUF method effectively generates an unpredictable response $R = P(C)$, where $C$ is the input challenge.

Other cross-layer techniques have been proposed for enhancing the security of wireless communication systems. One such approach involves the integration of cryptographic-based methods with PHY-layer-based methods in diverse ways. Zenger et al. [98] introduced a novel technique in situations where computational capabilities are limited. This technique involves two distinct authentication phases, referred to as Phases I and II. In Phase I, authentication is dependent upon channel characteristics, specifically, the high correlation coefficient observed between channel estimates of different terminals $h_{B\rightarrow A}(t) \approx h_{C\rightarrow A}(t)$, where $A$ is the access point, $B$ is the authenticated node, and $C$ is the unauthenticated node. This correlation coefficient is observed when the distance between nodes $B$ and $C$ is less than or equal to $\lambda/2$, as depicted in Fig. 19. The delegation of trust between entities ($B$) and ($C$) is examined in the context of their proximity to each other within the vicinity zone and upon receipt of a command by the user. Phase II involves the use of a PHY-layer key extraction method to generate a shared key that can be utilised for cryptographic purposes at the upper layers.

Chen et al. [99] introduced a novel authentication scheme, referred to as clustering-based PHY-layer authentication scheme (CPAS).

**Table 6**
Challenges and limitations of PHY-layer authentication.

| No. | Problem Statement | Method | Limitations |
|---|---|---|---|
| [71] | Crypto-based authentication ignores the channel's unique features, which hinders attack detection and key management at the physical layer. | Single attribute based authentication | 1- The application of this method becomes unfeasible in scenarios with significant channel variations and low signal-to-noise ratios due to its limited detection probability. This drawback hinders its usability in resource-limited and long-range settings.<br>2- For dynamic and high-density use cases, it becomes impractical to extensively monitor all related terminals to gather their wireless channel characteristics within the time frame $T_c$.<br>3- To establish the legitimacy of the corresponding terminal and extract its unique features, initial identity verification is essential, and this can be achieved through existing cryptographic protocols. |
| [72] | Cryptographic techniques are inadequate in providing a comprehensive defence against malicious attacks, particularly in wireless communication channels. | | |
| [73] | Current security techniques fail to account for the channel temporal variations, which can serve as a valuable security resource and are difficult to replicate. | | |
| [74] | Crypto-based methods incur high computation and communication overheads. | | |
| [75] | Spoofing attacks pose a significant threat and traditional methods are computationally expensive and resource-intensive. | | |
| [76] | Traditional authentication schemes include complex key distribution and management processes, large key lengths, and high computation complexity. | | |
| [77] | Deep neural and convolution neural networks cannot provide low latency and high authentication rates with few hidden layers. | | |
| [78] | Intelligent attackers can mimic the CSI using beamforming. An attacker uses machine learning to maximise long-term reward accumulation by taking an attack action. | | |
| [79] | Existing authentication schemes are an effective security solution, but detection accuracy decreases on high-mobility terminals and massive connections. | | |
| [80] | PHY-layer secret key generation extracts a shared key between nodes. However, the information reconciliation corrects mismatched bits through public channels, posing an immense threat. | | |
| [81] | Traditional authentication methods are not practical for very small, low-cost, and resource-constrained devices. Therefore, the need for a lightweight authentication scheme is high-priority to address these limitations. | Hardware imperfections based authentication | 1- This method is susceptible to false decision-making due to the slight variations in extracted features across different devices.<br>2- Additionally, these features are prone to instability caused by voltage fluctuations and electromagnetic interference. |
| [82] | Cryptographic authentication is processed at the upper layers without configuring the physical layer attributes, which is an effective authentication resource. | | |
| [83] | Multiple attributes-based PHY-layer authentication requires high computation complexity. Additionally, sophisticated adaptive techniques must be used to detect any disclosure within $T_c$. | Multiple attributes based authentication | 1- The implementation of machine/deep learning methods presents a constraint on performance, primarily stemming from the requisite utilisation of extensive datasets to train kernels/neurons.<br>2- In the network's operational framework, prior registration of each terminal is imperative to extract its unique characteristics, a necessary step for deploying supervised authentication methods.<br>3- Despite leveraging existing cryptographic protocols for authenticity verification, the initial identity validation of the respective terminal remains a crucial requirement. |
| [84] | Low reliability of channel-based PHY-layer authentication due to signal quality fluctuation. In addition, frequent authentication handovers degrade 5G communication system performance. | | |
| [85] | In Wi-Fi applications, extracting channel features without affecting communication performance, and providing lightweight authentication are considered challenging. | | |
| [86] | The open nature of wireless networks leaves the nodes open to traffic analysis and interception by eavesdroppers and man-in-the-middle platforms. | | |
| [88] | Conventional authentication requires high computation and storage capacity which is not suitable for resource-constrained applications. | Keyed authentication | 1- The establishment of a pre-agreed shared key remains a fundamental requirement between terminals.<br>2- Furthermore, to ensure legitimacy and facilitate the creation of a symmetric key, an initial identity verification for the corresponding terminal is necessary using existing cryptographic protocols. |
| [89] | Wireless communication through open networks is vulnerable to spoofing attacks where an attacker impersonates a legitimate party. | | |
| [90] | PHY-layer key extraction suffers from low key generation rates due to diverse extraction steps. In addition, the extracted keys have low entropy because of minimal channel variations. | | |
| [91] | Traditional cryptographic techniques suffer from high computation and complex key management. | Tag-based authentication | 1- The trade-off between decoding performance and security represents a significant concern, particularly when confronted with varying signal-to-tag power allocation ratios.<br>2- The initial authentication of the corresponding terminal's legitimacy and the agreement upon a confidential tag remain indispensable. This validation process relies on established cryptographic methods. |
| [92] | Many contributed tag-based authentication schemes cannot resist impersonation attacks as the computed tag signal depends on the message contents and is easy to forge by an adversary. | | |
| [93] | Lightweight cryptographic schemes are widely used in resource-constrained applications that cannot provide high levels of security against potential attacks. | | |

