SN Computer Science (2023) 4:589 https://doi.org/10.1007/s42979-023-02122-3

Privacy-preserving Authentication Protocols in VANET: A Review

Himun Nath[1] and Hiten Choudhury[1]

[1]Department of Computer Science & IT, Cotton University, Panbazar, Guwahati, 781001, Assam, India.

Contributing authors: CSC1891001_himun@cottonuniversity.ac.in; hiten.choudhury@cottonuniversity.ac.in;

Abstract

Vehicular Ad hoc Network (VANET) is a versatile and ad hoc network, where the vehicles must be authenticated before sharing any critical information. During authentication, privacy of the users must be preserved. There are several surveys on privacy-preserving authentication schemes in VANET. However, none of them are focused on the ability of the schemes to address different security issues and their robustness against security attacks. In this paper, we present a review on various privacy-preserving authentication schemes in VANET. These schemes may be categorized into several types like symmetric/asymmetric key cryptography based schemes, digital signature based schemes, ID cryptography based schemes, pseudonym based schemes, homomorphic encryption based schemes and blockchain based schemes. A comprehensive study of the prominent schemes, with regards to their effectiveness in addressing different security issues and their robustness against possible attacks, has been performed. Open issues and scope for future work are also highlighted.

Keywords: Vehicular Adhoc Network (VANET), security, privacy, authentication, blockchain, homomorphic

1 Introduction

Vehicular Ad-Hoc Network (VANET) can be thought of as a kind of Mobile Ad-Hoc Network (MANET) with each node as a vehicle [1]. It has gained

attention for its advantage on the road. VANET refers to a collection of vehicles that are either stationary or on the move. Generally, the entities in VANET are Trusted Authority (TA), Road Side Units (RSUs) and On-Board Units (OBUs). The TA provides the credentials to RSUs and OBUs, which are required for communication in VANET. The TA also requires monitoring the messages that are exchanged among the RSUs and OBUs and simultaneously take necessary actions on complaints. The OBUs which are installed in the vehicles, need to be authenticated by RSUs and TA before using the VANET services. The authentication in VANET can be either node authentication or message authentication. In node authentication, the RSUs and vehicles are authenticated for its communication in ad hoc network whereas, in message authentication integrity of the messages checked [1]. In addition, there might be users in VANET with malicious intentions and they may steal or manipulate personal information of the authentic users. Therefore, in order to prevent personal information from malicious or any other users, concealing personal information while communicating in VANET is a must [2]. To overcome the privacy concern and to provide privacy-preserving authentication in VANET, several schemes have been proposed. The schemes differ in various aspects like access technologies, mechanisms to preserve privacy, cryptographic techniques, etc. There are several surveys in the literature that discuss the different types of VANET schemes. These prominent surveys or reviews highlight open issues, future directions and points out the advantages of one technique over the other [3]. But most of the surveys do not include schemes that are based on blockchain, hash-XOR operation and homomorphic encryption. They also do not present a comparative analysis of the different types of schemes with respect to their effectiveness in addressing different security issues and their robustness against possible security attacks. In this survey, we have filled the gap by considering the aforementioned issues.

The rest of the paper is organised as follows: In Section 2 provides a general overview of VANET. Section 3 explains about the authentication in VANET. Section 4 presents the security attacks and security requirements of privacy-preserving authentication schemes. Section 5 presents some of the related works. Section 6 provides a comprehensive explanation of different technologies that are used to devise a privacy-preserving authentication scheme, followed by its discussions and effectiveness in Section 7. Finally in Section 9 concludes our review with future direction.

2 VANET overview

Taking into consideration the VANET standards in automotive industry of US, Europe and Japan, it is found that a radio frequency of 5.8 GHz to 5.9 GHz is used for the ITS applications. [4] The ETSI ITS of Europe or WAVE of U.S utilizes the allotted frequency band to exchange information among the vehicles or infrastructures. Generally, the components of VANET are OBU, RSU and TA. [5] The OBUs are installed in the vehicles and are responsible

for sending/verifying information to/from RSUs and other vehicles. The TA monitors the information that are being exchanged among the vehicles and RSUs. The components, characteristics and standards of VANET are discussed below. Table 1 lists the acronyms that is frequently used in our work.

Table 1 List of acronyms

Acronyms	Description
VANET	Vehicular Ad-hoc Network
TA	Trusted Authority
RSU	Road Side Unit
OBU	On Board Unit
TPD	Tamper Proof Device
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure
ROM	Random Oracle Model
SDN	Software Defined Network

2.1 System Model

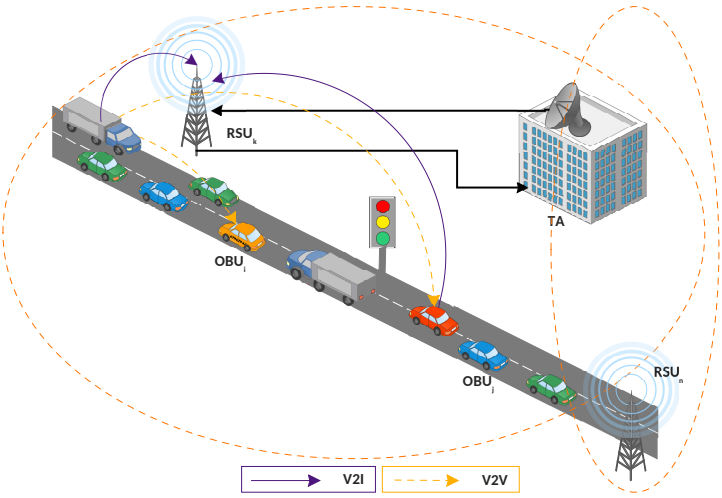


Fig. 1 A VANET environment

Figure 1 illustrates a basic VANET system model that includes the following components. [5]

1. OBU: OBU is a device installed in a vehicle to perform computations required during exchange of messages. The OBU collects information like location, speed, etc. and using wireless link it shares with RSUs and OBUs of other vehicles. Other than sensors, it also possess storage capability to store and update its credentials that are required for exchanging information.

2. RSU: RSUs are devices that are installed on the road, especially at critical junctures like crossing or parking area, after every interval. It serves as a communication link to all the OBUs within its range and are assigned tasks for informing critical information among the OBUs. It consists of network devices that support DSRC as well as other infrastructure communication.
3. TA: The TA is in charge of the entire VANET. It generates and broadcasts system parameters to both RSUs and OBUs. The TA registers and authenticate RSUs, OBUs and holds the authority to revoke or remove any RSU, OBU on account of malicious activity. For its tasks, it holds large computational and storage capability as compared to RSUs and OBUs.

2.2 VANET characteristics

The following are the VANET characteristics that challenges a vehicle's security.

1. Mobility: Vehicles that are on the move often requires configuring itself with the newly available network. On highways, vehicles are generally at tremendous speed, and therefore, authenticating itself with the characteristic of high mobility is a challenge.
2. Real-time constraint: Vehicles in VANET must possess the ability to exchange information with infrastructure and other vehicles instantaneously. The sender and the receiver of a message in VANET should act within a given time frame.
3. Dynamic network topology: Due to the mobility of a vehicle, it needs to change its network configuration frequently. Thus, an adversary on acquiring credentials from another vehicles can benefit from such scenarios.
4. Unpredictability: The users or vehicles in VANET are at high speed and they frequently join and leave the network. Thus, the credentials needed to be in VANET must be available to the authentic users or else it might pose a security threat.
5. Computation and Storage: A vehicle equipped with an OBU or a storage device has the adequacy for performing computations and store the results in a database. [6] However, challenge lies whenever a vehicle's capability has to match its dynamic nature.

2.3 VANET standards

Standards in VANET provides a generally accepted form of wireless communication among the vehicles. The standards aides enhancing the communicative latency and interoperability among vehicles and infrastructures. [7] Many surveys on authentication and privacy preservation of the vehicles considers IEEE802.11, DSRC, and WAVE as VANET standard leavingaside the wireless cellular network [8][9][10][11]. After surveying the different available standards, the following are found to be applicable in many of the existing VANET schemes.

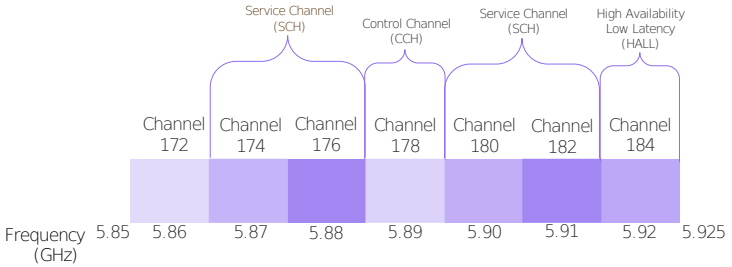


Fig. 2 DSRC channel allocation

1. DSRC: DSRC is basically a wireless communication technology. The Federal Communications Commission (FCC), which is an independent agency of United States federal government, allocated the band from 5.850 to 5.925 GHz, with a spectrum of 75MHz for DSRC. It supports short to medium range communication service that are based on IEEE 802.11a physical (PHY) layer and IEEE 802.11 Medium Access Control (MAC) layer. The middle of the stack of DSRC is defined by the IEEE 1609 working group. Moreover, it supports IPV6 stack together with network and transport layer protocol known as WAVE Short Message Protocol (WSMP) [12]. Figure 2 shows the channel diagram of DSRC. [13]
2. WAVE: The WAVE describes the architecture, protocols, interface and mechanisms required to develop the communication among vehicles and interfaces. WAVE generally represent standards of IEEE 1609.1, 1609.2, 1609.3, 1609.4 and IEEE 802.11p. Other than applications for transportation, it also provides security services. Figure 3 shows the WAVE communication stack consisting of data plane and management plane. [14] The data plane describes the processing of data whereas management plane describes the communication command required for performing operations like synchronization, channel switching etc.
3. IEEE 802.11p: The IEEE 802.11p standard is derived from IEEE 802.11a and operates at 5.9 GHz spectrum. IEEE 802.11p standard together with DSRC band provide vehicular communication network. Because of IEEE 802.11p, DSRC applications are not affected by interferences from other wireless devices.
4. Cellular network: VANET that utilizes cellular network for communication, exchanges the information among the vehicles through the Base Stations (BS). The BS resembles an RSU in DSRC/WAVE standard. The BSs are connected to vehicles via a cellular network like 4G/LTE. [15] In VANET Cellular integrated network architecture (VCNET), which is based on the 3GPP LTE/EPC architecture, consists of an access networks (E-UTRANS) and core networks (EPC). The task of authenticating authorised vehicle is assigned to Mobility Management Entity (MME), which is part of the core network. [16]

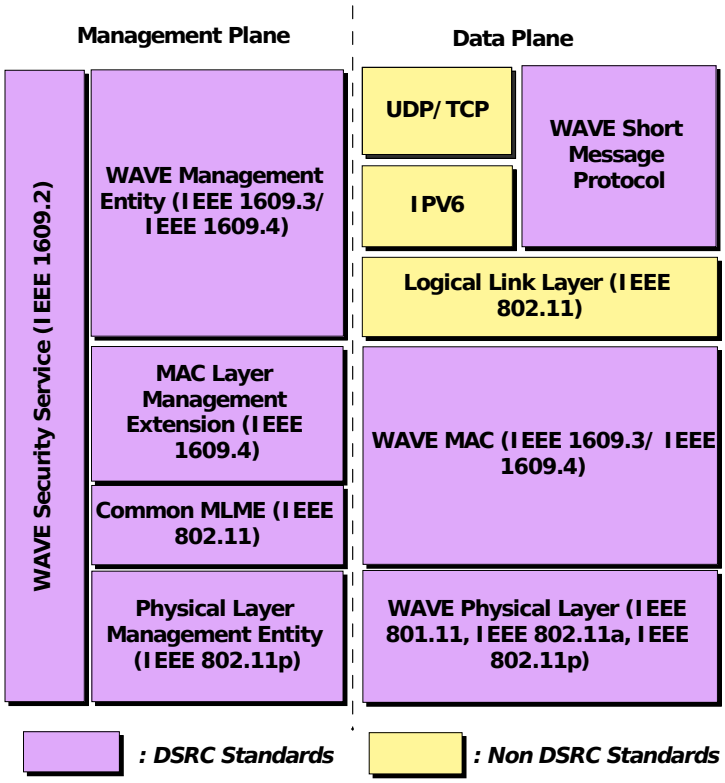


Fig. 3 A WAVE protocol stack

3 Authentication in VANET

The information in VANET is exchanged among users in an open access environment and hence security is a major concern. This involves factors like continuous exchange of messages without any malicious party interpreting /acquiring /broadcasting the messages. Moreover, the exchanged information might contain personal or crucial information of a sender or its group, which calls for the need for confidentiality, integrity and anonymity of such information [17]. To exchange crucial information among the vehicles and RSUs, authentication is required in VANET. The vehicles plying in the road needs to exchange crucial information and authentication among the entities will exclude malicious users from attacking and acquiring information of a authentic user. Authentication can be carried out in different ways. The messages can either be encrypted and then later decrypted for verification or the messages can be signed and later the receiver verifies signature of the message [18]. The TA, AS and RSUs requires constant monitoring of the vehicles. Although a vehicle can be equipped will enough storage capacity and computation ability, but to match the speed of the vehicles, authentication must be done with minimal latency [19]. Moreover, the receiving vehicle requires verifying the

message content within a limited time frame. Otherwise, mismatched messages will lead to blow hot and cold decisions among the VANET users. This will allow a malicious user to duplicate or repudiate messages in VANET or halt the VANET services. Other than modification, repudiation, man-in-the middle (MIM) attack, an adversary might track a user to acquire route information [20]. Therefore, to withstand attacks and tracking of a genuine user, the vehicles must be authenticated efficiently.

4 Privacy-Preserving authentication in VANET

The security and privacy is of utmost importance in VANET environment due to its open communication environment. VANET is used for exchange of general or crucial life saving information among the authentic users. But the information exchanged must not reveal any real identity of a user because anyone might track or impersonate another user for personal gains. The vehicles in VANET must be able to preserve privacy. Privacy in VANET can be categorized as follows:

1. User Data Privacy: an adversary or an outsider should not be able to acquire any information regarding the installed sensors or personal data when there is a message exchange among the entities.
2. Location privacy: the geographical location of a user must not be known to any outsider.
3. Route privacy: a user travelling from a source to destination point must not let others known the route information or its geographical location to any other user [21].