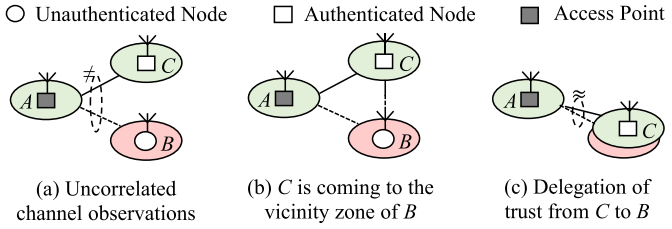



**Fig. 19.** PHY-layer authentication based on vicinity zone [98].

The proposed scheme is intended for two legitimate entities, namely Alice and Bob, who have a pre-established shared key ($key$). The cryptography-based authentication process comprises the following steps.

1. Alice generates a pseudorandom number denoted as $PS_1$, which is subsequently encrypted using a lightweight symmetric encryption algorithm, resulting in a cipher denoted as $\gamma_1 = E_{key}(PS_1)$. Alice sends the cipher to Bob, who extracts the CSI ($H_1$) and decrypts the cipher to obtain the original pseudorandom number as $PS'_1 = D_{key}(\gamma'_1)$. Bob then concatenates pairs of pseudorandom numbers, namely ($PS_2, PS_3$), with the original pseudorandom number $PS'_1$, resulting in a new sequence that is subsequently encrypted using a shared secret key, denoted as $\gamma_2 = E_{key}(PS'_1 \| PS_2 \| PS_3)$. The resulting cipher $\gamma_2$ is then transmitted back to Alice.
2. Upon receiving the encrypted message $\gamma_2$ from Bob, Alice decrypts the message using the shared secret key to obtain the concatenated sequence of pseudorandom numbers ($PS'_1, PS'_2, PS'_3$). To verify the authenticity of Bob, Alice tests whether the decrypted pseudorandom number $PS'_1$ obtained from $\gamma_1$ is equal to the original pseudorandom number $PS_1$. If Alice is confident in Bob's identity, she encrypts the pseudorandom numbers $PS'_2$ and $PS'_3$ using the shared secret key, resulting in two new ciphers denoted as $\gamma_3 = E_{key}(PS'_2)$ and $\gamma_4 = E_{key}(PS'_3)$. Alice subsequently sends the encrypted messages $\gamma_3$ and $\gamma_4$ to Bob.
3. Upon receiving the encrypted messages $\gamma_3$ and $\gamma_4$ from Alice, Bob decrypts the ciphers using the shared secret key to obtain the pseudorandom numbers $PS'_2$ and $PS'_3$, respectively. Bob then estimates the CSI for the newly established connection, denoted as $H_2$ and $H_3$. To ensure the legitimacy of Alice, Bob compares the decrypted pseudorandom numbers ($PS'_2, PS'_3$) with the original pseudorandom numbers ($PS_2, PS_3$). If the two sets of pseudorandom numbers are equal, it confirms the authenticity of Alice, and the communication between Alice and Bob can proceed securely.

The CPAS scheme comprises the following steps.

1. Bob obtains the CSI for the three connections, denoted as $H_1$, $H_2$, and $H_3$. To estimate the statistical characteristics of the channel, Bob accumulates the absolute values of the real and imaginary parts of each element estimated from the number of $m$ subcarriers and $n$ antennas. This process results in three new points denoted as $H'_1 = \{x_1, y_1\}$, $H'_2 = \{x_2, y_2\}$, and $H'_3 = \{x_3, y_3\}$, as depicted in Fig. 20.
2. Using the estimated statistical characteristics $H'_l = \{x_l, y_l\}$, $\forall l \in \{1, 2, 3\}$, the central point $W_i(x, y)$, and the coverage area $dist_i$ are evaluated. The distance $dist_i$ is determined by adding the radius of the coverage area $R$ (see Fig. 20) to an adjusting parameter $\theta$.
3. To authenticate a terminal $k$, Bob calculates the Euclidean distance between the statistical information received from the terminal and the central point $W_i$ of the coverage area for each legitimate terminal $i$. The Euclidean distance is denoted as $\|H'_k\ W_i\|$. If $\|H'_k\ W_i\|$ is less than the distance threshold $dist_i$, then the terminal $k$ is authenticated as a legitimate device. Otherwise, $k$ is authenticated as an unauthorised device.

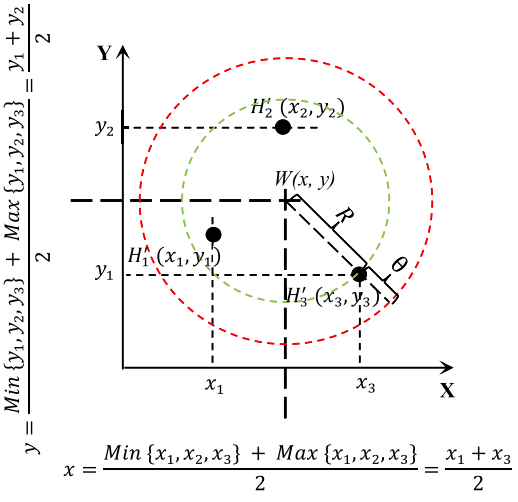



**Fig. 20.** Principle map of the PHY-layer channel observations in [99].

In case Alice fails to pass the CPAS scheme, the lightweight symmetric encryption scheme is executed as an alternative. Once a new terminal has passed the cryptographic scheme, it can be added to the network. Finally, the new central point $W_{new}\{x_{new}, y_{new}\}$ and coverage distance $dist_{new}$ are estimated for the newly added terminal.