Generally, most of the VANET schemes implement the idea of anonymous or pseudo ID during the message exchange among the entities. Pseudonyms are helpful to maintain anonymity among the users. But the pseudonyms used must not be traceable or linkable by other vehicles. However, in the hour of need like lawful interception etc., TA together with RSU, must be able to trace a vehicle.

4.1 Security Attacks against Privacy-Preserving authentication in VANET

Due to high mobility of the vehicles, the attackers tend to disguise the authorities of the network. An adversary can use any means to compromise communication of the vehicular network. Therefore, classification of various possible attacks helps in formulating strategies for avoidance and detection of attempts made by malicious parties [22]. The following are the known attacks that pose a threat to the VANET users.

1. Impersonation attack: In this type of attack, the attacker pretends to be an authentic user of VANET, and exchanges messages on behalf of the

disguised identity. In case of any anomalies in the network, the attacker rejects its involvement.
2. Modification attack: Here, an attacker modifies the messages that are exchanged among users of VANET. Modification is an attack that affects the integrity and availability of the messages.
3. Sybil attack: In this type of attack, an attacker manages to create numerous pseudo-identity of its own to subvert the VANET. With this approach, the attacker tries disrupting the services availed by entities in VANET.
4. ID disclosure attack: Here, an attacker gathers the real ID of an authenticated user.
5. Location tracking: In this attack, an attacker tries tracking a user to gather its location, thereby posing a threat on location privacy.
6. Replay attack: Here, an attacker repeatedly broadcasts messages that can be either genuine or fake.
7. Bogus information attack: Here, an attacker injects false information in the broadcast message.
8. DoS attack: This attack resists a user from accessing its intended message. This is done by jamming or flooding the communication channel with bogus information.
9. Collusion attack: This attack is also known as ballot-stuffing attack [23]. Multiple vehicles forms an alliance and forges the attack to disrupt the genuineness of the exchanged messages.

4.2 Security Requirement of a Privacy-Preserving authentication scheme

In addition to the above discussed attacker, the following security requirements needs to be considered by a privacy-preserving authentication scheme for VANET:

- Message authentication: The message exchange in VANET should be among the authorised users. Hence, the users exchanging the messages should be authenticated. The authentication scheme should resist an attacker from impersonating another authorised user or a service provider.
- Conditional privacy-preservation: A vehicle requires preserving its real ID during message exchange. The real ID must be guarded because an attacker might harm or disrupt communication service of a user. Hence, a vehicle requires maintaining its real ID secret, thereby use anonymous ID instead, and prevent itself from tracking. However, the TA, due to liability issues, require maintaining a map of the real ID and its corresponding anonymous ID.
- Confidentiality, Integrity and Availability (CIA): Ensuring confidentiality, integrity and availability in VANET is paramount to VANET's operability [24]. For confidentiality of the messages, encrypting the messages during its exchange resists an attacker from knowing its contents. Integrity of the messages ensures that messages are unaltered during transition. Moreover, the

service provider requires blocking malicious users and restrict the message availability. But, restricting such users must not affect the authentic users of VANET.

- Traceability: The governing authority of VANET requires to tracing a vehicle under certain circumstances like on lodging of a complaint or on exchange of offensive messages. Generally, the TA with the help of RSU, posses the ability to trace a vehicle.
- Unlink-ability: Any user, under any circumstances must not be able to match a message transmitted by any user. If linking of the exchanged credentials is possible, then an attacker can trace an authentic user and gather personal information.
- Non-Repudiation: The users of VANET must hold accountable for sending or broadcasting a message. Otherwise, a user might flood the network with unwanted or false messages for personal amusement.
- Key freshness: The credentials or parameters used for communication in VANET requires frequent update to prevent from attackers. This is required to resist an attacker from gathering or interpreting the keys that can be used in near future.

5 Related works

In this section, we discuss similar work that surveyed on authentication and privacy-preserving mechanisms in VANET.

In [10], the authors have done a comprehensive review on authentication and privacy-preserving mechanisms. The work considered the cryptographic techniques like symmetric key cryptography-based schemes, public key cryptography-based schemes, pseudonym-based schemes, identity-based schemes, group signature-based schemes, ring signature-based schemes and block-chain based schemes. The authors presented a detailed survey of the works that were based on the above mentioned cryptographic primitives but excluded the schemes that considers homomorphic encryption. Moreover, the authors also emphasised on the privacy preservation and security mechanisms in VANET. But in the paper, while considering the architecture, the authors did not consider VANET through cellular communication.

In [8], Manvi et al., discusses different techniques for authenticating the vehicles that are plying on the road. The authors considered three mechanisms i.e., cryptographic techniques, digital signatures, and message verification techniques for classifying the authentication mechanism. Although the survey presents a lucid description of all the considered authentication mechanism but the discussed authentication techniques are limited. Prominent works on block-chain and homomorphic encryption are not included in the discussions.

In [9], Sheikh et al., presented a comprehensive review on architecture, standards, security and its challenges of VANET. The work also covers detailed survey of authentication schemes and simulation tools used to display the performance of VANET schemes. Communication through both cellular and

Table 2 Surveys on authentication and privacy-preservation

Schemes	Contributions	Limitations
"A comprehensive survey on authentication and privacy-preserving schemes in VANETs" Munde et al. 2021 [10]	Provided a comprehensive review of the existing authentication schemes based on security and privacy.	Does not consider schemes based on Hash XOR operations and homomorphic encryption. Do not consider the robustness of the schemes against possible attacks
"A survey on authentication schemes in VANETs for secured communication Manvi et al. 2017 [8]	Surveyed authentication schemes based on cryptography, signature and verification used.	Does not include schemes based on cellular architecture. Schemes based on blockchain and homomorphic encryption are not considered. Did not consider robustness and security issues against possible VANET attacks
"A comprehensive survey on VANET security services in traffic management system" Sheikh et al. 2019 [9]	Discussed architecture, standards, security and its challenges. Surveyed about the threats showered by malicious users on traffic related messages.	Did not consider blockchain and homomorphic encryption based schemes. VANET using cellular network is also not included. Robustness against possible VANET attacks are not considered
"A survey on authentication schemes of VANETs" Jenefa et al. 2016 [25]	Discusses some prominent schemes that provide authentication and privacy in VANET.	Limited number of papers were discussed. Schemes based on blockchain are not discussed. Security issues and robustness against possible VANET attacks are not considered

DSRC were considered. But, blockchain and homomorphic based encryption schemes were not considered.

In [25], Jenefa et al., presented different authentication mechanisms through which vehicles communicate among themselves. The survey includes several prominent authentication schemes with their respective limitations. But in the work, the discussed approaches of providing authentication to the vehicles were limited.

In the work proposed in [11], Azam et al. surveyed authentication schemes considering privacy, confidentiality and scalability requirement of the owner of the vehicles. Schemes based on 5G, SDN enhanced 5G cellular network and blockchain based schemes are considered in the survey.

Though there are several works discussing the different aspects of authentication and preserving privacy, but as described in Table 2, many of the works are of similar nature. The discussions on the cryptographic techniques excludes works like homomorphic encryption and block-chain based authentication. Considering the architecture, many of the surveys skipped the possibility of implementing the cellular communication in VANET. Moreover, discussions to overcome the possible attacks are limited in these works. Therefore, in this work we have performed a survey on authentication and privacy preservation to fill the above mentioned gap.

6 Taxonomy of privacy-preserving authentication schemes

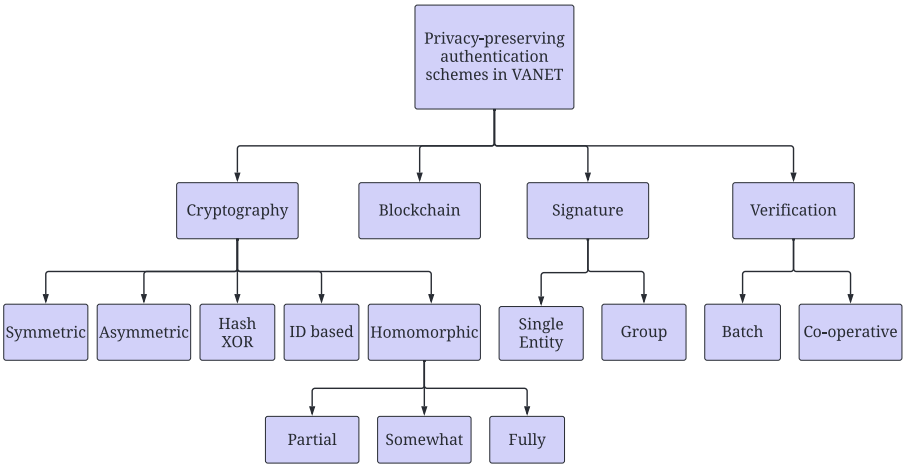


Fig. 4 Taxonomy of privacy-preserving authentication schemes in VANET

In VANET, authentication is required to provide essential and life saving information of the road to the legitimate users [26]. To match the dynamics of the vehicles with the task of authenticating large number of VANET entities by the trusted parties is a challenge [27]. The classification of the authentication schemes is illustrated in Figure 4. Generally, the authentication schemes are classified based on cryptography, signature and verification [8]. On the basis of cryptographic techniques used, schemes can be divided into symmetric, asymmetric and ID-based encryption schemes. In symmetric key based schemes, a shared key is used, whereas in asymmetric key based schemes public/private keys are used for authentication and message exchange [28]. In ID based encryption schemes, a recognizable public key is used by the VANET entities for authentication and message exchange. The private key corresponding to the public key is shared by TA [29]. The ID is however is not real ID, instead anonymous ID and is obscured to preserve privacy [30]. In signature based scheme, the messages are signed with a secret key. Then the sender sends the message and the signed message together to the receiver. The receiver checks the integrity of the message by signing the received message and compares it with the received signed message. Signature based schemes can be divided into single entity signature and group signature schemes. In group Signature based schemes user of a group signs the credentials on behalf of the group. Other users verifies the signature but only a designated entity called opener can gather information about particular signer. Generally, in V2V communication, only a single authority issuing untraceable data or single opener tracing

other users is not applied [31]. Homomorphic encryption has its unique feature that allows the third party to perform operations over the encrypted data and thereby preserving user's privacy [32]. Unlike most of the surveys, homomorphic encryption based schemes are included in our survey. It can be classified into partial, somewhat and fully homomorphic encryption. Moreover, symmetric homomorphic encryption uses symmetric key and asymmetric homomorphic encryption uses asymmetric key [33].

In this section, we discuss some of the prominent privacy preserving authentication protocols with regards to the type in the taxonomy to which they belong (Figure 6). Unlike many other works, we have also included block-chain based, homomorphic encryption based and simple Hash-XOR based authentication schemes in our study. We also analyse the proposals with respect to their ability to withstand the attacks that are discussed in Section 4.1 and meet the security features that are discussed in Section 4.2.

6.1 Cryptography based schemes

The messages exchanged in VANET needs to be secured, as critical information might get in the hands of an adversary [34]. Encryption techniques include both symmetric and asymmetric encryption. Depending on the complexity and bandwidth of the VANET architecture encryption mechanisms are built [35].

6.1.1 Symmetric key cryptography based schemes

In symmetric key based encryption techniques, only a single key (secret or private key) is used to encrypt and decrypt the messages that are being exchanged among the entities (both sender and receiver) of VANET. Therefore, symmetric encryption is simple and faster to match the dynamic nature of vehicular communication [36][37]. In this subsection, we present some of the symmetric cryptography based schemes. A generalised description of the security requirements and robustness against attacks of different schemes based on symmetric cryptography are presented in Table 3.

Wang et al. [38] proposed a scheme that is lightweight and efficient in nature and named it as Lightweight and Efficient Strong Privacy Preserving (LESPP) authentication scheme. The scheme uses Message Authentication Code (MAC) and symmetric encryption mechanism and is proposed to preserve identity privacy, avoid DoS attack, and provide conditional traceability and unlinkability to the vehicles. The authors criticised the usage of traditional digital signature technique as is not efficient when many vehicles are deployed in VANET. Moreover, as mentioned in the work of Ren et al., that usage of traditional digital signature technique might result in compromising user's real ID [39]. Similarly Liu et al., proposed a symmetric key encryption based VANET [40]. The scheme is built to provide message dissemination with policy enforcement providing data confidentiality.

Lim et al. [41] devised a scalable and secure group signature based authentication scheme that provides traceability and prevents from MIM attack,

replay attack. The authors considered the challenge of distributing credentials to the fast pace vehicles and thereby proposed an efficient key management protocol. In the scheme, RSU generates a group private key by the parameters initially provided the TA. Using the private key, multiple RSUs (Member RSU or M-RSU) can initiate communication among themselves and vehicles. The vehicles on receiving *beacon* message from RSU, requests for the private/public key pair. The RSU then generates a shared secret key with the credentials provided by the vehicle.

Eiza et al. [42] proposed a secure, reliable and real-time video reporting service. The scheme leverage 5G enabled vehicular communication and is proposed to be efficient in computational ability. The entities involved in the scheme are TAs, Department of Motor Vehicles (DMV), Law Enforcement Agency (LEA) and the vehicles. Initially, the DMV with TA, provide pseudonym and certificates to the authorised vehicles. Later, with the parameters received from service providers, a vehicle can exchange information among the entities. The videos that are exchanged among the vehicles are encrypted using symmetric encryption mechanism. However, the symmetric key is exchanged by encrypting it with TAs public key. The scheme is robust against attacks like sybil attack, DoS attack and provides features like privacy-preservation, unlinkability, traceability, non-repudiation and integrity of the exchange messages.

In [43], Vijayakumar et al. proposed a privacy-preserving dual authentication and key management mechanism for secure transmission of data among the VANET entities. The entities included in the scheme are TA, RSU and the vehicles. The dual key management allows the TA to broadcast the information to the group of vehicles in a secure manner. Two groups are created (dual) according to the service requested by the vehicles. Vehicle users enjoys VANET services by paying through a Service Level Agreement (SLA). The categorization of the users are Primary Users (PU), Secondary Users (SU) and Unauthorized Users (UU). There exist a common group key among all the users, which is generated using Chinese Remainder Theorem (CRT). The TA provides a secret key (VSK) to each vehicle in the VANET, using which a vehicle generates hash code and thereby initiate VANET communication with TA and RSUs. The VSK is provided during the registration phase of the vehicle. The TA also provides each RSU an RSU Secret Key (RSK), using which exchange of confidential information with the TA can be established. The scheme is efficient and robust against MIM attack, replay attack, sybil attack, modification attack and collusion attack.