Shawky et al. [23] presented a novel cross-layer approach that employs PKI-based authentication for the initial handshaking process and the establishment of a symmetric shared key, which is subsequently utilised in the message signing and verification phase. Within this phase, a PHY-layer signature is generated using the shared key and the message payload. Through comprehensive computational and communication evaluations, this method demonstrates significant cost-efficiency advantages, achieving reductions of approximately 94% and 77% in computation costs and 37% and 64% in communication costs when compared to the NERA [48] and CPPA [50] methods, respectively.

Reference [24] integrates pseudo-ID-based authentication for initial legitimacy detection and PHY-layer secret key generation for generating a shared key used for the PHY-layer re-authentication process. The re-authentication process is considered a keyed PHY-layer authentication that supports a high probability of detection $\geq 0.9$ at low false alarm probabilities $\leq 0.1$ under small SNR values $\geq 5$ dB. Furthermore, in the comprehensive comparison, the time required for verifying 1000 signatures in our scheme is improved by 71%, 97%, and 72% compared to ID-MAP [47] at the side of the proxy vehicle, NERA [48], and CPPA [50], respectively. Reference [24] introduces a novel integration of pseudo-ID-based authentication for initial legitimacy detection, along with PHY-layer secret key generation to establish a shared key for the PHY-layer re-authentication process. This re-authentication process operates as a keyed PHY-layer authentication, exhibiting a high probability of detection ($\geq 0.9$) with low false alarm probabilities ($\leq 0.1$) even under small SNR values ($\geq 5$ dB). Moreover, the proposed scheme demonstrates substantial improvements in the time required for verifying 1000 signatures. Specifically, compared to ID-MAP [47] when observed from the perspective of the proxy vehicle, the proposed scheme achieves an improvement of 71%. Furthermore, compared to NERA [48], and CPPA [50], the proposed scheme achieves even greater improvements of 97% and 72%, respectively.

In reference [26], two PHY-layer re-authentication mechanisms, namely PHY-layer signature-based identity authentication mechanism (PHY-SIAM) and PHY-layer feature tracking mechanism (PHY-FTM), are introduced. These mechanisms are designed to facilitate identity and integrity verification, respectively, thereby alleviating the significant costs associated with traditional cryptographic techniques. This work involves the development of an efficient Doppler emulator to

**Table 7**
Challenges and limitations of cross-layer authentication.

| Ref. | Problem Statement | Authentication Method | Limitations |
|---|---|---|---|
| [25] | High computation cost of the public key certification services for Wi-Fi network cards and RFID. | Utilising PKI-based authentication during handshaking and generating radio frequency fingerprints for re-authentication. | Unable to support high re-authentication performance for scenarios involving high mobility and significant channel variations, such as vehicular communication networks. |
| [94] | PHY-layer authentication lacks a high authentication rate in mobile MIMO systems. | PKI-based authentication initially and feature tracking for re-authentication. | Limited performance evaluation of real-time computation; adaptation in mobile environments. |
| [95] | FCC-assigned a limited bandwidth for V2X communication, needing reduced signature overhead. | Adaptive Kalman filter predicts CSI and RSS for 2D hypothesis testing. | Increased computational complexity; real-time adaptation challenges. |
| [96] | Multiple vulnerabilities exist in upper-layer cryptographic techniques, leaving them susceptible to active attacks. | Fault-tolerant hashing masks PHY response through channel frequency response. | Lack of computation time assessment for high-speed vehicular communication. |
| [97] | WSNs require secure and low-cost authentication for real-time data access, emphasising security and efficiency. | Utilising physically unclonable functions to create unpredictable responses in ICs. | Reliability dependent on slight variations of the IC characteristics. |
| [98] | Complex cryptographic operations are not a reliable security solution for resource-constrained applications. | Vicinity-based pairing using high correlation in channel estimates of terminals in close proximity. | Dependency on spatial closeness between authenticated and unauthenticated nodes. |
| [99] | Machine learning-based authentication methods require extensive channel data, making it impractical for real-time use. | Cryptographic scheme with pseudorandom numbers and CSI for authentication. | Need for accurate channel statistical analysis and computation of Euclidean distances for authentication. |
| [23] | High computation and communication costs of verifying and transmitting a crypto-based signature for each message transmission. | Generating PHY-layer signatures using shared keys for cost-efficient message signing and verification. | These schemes depend on the highly correlated and short-term reciprocity of channel phase responses between different terminals. Accordingly, accurate synchronisation among diverse terminals is essential for high performance. |
| [24] | | Integrating pseudo-ID-based authentication and PHY-layer secret key generation for re-authentication | |
| [26] | PHY-layer security assumes $\lambda/2$ spacing for channel decorrelation. In V2I, the attacker's distance $< \lambda/2$ causes highly correlated channels, comprising security. | Introducing PHY-layer re-authentication mechanisms (PHY-SIAM and PHY-FTM) to reduce computation and communication costs. | |

experimentally assess the re-authentication performance in a realistic vehicular wireless channel under various speeds and SNRs in a V2I scenario. The experimental measurements demonstrate the efficacy of the re-authentication algorithm in achieving high detection rates while maintaining low false alarm probabilities ($P_{fa} \leq 0.1$) for SNR values greater than or equal to 0 dB and transmitter speeds of up to 45 m/s. Table 7 presents a concise summary of the problem statement and limitations associated with the current state-of-the-art of cross-layer authentication.