6.1.2 Asymmetric key cryptography based schemes

In asymmetric key cryptography based schemes, two key pairs are used for exchanging messages securely. The senders encrypts the message with their public key and the receiver decrypts the same with their provided private key

Table 3 Symmetric cryptography based schemes

Security and Attacks	Schemes			
	[38]	[41]	[42]	[43]
Privacy Preservation	✓	×	✓	✓
Unlinkability	✓	×	✓	×
Traceability	✓	✓	✓	×
Non-Repudiation	×	×	✓	×
Unforgeability	×	×	×	×
Message Integrity	✓	×	✓	×
Anonymity	✓	×	✓	×
DoS	✓	×	×	×
MIM	×	✓	×	✓
Replay attack	✓	✓	×	✓
Sybil attack	×	×	✓	✓
Modification attack	✓	×	×	✓
Collusion attack	✓	×	×	✓

Table 4 Asymmetric cryptography based schemes

Security and Attacks	Schemes			
	[44]	[45]	[46]	[47]
Privacy Preservation	✓	×	✓	✓
Unlinkability	✓	✓	✓	✓
Traceability	✓	✓	✓	✓
Non-Repudiation	×	×	✓	×
Unforgeability	×	✓	✓	✓
Message Integrity	×	✓	✓	✓
Anonymity	×	✓	✓	✓
DoS	✓	×	✓	×
MIM	×	×	×	×
Replay attack	✓	✓	✓	✓
Sybil attack	×	×	×	×
Modification attack	✓	✓	✓	✓
Collusion attack	✓	✓	✓	✓

[22][48]. Table 4 presents a summary of the ability to meet security requirements and robustness against attacks that are considered in schemes based on asymmetric cryptography.

Azees et al. [44] devised an efficient scheme that is based on bilinear pairing. The authors proposed the scheme to be computationally efficient for both the OBU and RSU. The signature verification cost and message loss ratio of the scheme is proposed to be minimal and provides Location Based Safety Information (LBSI) through the RSUs. The scheme also provides tracking of mischievous users, which adds the feature of conditional privacy. Other than conditional privacy, the scheme provides features like unlinkability, traceability, non-repudiation and can withstand DoS attack, replay attack, modification attack, collusion attack.

Shao et al. [45] proposed a new authentication protocol using a technique called new group signature scheme. The scheme is primarily proposed to overcome the heavy workload while using Certificate Revocation List (CRL) and issues regarding the trust of messages as they are authenticated anonymously.

The scheme is built considering four participating entities in VANET. It consists of tracing manager (TM), central authority (CA), RSUs and OBUs. The task of CA is to authenticate the public keys of RSUs and that of TM is to authenticate public keys of OBUs. Moreover, the scheme uses group signature to exchange information among authenticated users in a group. The entities used in group signature are a group manager, a group tracer, and many group members. All the entities of group signature contribute to form a new group signature scheme that provides threshold authentication, unforged exchange of messages and revocation of certificates, anonymity and traceability. The scheme is proposed to be robust against replay attack, modification attack and collusion attack.

Chim et al. [46] proposed a navigation-based positioning of the vehicles that would help the vehicles to reach its designation in proper time. The privacy is preserved with the use of pseudo identity. The authorities that include TA and RSUs, can gather the legitimate information when required for verification purpose.The work leveraged the proxy re-encryption in the VANET Secure and Privacy-preserving Navigation (VSPN) scheme. For each vehicle the TA initially assigns re-encryption keys, which is later used by the RSU to encrypt the master key. RSU then forwards it to the destined vehicle. The receiving vehicle decrypts for the master key with its own private key. This is how the master key is kept secret from the RSU and at the same time, distributed by the RSU as well. The scheme is proposed to achieve security features like privacy-preservation, unlinkability, traceability, non-repudiation, unforgeability, message integrity and anonymity. In addition, the scheme is secure against attacks like DoS, replay attack, modification attack and collusion attack.

Wei et al. [47] devised a scheme that uses identity-based signature. The scheme is designed to provide privacy and resist chosen message attack and is achieved through Identity-Based Signature (IBS). Moreover, the scheme provides security features like unlinkability, traceability, non-repudiation, unforgeability, message integrity, anonymity. The scheme is also proposed to be secure against attacks like replay attack, modification attack and collusion attack.

6.1.3 Hash and XOR operation based schemes

In VANET, as the vehicles are at high speed, therefore the exchange of credentials among the entities should take place at minimal latency [21] [49]. So, it is preferable that the VANET schemes be built with minimal latency [50]. There are several authentication schemes that are built using the lightweight cryptographic operations, i.e., hash and XOR operations [51]. Considering the VANET authentication schemes, where the assorted vehicles need to be authenticated and at the same time messages need be verified, lightweight cryptographic operation schemes are efficient and practical. In this section, we will discuss several prominent authentication schemes that are based on hash function and XOR operation. A generalised description of the security

requirements and robustness against attacks of the schemes using hash-XOR operation is presented in Table 5.

In [52], Wazid et al. proposed a VANET scheme that is cluster based to overcome computation and communication overhead in VANET network. The scheme uses only one way hash function and bitwise XOR operation to provide authentication and key agreement. In the scheme, three types of mutual authentication exists and they are 1) authentication among the vehicles; 2) authentication between the vehicles and their cluster head; and 3) authentication between the vehicles and their nearest RSUs. The authentication scheme is proposed to be robust against MIM attack, replay attack, modification attack, collusion attack and is provides security features like traceability, anonymity.

In [53], Alazzawi et al. proposed a scheme that utilizes pseudonym to facilitate conditional anonymity, message integrity and authentication in VANET. Moreover, the scheme provides features like unlinkability, traceability, non-repudiation, unforgeability and is secure against MIM attack, DoS attack, replay attack, collusion attack. The scheme uses hash function and XOR operation during the exchange of credentials. The authors have devised the pseudo ID based scheme to overcome the shortcomings of Identity based (ID) schemes. The three areas where the scheme has primarily focused includes: 1) the use of bilinear pairing operation; 2) failure of resisting bogus information from malicious users; and 3) the task of RSU on maintaining the revocation list and broadcasting the same to the authentic users.

In [54]. Cui et al. proposed a privacy-preserving authentication scheme for VANETs using group-key agreement. The scheme is built on cryptographic hash function that takes variable length data as input and outputs a fixed length hash value. In the scheme, the TA through through the RSU shares a group key using Chinese Remainder Theorem (CRT). While generating and sharing the group key among the group member, complicated operations like encryption and decryption are not needed. Moreover, when a vehicle leaves the group, the group key can be updated dynamically by the TA and vehicles within the group. The scheme is efficient and provides security features like privacy-preservation, unlinkability, traceability, non-repudiation, message integrity and anonymity. Moreover, the scheme is secure against replay attack and modification attack.

Islam et al. [55] proposed a conditional privacy-preserving authentication protocol using cryptographic hash functions. The scheme is based on Certificate authority-based public key cryptography (CA-PKC) and Identity-based public key cryptography (ID-PKC). In the protocol, while hashing the messages of any length, the resultant output is considered to be of fixed length. Facilities like password update, user join and leave, and group key generation is provided in the work. Security features like privacy-preservation, unlinkability, unforgeablity, message integrity and traceability are provided in the scheme. The scheme is also proposed to be secure against replay attack and modification attack.

Table 5 Hash and XOR operation based schemes

Security and Attacks	Schemes				
	[52]	[53]	[54]	[55]	[56]
Privacy Preservation	×	✓	✓	✓	✓
Unlinkability	×	✓	✓	✓	×
Traceability	✓	✓	✓	✓	×
Non-Repudiation	×	✓	×	×	×
Unforgeability	×	✓	✓	✓	×
Message Integrity	×	✓	✓	×	×
Anonymity	✓	✓	✓	✓	×
DoS	×	✓	×	×	×
MIM	✓	✓	×	×	×
Replay attack	✓	✓	✓	✓	✓
Sybil attack	×	×	×	×	×
Modification attack	✓	×	✓	✓	✓
Collusion attack	✓	✓	×	×	×

Gupta et al. [56] proposed an authentication protocol for VANET called Authentication-based Medium Access Control (A-MAC). To maintain security and privacy of the vehicles, authors utilized hash and XOR operations. The authenticating entity of the vehicles is TA, which monitors the vehicles within a region. TA provides parameters to all the vehicles for its communication. The architecture considered in the scheme is 5G cellular network. With hash and XOR operation the scheme is proposed to preserve privacy and withstand replay attack and modification attack.

6.1.4 Identity Based Cryptography (IBC) based schemes

Identity based schemes are almost similar to asymmetric key cryptography based schemes [8]. IBC based schemes uses a particular ID such as email, telephone number etc. to generate a public key. Because of this ID based schemes do not require certificates to prove the authenticity of the messages. Shamir proposed the idea to use a unique ID and thereby generate a public ID for exchanging messages in VANET [57]. As discussed in Subsection 6.1.2, the works of Wei et al. [47] uses identity based signature for providing authentication to the three parties i.e., the TA, RSU and vehicles. The advantage of ID based schemes is that it abstains the use of certificates, which is generally a overhead when there are large number of vehicles deployed on the road. However, the disadvantage of ID based schemes id that, it suffers from key escrow problem [58].

6.1.5 Homomorphic encryption based schemes

Homomorphic encryption allows computations over the encrypted data [59]. The advantage of homomorphic encryption is that multiple parties can perform arbitrary functions over the encrypted data (cipher text), without knowing its content. The final result will be same to the one if those functions were applied over the plain text. For example, let us consider that we want to perform the operation $u \times v + v$ without letting others know the plain-texts u

Table 6 Homomorphic encryption based schemes

Security and Attacks	Schemes			
	[62]	[63]	[64]	[65]
Privacy Preservation	✓	✓	✓	✓
Unlinkability	×	✓	×	✓
Traceability	✓	✓	✓	×
Non-Repudiation	✓	✓	×	×
Unforgeability	×	✓	×	✓
Message Integrity	✓	×	✓	✓
Anonymity	✓	✓	✓	✓
Scalability	×	×	×	✓
DoS	×	×	×	×
MIM	×	✓	×	×
Replay attack	×	✓	×	✓
Sybil attack	×	×	✓	×
Modification attack	×	×	✓	✓
Collusion attack	×	✓	×	✓

and v. Then according to homomorphic encryption, we first encrypt the plain texts u and v to cipher text as $ENC(u)$ and $ENC(v)$ respectively. Later, on computing $ENC(u \times v + v)$ we obtain same result as the homomorphic encryption $ENC(u) \times ENC(v) + ENC(v)$. Moreover, any search operation over the encrypted data can be performed and thereby enhances multi-party computation [60]. Homomorphic encryption was proposed by Rivest et al. in 1978 [61]. It can be categorised into three and they are partial, somewhat and fully homomorphic encryption. Partial homomorphic encryption allows selected mathematical operations on the encrypted data. Somewhat homomorphic encryption allows limited number of operations on the encrypted data that can be performed for a selected number of times. Fully homomorphic encryption multiple or infinite number of mathematical operations on the encrypted data. A summary of the ability to meet security requirements and robustness against attacks of the schemes using homomorphic encryption are tabulated in Table 6.

Prema et al. [62] proposed a secure data aggregation scheme which is based on pseudonym and fully homomorphic encryption. Though homomorphic encryption adheres high computation overhead with the security it provides, the authors proposed the use of pseudonym together with homomorphic encryption to reduce its computation overhead. The scheme allows computation on the encrypted data with two level decryption. Moreover, the scheme also provides re-encryption with homomorphism. The scheme is devised to facilitate security features like privacy-preservation, traceability, non-repudiation, message integrity and anonymity.

Kang et al. [63] presented a Randomized Authentication (RAU+) protocol for VANET using homomorphic encryption. The primary focus of the vehicle is to ensure privacy of the vehicle and provide traceability on liability issues. The two major entities involved in RAU+ are users' server and authentication server. The users' server include the vehicles enjoying the VANET services whereas the authentication server include the Registration Server (RS) and

Verification Server (VS). The scheme is proposed to preserve privacy of the vehicles and provide other security features like unlinkability, traceability, non-repudiation, unforgeability, anonymity. Moreover, the scheme is devised to withstand MIM attack, replay attack and collusion attack.

Farouk et al. [64], proposed a scheme with the use of Location Based Service (LBS) for location and tracking of the vehicles. However, tracking of a vehicle might lead to loss of location privacy of a vehicle. Therefore, to preserve its privacy, the authors proposed a scheme called Privacy-Preserving Fully Homomorphic Encryption over Advanced Encryption Standard (P2FHE-AES). Other than privacy, the scheme facilitates security features like traceability, message integrity and anonymity. The scheme is also robust against sybil attack and modification attack.

Tan et al. [65] proposed an authentication scheme considering the COVID-19 pandemic scenario. The authors devised the scheme for tracing the infected patients through novel cloud infrastructure and hybrid medical acquisition model. The scheme also implements decentralised blockchain to monitor route details of the VANET users. The vehicles together with the RSUs collaboratively update the blockchain by maintaining the confidentiality of the vehicles. Security features like privacy-preservation, unlinkability, unforgeability, message integrity, anonymity and scalability are provided in the scheme. Moreover, the scheme is based on certificate-less based encryption and thereby discourages attackers with key escrow problem. The scheme is proposed to withstand attacks like replay attack, modification attack and collusion attack.

6.2 Blockchain based authentication schemes

Block-chain is shared, immutable and distributed ledger that facilitates registering and tracking the transaction records of a business network. Other than financial transactions it has its potential of implementation in an IoT-based environment by creating a smart contract. [66][67] In VANET, implementing Distribute Ledger Technology (DLT) like block-chain or IOTA Tangle minimises the management of CRL by TA/CA. Thus, block-chain delegates the task of trusted third party like CA/TA, ensuring the vehicles with message integrity, anonymity and assures non-repudiation [68]. The feature of block-chain being decentralised and transparent adds to its advantage. Moreover, block-chain is immutable i.e., data once stored, cannot be modified. Table 5 illustrates the provided security requirements and robustness against security attacks in the paper [69], [70], [71] and [72].