In the context of VANETs, the integration of PHY-layer with upper-layer authentication is a critical consideration. The successful integration of these components must be both rational and practical, taking into account the application nature in terms of factors such as dynamicity, resource availability, broadcasting rate, and channel conditions. One of the key challenges in this regard is the selection of an appropriate re-authentication technique. This selection must be made with careful consideration of the aforementioned factors, as well as other relevant considerations such as security, privacy, and scalability. This study conducts comprehensive research on the available PHY-layer re-authentication techniques and their suitability for VANET applications. In addition, this work involves a detailed analysis of the strengths and weaknesses of different techniques, as well as an evaluation of their performance under various conditions.

## 6. 6G authentication: future insights

There is substantial potential for continued research and development in this domain. Several promising avenues for future investigation encompass the exploration of novel designs for adaptable cross-layer authentication schemes tailored to various applications of VENAT. The following subsections provide a concise introduction to these avenues.

### 6.1. Machine learning for adaptive authentication

In the realm of PHY-layer re-authentication, diverse methods have varying dependencies on SNR values for optimal performance. Tag-based approaches often demand higher SNR levels for effective functionality, while keyed PHY-layer authentication methods demonstrate resilience in lower SNR conditions. Conversely, cryptographic-based methods exhibit advantages in scenarios characterised by poor SNRs.

1. *Adaptive model selection*: Introducing a machine learning model to dynamically select the most appropriate re-authentication method based on estimated SNR values presents a promising solution. This adaptive approach aims to optimise authentication performance by intelligently choosing the most suitable technique during the initial time slot.
2. *Enhancing cross-layer adaptability*: The integration of machine learning models for cross-layer authentication could revolutionise how wireless systems handle varying SNR conditions. By leveraging historical data and real-time SNR estimations, these models can predict and select the most effective authentication method, ensuring robustness in diverse wireless environments.
3. *Challenges of model training*: However, challenges such as model robustness, data representation, and real-time adaptation need careful consideration. Ensuring that machine learning models are trained on comprehensive and diverse datasets, accounting for various SNR levels, is crucial for their reliability and adaptability.

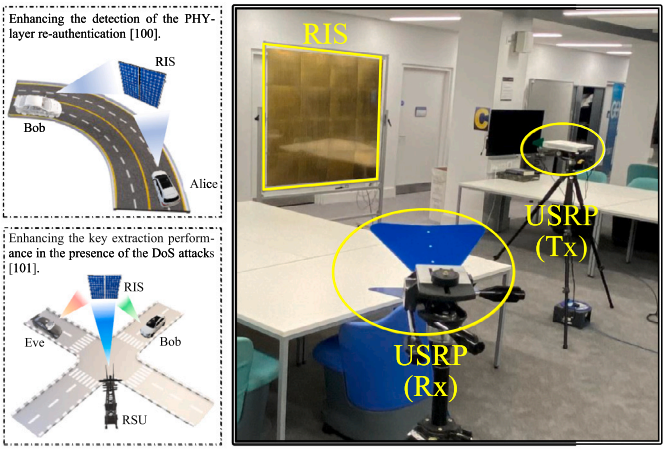



**Fig. 21.** RIS assisted communication security.

4. *Addressing contextual variability*: Additionally, the adaptability of such models in dynamically changing environments, characterised by SNR fluctuations and diverse wireless conditions, needs careful calibration. Model accuracy and efficiency in making real-time authentication decisions in such contexts remain key challenges.

By leveraging machine learning to dynamically select authentication methods based on estimated SNR values, the potential for robust, context-aware cross-layer authentication could be significantly enhanced, offering adaptability in the face of dynamic wireless conditions.

### 6.2. Reconfigurable intelligent surface for enhanced authentication

In the realm of PHY-layer re-authentication, the SNR value is a critical metric in determining detection probability while maintaining acceptable false alarm rates. Researchers have investigated RIS technology to optimise communication performance in wireless networks. These surfaces, comprising arrays of passive, tunable elements capable of manipulating electromagnetic waves by adjusting phase and amplitude, show promise in improving the re-authentication performance [100].

1. *Enhanced detection probability*: Incorporating RIS in re-authentication has shown significant improvements, as demonstrated in [100], see Fig. 21. Activating RIS with 4096 elements enhances the detection probability, increasing it from approximately 0.92 (without RIS) to around 0.99 for a false alarm rate of 0.2. This significant improvement underscores RIS technology's potential in shaping the future of cross-layer authentication.
2. Security enhancement: References [101,102] have delved into leveraging RIS to the PHY-layer secret key extraction, especially in the presence of DoS attacks. By manipulating signal strengths, RIS can strengthen designated users' received signals while diminishing potential attackers' reception. This approach improves key extraction metrics such as the secret bit generation rate (SBGR) and bit mismatch rate (BMR) under challenging SNR conditions. Specifically, the SBGR increases from 1.62 to 1.75 bits/sample when the RIS is activated, and the BMR decreases from 0.38 to 0.25 bits/sample under challenging SNR conditions of 0 dB [101]. This approach shows the effectiveness of RIS in improving security measures.
3. *Future prospects*: Integrating RIS technology into authentication methods across wireless communication networks holds the promise of extending communication range and fortifying security. Further research avenues involve exploring RIS integration in various authentication techniques, including tag-based and keyless PHY-layer authentication. Leveraging RIS capabilities to intelligently manipulate electromagnetic waves opens new horizons for extending communication range, ensuring enhanced security, and fostering the development of more efficient and reliable authentication protocols.