In [69], Lu et al. proposed a distributed authentication scheme with a block-chain that uses the data structure called Chronological Merkle Tree (CMT) and Merkle Patricia Tree (MPT). The MPT is a combination of Merkle tree and Patricia tree. The data structures based in Merkle tree are chronological merkle tree and lexicographical merkle tree [73]. Generally, merkle tree is used to maintain data integrity and Patricia tree enables fast searching. In the Ethereum block-chain, each block utilizes the functionality of both the Merkle tree and Patricia tree. The three nodes of MPT, i.e. leave node, branch node

Table 7 Blockchain based schemes

Security and Attacks	Schemes			
	[69]	[70]	[71]	[72]
Privacy Preservation	✓	✓	×	×
Unlinkability	✓	✓	×	×
Traceability	✓	✓	✓	✓
Unforgeability	✓	✓	✓	×
Message Integrity	✓	✓	×	✓
Anonymity	×	✓	×	×
DoS	×	✓	✓	×
MIM	✓	✓	×	✓
Replay attack	✓	✓	×	✓
Sybil attack	×	×	×	✓
Modification attack	✓	×	✓	✓
Collusion attack	✓	✓	✓	×

and extension node contains the public key and encrypted link between the real ID and certificate, hash of the next node, and linkability of the parent-child node respectively. The scheme is proposed to achieve security features like privacy-preservation, unlinkability, traceability, unforgeability and message integrity. In addition, the authentic users can withstand replay attack, MIM attack, modification attack and collusion attack.

Ali et al. [70] proposed an efficient Certificateless Public Key Signature (CL-PKS) scheme to provide authentication and facilitate conditional privacy among the vehicles. The CL-PKS is built to minimize the computation overhead during signature generation and verification. To provide conditional privacy-preserving authentication in V2I communication, the scheme is built using the bilinear pairing operation. The features of block-chain allows transparent revocation of pseudo IDs. Security features like privacy-preservation, unlinkability, traceability, unforgeability, message integrity, anonymity are provided in the scheme. Moreover, the scheme is secure against replay attack, DoS, MIM attack, modification attack and collusion attack.

In [71], Ma et al. utilized the features of block-chain to enhance the flow of credentials among the entities in the VANET. The scheme is built using decentralised voting technique using smart contracts that detects malicious users in the VANET environment. The use of smart contracts allows automatic management of the user's parameters, which include registration, update and revocation of the user's public keys in the block-chain. The scheme also provides mutual authentication using bivariate polynomial, that enhances security in V2V and V2I communication. The scheme is proposed to achieve security features like traceability, unforgeability and is robust against modification attack, DoS and collusion attack.

The work in [72] by Dwivedi et al, proposed a block-chain based novel decentralised architecture for VANET. In the scheme, VANET information are not stored in the cloud rather leverage Interplanetary File System (IPFS) for storing information in a distributed manner. Other than its decentralised architecture, the authors also proposed a secure authentication protocol that can protect the event related information. To legitimize the data accessibility

among the vehicles using IPFS, the protocol is built on Ethereum smart contracts. The scheme is proposed to provide security features like traceability, message integrity and can withstand MIM attack, replay attack, sybil attack, modification attack.

6.3 Signature based schemes

There are several authenticating schemes in VANET that uses digital signature. The usage of digital signature in VANET schemes provides authentication, message integrity and non-repudiation [8]. In signature based schemes a user signs the message with the private key that was initially shared by a trusted third party. The receiver on receiving the message verifies the message with the public key that are distributed when a vehicle joins the VANET. Digital signature that are based in identity of a user is known as Identity Based Signature or IBS. In IBS, a user uses an identity to generate a public key. For exchanging the messages in IBS schemes, a user signs the message with the private key that is initially shared by a trusted third party. The signature based scheme can be divided into single entity signature and group signature. Since signature based schemes require two keys for exchanging messages in VANET; therefore, in our manuscript we have discussed the signature based schemes proposed by Azees et al. [44] and Shao et al. [45] in the Subsection 6.1.2.

6.4 Verification based schemes

With the dynamic nature of VANET, the vehicles are generally at tremendous high speed. Considering such a scenario, message flow at critical junctures must take place with minimal latency [74]. Moreover, a vehicle communicating with another vehicle must verify the received message and also act on it [75]. But verifying messages from a large number of vehicles calls for the need of batch verification of the messages [76]. The verification of messages can be classified as cooperative verification based authentication schemes and batch verification based authentication schemes. The ability to meet security requirements and defend various attacks of the schemes using co-operative and batch verification are summarised in Table 8.

Hao et al. [77] proposed a cooperative message authentication protocol in VANET, using distributed key management framework and group signature. Using group signatures the members can exchange information within the group. In a group there are vehicles with its individual group private key and a single group public key. A user can exchange messages using their individual group private key, which can later be verified by any authentic user using the unique group public key. The scheme is built considering short group signatures protocol for availing services with minimal communication overhead among the vehicles and can avail security features like privacy-preservation, traceability and message integrity. Moreover, the scheme can withstand sybil attack and collusion attack.

Table 8 Verification based schemes

Security and Attacks	Schemes			
	[77]	[78]	[79]	[80]
Privacy Preservation	✓	✓	✓	✓
Unlinkability	×	×	✓	×
Traceability	✓	✓	✓	×
Non-Repudiation	×	×	×	×
Unforgeability	×	×	✓	✓
Message Integrity	✓	✓	✓	×
Anonymity	×	✓	×	✓
DoS	×	×	×	×
MIM	×	×	×	✓
Replay attack	×	✓	×	✓
Sybil attack	✓	×	×	×
Modification attack	×	✓	✓	✓
Collusion attack	✓	×	×	✓

Zhang et al. [78] introduced an RSU aided scheme termed as RAISE. In the scheme, the RSU checks the authenticity of the messages that are exchanged and acknowledges the response messages among the vehicles. For privacy of the messages, RAISE utilizes the k-anonymity principle. Other than privacy-preservation, the scheme facilitates security features like traceability, message integrity and anonymity. The scheme also introduces an additional property called cooperative message authentication (COMET) where a vehicle can check the authenticity of the messages received without the aid of RSU. This is done by cooperating with the neighbouring vehicles. The scheme is also proposed to withstand security attacks like replay attack and modification attack.

In [79], Lin et al. proposed a cooperative authentication scheme for VANET. The scheme is built to minimize the authentication time by excluding the repetitive authentication over the same message. The scheme is built primarily to abstain free riding attacks by the malicious users. In addition, the scheme can withstand modification attack and provides security features likr privacy-preservation, unlikability, traceability, unforgeabilty and message integrity.

Wu et al. [80] devised a conditional privacy-preserving authentication scheme. With the help of ECC and batch message verification, the scheme is proposed to be efficient. The scheme also utilizes short-lived pseudonyms and partial secret key that are initially provided by the RSU to sign its message. The scheme facilitates security features like privacy-preservation, unforgeability, anonymity and is secure against MIM attack, replay attack, modification attack, collusion attack.

7 Discussions

As illustrated in Figure 5 there are different types of authentication schemes in VANET for providing security services to the vehicles. The schemes are classified according to the services they provide. However, each type of

authentication scheme has its own advantages and disadvantages. For example, symmetric cryptography based VANET schemes are efficient and fast compared to asymmetric cryptography based schemes. The phenomenon of preserving privacy during message exchange among authentic entities can be done with a minimal latency using symmetric cryptography method. Similarly, privacy-preserving authenticating schemes that use ECC during encryption/decryption or verification of signatures, require less storage space compared to the ones using traditional methodologies like RSA. In this section, we highlight the advantages and limitations of the existing schemes.