### 6.3. Federated learning for efficient PHY-layer re-authentication

Federated learning is a decentralised machine learning approach where multiple devices (e.g., IoT devices, smartphones) collaborate to train a global machine learning model without sharing raw data with a central server [103,104]. In the context of physical layer authentication performance, federated learning can be applied to improve the authentication process in the following ways:

1. *Collaborative model training*: Devices in a wireless network can collectively participate in training a shared physical layer authentication model. Each device can use its locally collected data to update the model parameters without transmitting the raw data to a central authority. The global model can then be improved by aggregating the locally updated models from different devices.
2. *Privacy preservation*: Traditional centralised authentication methods often require devices to transmit sensitive information to a central server, raising privacy concerns. Federated learning helps to address this issue by allowing devices to keep their data locally and only share model updates. This way, the privacy of the individual devices' data is preserved.
3. *Adaptation to diverse environments*: Different devices in a wireless network may experience varying communication conditions due to channel fading, interference, and mobility. By incorporating federated learning, devices can adaptively learn and update the physical layer authentication model based on their local experiences, leading to improved performance in diverse environments.
4. *Real-time learning*: Federated learning can facilitate continuous learning and adaptation of the authentication model in real-time. As devices collect new data and experience changing channel conditions, they can continuously update the global model without requiring centralised retraining.
5. *Robustness to attacks*: In the presence of adversarial attacks that attempt to spoof or compromise the authentication process, federated learning can provide robustness by aggregating the knowledge from multiple devices, making it harder for attackers to target a single central authority.

However, it is essential to consider challenges such as communication overhead, synchronisation, and model aggregation techniques to ensure efficient and effective federated learning for physical layer authentication. Additionally, security measures should be taken to protect the federated learning process itself, ensuring that adversaries cannot manipulate the model updates or extract sensitive information during the collaboration.

### 6.4. MAC layer considerations for cross-layer authentication

In the context of cross-layer authentication, particularly concerning the media access control (MAC) layer, there are some considerations and challenges:

1. *Access control mechanisms*: The MAC layer controls access to the shared wireless medium. Cross-layer authentication techniques should seamlessly integrate with MAC layer access control mechanisms to ensure that only authenticated devices gain access to the channel. This integration needs to be efficient to avoid latency issues and to ensure fair access to the network resources.
2. *Timing and synchronisation*: Authentication processes can impact the timing and synchronisation mechanisms of the MAC layer. Efficient cross-layer authentication should consider MAC layer timing re-

quirements to avoid disruptions in communication schedules and ensure synchronization among authenticated devices.

3. *Dynamic network conditions*: MAC layer protocols adapt to dynamic network conditions. Cross-layer authentication should be resilient to these changes and adaptable to varying channel conditions, mobility, and network topologies without causing disruptions or authentication failures.

## 7. Conclusions

In conclusion, this research highlights the potential benefits of PHY-layer authentication in reducing the computational and communication overhead associated with cryptography-based authentication. The study presents a comprehensive classification of authentication techniques in VANETs, examining the strengths and weaknesses of each approach. It is evident that PHY-layer authentication cannot serve as a standalone method in VANETs but shows promise as a supplementary strategy when combined with upper-layer methods. Furthermore, the research conducts a thorough evaluation and comparison of various authentication methods and algorithms, providing valuable insights into their effectiveness and performance. The classification facilitates a clear understanding of which PHY-layer authentication approaches are suitable for integration with upper-layer methods, taking into consideration factors such as computation availability, broadcasting rate, and channel conditions. It is crucial to note that not all PHY-layer authentication methods designed for indoor scenarios with low channel variations can effectively function in outdoor environments with high mobility and dense traffic. This analysis offers researchers in the field a valuable resource, inspiring innovation and the development of robust authentication schemes to meet the evolving demands of VANET applications in the future.

## CRediT authorship contribution statement

**Mahmoud A. Shawky:** Formal analysis, Methodology, Validation, Visualization, Writing – original draft, Writing – review & editing. **Syed Tariq Shah:** Conceptualization, Visualization, Writing – review & editing. **Mohammed Abdrabou:** Formal analysis, Writing – review & editing. **Muhammad Usman:** Formal analysis, Investigation, Visualization. **Qammer H. Abbasi:** Formal analysis, Supervision, Validation. **David Flynn:** Visualization, Writing – review & editing. **Muhammad Ali Imran:** Formal analysis, Supervision, Visualization. **Shuja Ansari:** Formal analysis, Resources, Supervision, Writing – review & editing. **Ahmad Taha:** Formal analysis, Supervision, Validation, Visualization, Writing – review & editing.

## 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.

## References


[1] Who, 2nd global safety report on road safety 2011-2020, 2018, June.
[2] CARE, European road accident database, 2020, June.
[3] UNECE, A foundational safety system concept to make roads safer in the decade 2021-2030, 2020, July.
[4] S. Zeadally, R. Hunt, Y.S. Chen, A. Irwin, A. Hassan, Vehicular ad-hoc networks (VANETS): status, results, and challenges, Telecommun. Syst. 50 (2012) 217–241.
[5] Ahmed Refaat Ragab, A new classification for ad-hoc network, Int. J. Interact. Mob. Technol. 14 (2020, August) 214–223.
[6] K. Nabben, R. Ellie, Ad hoc network, Int. Policy Rev. 11 (2) (2022, April).
[7] L. Chen, Y. Ji, T. Xie, J. Ding, J. Wan, Cross-layer cooperative offloading in vehicular edge computing networks, Veh. Commun. 42 (2023, August).
[8] J.B. Kenney, Dedicated short-range communications (DSRC) standards in the United States, Proc. IEEE 99 (2011, July) 1162–1182.
[9] N. Gupta, A. Prakash, R. Tripathi, Medium access control protocols for safety applications in vehicular ad-hoc network: a classification and comprehensive survey, Veh. Commun. 2 (4) (2015) 223–237.
[10] M.A. Shawky, M. Usman, M.A. Imran, Q.H. Abbasi, S. Ansari, A. Taha, Adaptive and efficient key extraction for fast and slow fading channels in V2V communications, in: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), London, United Kingdom, 2022, pp. 1–6.
[11] N. Gupta, A. Prakash, R. Tripathi, Clustering based cognitive MAC protocol for channel allocation to prioritize safety message dissemination in vehicular ad-hoc network, Veh. Commun. 5 (2016) 44–54.
[12] R. Jiang, Y. Zhu, Wireless access in vehicular environment, in: Encyclopaedia of Wireless Networks, 2020, January, pp. 1463–1468.
[13] M. Abu Talib, S. Abbas, Q. Nasir, M.F. Mowakeh, Systematic literature review on Internet-of-vehicles communication security, Int. J. Distrib. Sens. Netw. 14 (2018, December).
[14] R. Jiang, Y. Zhu, Wireless access in vehicular environment, in: Encyclopedia of Wireless Networks, Springer, 2020, August.
[15] H.M. Elkamchouchi, A.E. Takieldeen, M.A. Shawky, An advanced hybrid technique for digital signature scheme, in: 5th International Conference on Electrical and Electronic Engineering (ICEEE), Istanbul, Turkey, 2018, pp. 375–379.
[16] D. Hankerson, A. Menezes, Elliptic curve discrete logarithm problem, in: Encyclopedia of Cryptography and Security, Springer, Boston, 2011, pp. 397–400.
[17] J. Wang, Y. Shao, Y. Ge, R. Yu, Physical-layer authentication based on adaptive Kalman filter for V2X communication, Veh. Commun. 26 (2020, July).
[18] M. Bottarelli, P. Karadimas, G. Epiphaniou, D.K. Ben Ismail, C. Maple, Adaptive and optimum secret key establishment for secure vehicular communications and sensing, IEEE Trans. Veh. Technol. 70 (3) (2021, March) 2310–2321.
[19] B. Fu, Y. Xiao, H. Deng, H. Zeng, A survey of cross-layer designs in wireless networks, IEEE Commun. Surv. Tutor. 16 (1) (2014) 110–126.
[20] M.A. Shawky, R. Sohaib, M. Usman, Q. Abbasi, M. Imran, S. Ansari, A. Taha, Cooperative intelligent transport systems for net-zero, in: The Role of 6G and Beyond on the Road to Net-Zero Carbon, The Institution of Engineering and Technology, 2023, November.
[21] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Using the physical layer for wireless authentication in time-variant channels, IEEE Trans. Wirel. Commun. 7 (7) (2008) 2728–2739.
[22] A. Mukherjee, S.A. Fakoorian, J. Huang, A.L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: a survey, IEEE Commun. Surv. Tutor. 16 (3) (2014) 1550–1573.
[23] 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: Proceedings of the IEEE Intelligent Vehicles Symposium (IV), Aachen, Germany, 2022, pp. 1315–1320.
[24] M.A. Shawky, M. Bottarelli, G. Epiphaniou, P. Karadimas, An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks, IEEE Trans. Veh. Technol. (2023), Early Access.
[25] H. Wen, J. Zhang, R. Liao, J. Tang, F. Pan, Cross-layer authentication method based on radio frequency fingerprint, Patent number US 10251058 B2, United States Patent, 2019.
[26] M.A. Shawky, M. Usman, M.A. Imran, Q.H. Abbasi, S. Ansari, A. Taha, Adaptive chaotic map-based key extraction for efficient cross-layer authentication in VANETs, Veh. Commun. 39 (2023).
[27] M.A. Al-Shareeda, M. Anbar, I. Hasbullah, S. Manickam, Survey of authentication and privacy schemes in vehicular ad hoc networks, IEEE Sens. J. 21 (2) (2021, January) 2422–2433.
[28] S.S. Manvi, S. Tangade, A survey on authentication schemes in VANETs for secured communication, Veh. Commun. 9 (2017).
[29] I. Ali, A. Hassan, F. Li, Authentication and privacy schemes for vehicular ad hoc networks (VANETs): a survey, Veh. Commun. 16 (2019) 45–61.
[30] L. Bai, L. Zhu, J. Liu, J. Choi, W. Zhang, Physical layer authentication in wireless communication networks: a survey, J. Commun. Inf. Netw. 5 (3) (2020, September) 237–264.
[31] C. Yang, B. Qin, X. Zhou, Y. Sun, S. He, Q. Wu, Privacy-preserving traffic monitoring in vehicular ad hoc networks, in: IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, 2015, pp. 22–24.
[32] W. Ben Jaballah, M. Conti, C. Lal, Security and design requirements for software-defined VANETs, Comput. Netw. 169 (2020, March).
[33] L. Bariah, D. Shehada, E. Salahat, C.Y. Yeun, Recent advances in VANET security: a survey, in: IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), Boston, MA, USA, 2015, pp. 1–7.
[34] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, J. Shen, Secure intelligent traffic light control using fog computing, Future Gener. Comput. Syst. 78 (2018, January) 817–824.
[35] V. Poornachander, Security issues on cryptography and network security, Int. J. Comput. Sci. Inf. Technol. 7 (3) (2016) 1648–1654.
[36] S.S. Manvi, S. Tangade, A survey on authentication schemes in VANETs for secured communication, Veh. Commun. 9 (2017, July).

[37] M. Raya, J.P. Hubaux, The security of vehicular ad hoc networks, in: The 3rd ACM Workshop Security Ad Hoc Sensor Networks, 2005, November, pp. 11–21.
[38] T. Oulhaci, M. Omar, F. Harzine, I. Harfi, Secure and distributed certification system architecture for safety message authentication in VANET, Telecommun. Syst. 64 (2016, July) 679–694.
[39] S. Wang, N. Yao, LIAP: a local identity based anonymous message authentication protocol in VANETs, Comput. Commun. 112 (2017, November) 154–164.
[40] S. Wang, K. Mao, F. Zhan, D. Liu, Hybrid conditional privacy preserving authentication scheme for VANETs, Peer-to-Peer Netw. Appl. 13 (2020, May) 1600–1615.
[41] Z. Lu, W. Liu, Q. Wang, G. Qu, Z. Liu, A privacy-preserving trust model based on blockchain for VANETs, IEEE Access 6 (2018, August) 45655–45664.
[42] Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, A blockchain-based privacy-preserving authentication scheme for VANETs, IEEE Trans. Very Large Scale Integr. Syst. 27 (12) (2019, December) 2792–2801.
[43] C. Lin, D. He, X. Huang, N. Kumar, K.R. Choo, BCPPA: a blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 22 (12) (2021, December) 7408–7420.
[44] M.A. Shawky, A. Jabbar, M. Usman, M. Imran, Q.H. Abbasi, S. Ansari, A. Taha, Efficient blockchain-based group key distribution for secure authentication in VANETs, IEEE Netw. Lett. 5 (1) (2023, March) 64–68.
[45] A. Shamir, Identity-based cryptosystems and signature schemes, in: G.R. Blakley, D. Chaum (Eds.), Advances in Cryptology, CRYPTO 1984, in: Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 1985, pp. 47–53.
[46] Y. Liu, L. Wang, H. Chen, Message authentication using proxy vehicles in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 64 (8) (2015, August) 3697–3710.
[47] 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 (6) (2018, June) 5409–5423.
[48] 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.
[49] 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) 1687–1712.
[50] N.W. Lo, J.L. Tsai, An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings, IEEE Trans. Intell. Transp. Syst. 17 (5) (2016, May) 1319–1328.
[51] Z. Wei, J. Li, X. Wang, C. Gao, A lightweight privacy-preserving protocol for VANETs based on secure outsourcing computing, IEEE Access 7 (2019, January) 62785–62793.
[52] G. Zhang, Y. Liao, Y. Fan, Y. Liang, Security analysis of an identity-based signature from factorization problem, IEEE Access 8 (2020) 23277–23283.
[53] 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.
[54] T. Limbasiya, D. Das, Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication, IEEE Syst. 14 (1) (2020, March) 520–529.
[55] 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.
[56] 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.
[57] J. Cui, J. Chen, H. Zhong, et al., Reliable and efficient content sharing for 5G-enabled vehicular networks, IEEE Trans. Intell. Transp. Syst. 23 (2) (2022, February) 1247–1259.
[58] D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, IEEE Trans. Inf. Forensics Secur. 10 (12) (2015, December) 2681–2691.
[59] J. Li, K.R. Choo, W. Zhang, S. Kumarid, J.J.P.C. Rodrigues, M.K. Khan, D. Hogrefe, EPA-CPPA: an efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks, Veh. Commun. 13 (2018, July) 40–50.
[60] A.K. Sutrala, P. Bagga, A.K. Das, N. Kumar, J.J.P.C. Rodrigues, P. Lorenz, On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of vehicles deployment, IEEE Trans. Veh. Technol. 69 (5) (2020, May) 5535–5548.
[61] Y. Ming, H. Cheng, Efficient certificateless conditional privacy-preserving authentication scheme in VANETs, Mob. Inf. Syst. 2019 (2019, February) 7593138.
[62] H. Tan, I. Chung, Secure authentication and key management with blockchain in VANETs, IEEE Access 8 (2020) 2482–2498.
[63] J. Li, Y. Ji, K.-K.R. Choo, D. Hogrefe CL-CPPA, Certificate-less conditional privacy-preserving authentication protocol for the Internet of vehicles, IEEE Int. Things J. 6 (6) (2019, December) 10332–10343.
[64] Y. Wang, Y. Liu, Y. Tian ISC-CPPA, Improverd-security certificateless conditional privacy-preserving authentication scheme with revocation, IEEE Trans. Veh. Technol. 71 (11) (2022, November) 12304–12314.
[65] D. Chaum, E.V. Heyst, Group signatures, in: Proceedings of the Workshop on the Theory and Application of Crypto, Tech, Springer, Berlin, Heidelberg, 1991, pp. 257–265.
[66] L. Zhang, Q. Wu, A. Solanas, J. D.-Ferrer, A scalable robust authentication protocol for secure vehicular communications, IEEE Trans. Veh. Technol. 59 (4) (2010, May) 1606–1617.
[67] C. Zhang, X. Xue, L. Feng, X. Zeng, J. Ma, Group-signature and group session key combined safety message authentication protocol for VANETs, IEEE Access 7 (2019).
[68] K. Lim, W. Liu, X. Wang, J. Joung, SSKM: scalable and secure key management scheme for group signature based authentication and CRL in VANET, Electronics 8 (2019, November).
[69] Y. Jiang, S. Ge, X. Shen, AAAS: an anonymous authentication scheme based on group signature in VANETs, IEEE Access 8 (2020) 98986–98998.
[70] 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.
[71] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Using the physical layer for wireless authentication in time-variant channels, IEEE Trans. Wirel. Commun. 7 (7) (2008, July) 2571–2579.
[72] J.K. Tugnait, Wireless user authentication via comparison of power spectral densities, IEEE J. Sel. Areas Commun. 31 (9) (2013, September) 1791–1802.
[73] W.-L. Chin, T.N. Le, C.-L. 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.
[74] J. Liu, X. Wang, Physical layer authentication enhancement using two-dimensional channel quantization, IEEE Trans. Wirel. Commun. 15 (6) (2016, June) 4171–4182.
[75] J. Liu, X. Wang, H. Tang, Physical layer authentication enhancement using maximum SNR ratio based cooperative AF relaying, Wirel. Commun. Mob. Comput. 4 (2017, January) 1–16.
[76] J. Hamamreh, H. Arslan, Joint PHY/MAC layer security design using ARQ with MRC and null-space independent, PAPR-aware artificial noise in SISO systems, IEEE Trans. Wirel. Commun. 17 (9) (2018, September) 6190–6204.
[77] R.-F. 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).
[78] N. Gao, Q. Ni, D. Feng, X. Jing, Y. Cao, Physical layer authentication under intelligent spoofing in wireless sensor networks, Signal Process. 166 (2020, January).
[79] N. Li, S. Xia, X. Tao, Z. Zhang, X. Wang, An area-based physical layer authentication framework to detect spoofing attacks, Sci. China Inf. Sci. 63 (2020, October).
[80] A.K. Jadoon, J. Li, L. Wang, Physical layer authentication for automotive cyber physical systems based on modified HB protocol, Front. Comput. Sci. 15 (2020, December).
[81] J. Zhang, S. Rajendran, Z. Sun, R. Woods, L. Hanzo, Physical layer security for the Internet of things: authentication and key generation, IEEE Wirel. Commun. Mag. 26 (5) (2019, October) 92–98.
[82] W. Hou, X. Wang, J-Y. Chouinard, A. Refaey, Physical layer authentication for mobile systems with time-varying carrier frequency offsets, IEEE Trans. Commun. 62 (5) (2014, May) 1658–1667.
[83] H. Fang, X. Wang, L. Hanzo, Learning-aided physical layer authentication as an intelligent process, IEEE Trans. Commun. 67 (3) (2019, March) 2260–2273.
[84] X. Wang, P. Hao, L. Hanzo, Physical-layer authentication for wireless security enhancement: current challenges and future developments, IEEE Commun. Mag. 54 (6) (2016, June) 152–158.
[85] 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 (2020) 1011–1034.
[86] P. Ramabadran, P. Afanasyev, D. Malone, et al., A novel physical layer authentication with PAPR reduction based on channel and hardware frequency responses, IEEE Trans. Circuits Syst. 67 (2) (2020, February) 526–539.
[87] B. Widrow, S.D. Stearns, Adaptive Signal Processing, Chapter 11, Prentice-Hall, 1986, pp. 430–435.
[88] D. Shan, K. Zeng, W. Xiang, P. Richardson, Y. Dong PHY-CRAM, Physical layer challenge-response authentication mechanism for wireless networks, IEEE J. Sel. Areas Commun. 31 (9) (2013, September) 1949–1959.
[89] X. Wu, Z. Yang, Physical-layer authentication for multi-carrier transmission, IEEE Commun. Lett. 19 (1) (2015, January) 74–77.
[90] L. Cheng, L. Zhou, B.-C. Seet, W. Li, D. Ma, J. Wei, Efficient physical-layer secret key generation and authentication schemes based on wireless channel-phase, Mob. Inf. Syst. (Hindawi) 2017 (2017, July).
[91] 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, July) 1776–1780.
[92] P. Zhang, J. Liu, Y. Shen, H. Li, X. Jiang, Lightweight tag-based PHY-layer authentication for IoT devices in smart cities, IEEE Int. Things J. 7 (5) (2020, May) 3977–3990.
[93] N. Zhang, X. Fang, Y. Wang, S. Wu, H. Wu, D. Kar, H. Zhang, Physical layer authentication for Internet of things via WFRFT-based Gaussian tag embedding, IEEE Int. Things J. 7 (9) (2020, September) 9001–9010.
[94] S. Althunibat, V. Sucasas, G. Mantas, J. Rodriguez, Physical-layer entity authentication scheme for mobile MIMO systems, IET Commun. 12 (6) (2018, March) 712–718.
[95] J. Wang, Y. Shao, Y. Ge, R. Yu, Physical-layer authentication based on adaptive Kalman filter for V2X communication, Veh. Commun. 26 (2020, December).

[96] J. Yang, X. Ji, K. Huang, M. Yi, Y. Chen AKA-PLA, Enhanced AKA based on physical layer authentication, KSII Trans. Int. Inf. Syst. 11 (7) (2017, July) 3598–3617.
[97] 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) 4999–5007.
[98] C.T. Zenger, M. Pietersz, J. Zimmer, J.-F. Posielek, T. Lenze, C. Paar, Authenticated key establishment for low-resource devices exploiting correlated random channels, Comput. Netw. 109 (2016, November) 105–123.
[99] Y. Chen, H. Wen, J. Wu, H. Song, A. Xu, Y. Jiang, T. Zhang, Z. Wang, Clustering based physical-layer authentication in edge computing systems with asymmetric resources, Sensors 19 (8) (2019, April) 1926.
[100] M.A. Shawky, S.T. Shah, M.S. Mollel, J.R. Kazim, M.A. Imran, Q.H. Abbasi, S. Ansari, A. Taha, Reconfigurable intelligent surface-assisted cross-layer authentication for secure and efficient vehicular communications, arXiv preprint, https://doi.org/10.48550/arXiv.2303.08911, 2023.
[101] M.A. Shawky, S.T. Shah, Q.H. Abbasi, M. Hussein, M.A. Imran, S.F. Hasan, S. Ansari, A. Taha, RIS-enabled secret key generation for secured vehicular communication in the presence of denial-of-service attacks, Sensors 23 (2023, April).
[102] X. Lu, J. Lei, Y. Shi, W. Li, Intelligent reflecting surface assisted secret key generation, IEEE Signal Process. Lett. 28 (2021, February) 1036–1040.
[103] S. Wang, N. Li, S. Xia, X. Tao, H. Lu, Collaborative physical layer authentication in Internet of things based on federated learning, in: 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications, Helsinki, Finland, 2021, September, pp. 714–719.
[104] A.M. Elbir, A.K. Papazafeiropoulos, S. Chatzinotas, Federated learning for physical layer design, IEEE Commun. Mag. 59 (11) (2021, November) 81–87.