Symmetric cryptography based schemes: The symmetric cryptography based schemes are efficient and can meet the requirements of preserving privacy of the VANET entities. It is known for its simplicity and efficiency [81]. In the scheme of Wang et al. [38], the participating entities considered are vehicles, Key Management Centre (KMC) and RSUs. The KMC is a fully trusted entity which supervises registration of RSUs and vehicles, provides vehicle's real ID and keys to initiate VANET services. KMC is also in charge of verifying critical messages and trace malicious users. The RSUs are installed on the road to forward messages among the vehicles. It can communicate directly with KMC on VANET related queries. The vehicles in VANET exchange information among the vehicles with the help of OBUs that are equipped in them. Other than the OBU, each vehicle is also equipped with a TPD that store confidential information like secret key or other data used for performing cryptographic operations. In order to exchange information, the vehicles first sign the messages and then sent to other vehicles. However, though Wang et al. proposes not to use digital signature like most of the existing works, the authors made an exception to utilize the same during access token verification phase. Access token verification and message signing are the two phases of the scheme. Similarly, after a vehicle receives a message, it first verifies the message with two steps namely, access token verification and message verification. It can be observed from the scheme that the TPD has been assigned many tasks for authenticating a message. Moreover, as per the proposal, a TPD has four modules that include, authentication module, message signing module, message verification module and system key updating module. The inclusive works assigned to TPD can increase latency with large scale deployment of vehicles in VANET. Furthermore, in the scheme, the tokens are verified using bilinear pairing operation, which is computationally inefficient and time consuming considering the dynamic nature of VANET. In [41], proposed by Lim et al., the RSU generates and shares group key. Thus, considering vehicles deployed in a large scale, delegating the task of RSU will not only enhance the communication feasibility but also discourage an adversary to frame an attack. Vijayakumar et al., devised a scheme that leverage CRT for generating a common group key among the VANET entities [43]. Although the computation is efficient, but with gradual increase of key size, there is increase in overhead as well [82].

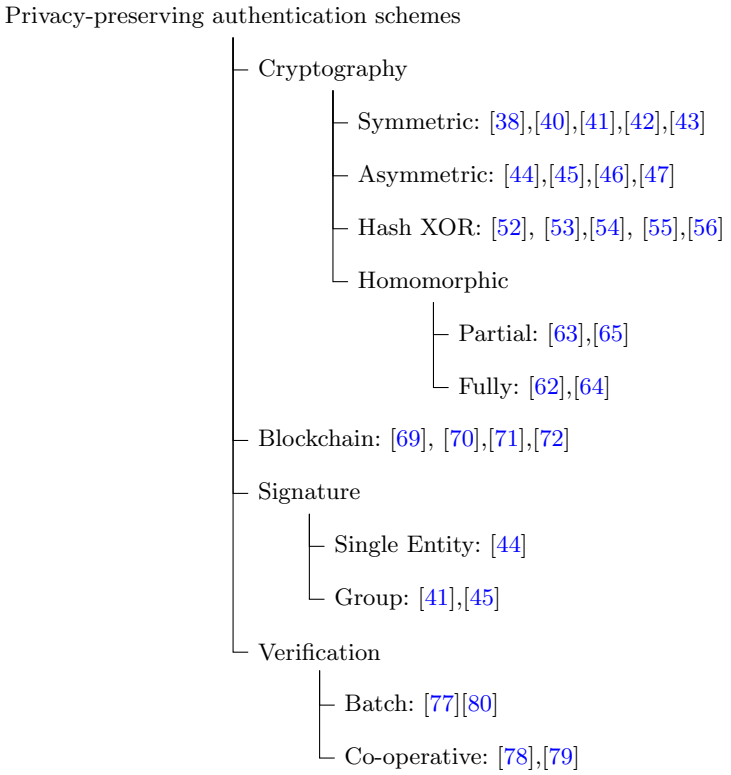


Fig. 5 Privacy-preserving authentication schemes.

Asymmetric cryptography based schemes: In asymmetric cryptography based schemes, there are two keys; one is the private key and the other is public key. The private key is known only to the users of the VANET whereas public key is shared with others as well. In [44], Azees et al. proposed an authentication schemes using bilinear pairing and digital signature. Similarly, in [45], Shao et al. introduced a novel authentication protocol called new group signature scheme. The phases involved in new group signature are: 1. Setup, where a group manager, and all the group member sets their own public/private key. 2. CertGen, where group manager generates certificate using its private key and one of the group members' public key. 3. Sign, where a group member signs the message and outputs eleven signatures. 4. Verify, where a receiver verifies by taking the received signatures and the public key of both group manager and group tracer. Using bilinear pairing equations, the received credentials are verified. 5. Open, where a group tracer has the capability of tracing a group member. The threshold authentication is achieved by a threshold anonymous authentication protocol consisting the steps: 1. Initialization, 2. Registration, 3. Join, 4. Verify, 5. Trace and 6. Verification. Together with threshold authentication and batch message verification technique, the scheme is proposed to be secure. Though the scheme is featured with threshold authentication,

anonymity, traceability and forgeability of messages, but the scheme possess many computations while generating digital signatures. Moreover, the scheme utilizes bilinear pairing operations during verification and signing of messages, which is not practical considering the dynamic nature of VANET. In [46], Chim et al. proposed navigation-based positioning for the vehicles that would ease communication in VANET. But in the scheme, RSUs need to share the master keys to the vehicles, and assigning such a crucial task to RSUs with large number of vehicles is tremendously challenging in real life. In [47], Wei et al. proposed a privacy-preserving scheme that uses Identity based signature, where RSU is assigned to convert OBU's signature into TA's signature. But, the scheme suffers from common modulus attack, because an RSU can obtain the private key of the OBU [83].

Hash function and XOR operation based schemes: These schemes are the most efficient and lightweight compared to other types of VANET schemes. Moreover, it enhances the message flow with minimal latency and avoids complex operation for privacy preservation [84]. Wazid et al. developed a lightweight authentication and key agreement scheme for VANET [52]. The entities in the scheme are vehicles (V), cluster heads (CH), application server (AS), RSUs and TAs. For exchanging information among the entities, the following types of communication takes place: vehicle to vehicle (V2V), vehicle to cluster head (V2CH), cluster head to RSU (CH2RSU) and RSU to RSU (RSU2RSU). The CH is chosen in such a way that it is tactically placed within a region and can communicate easily with all other vehicles within that region. The selection of CH is crucial and the scheme follows the similar steps involved in the work of Bali et al. [85]. Moreover, the authentication procedure involved in the communications during V2V, V2CH, CH2RSU and RSU2RSU are carried out following different steps in the scheme, thereby stating the dynamic nature of the scheme. Other than these, the OBU can update password to maintain its freshness. New RSU can be added in the VANET environment dynamically. The simulation results proves the scheme to be secure and efficient. In [53], Alazzawi et al. developed a pseudo ID based authentication scheme with message integrity. The work focuses in the shortcomings of the ID based scheme. In the scheme, when a vehicle visits the area of RSU, it requests the RSU with a message (containing its pseudonym and timestamp) to avail its services. RSU on receiving the request message from the vehicle, communicates with TA for verifying the request message. TA first validates the timestamp of the message from RSU. If valid, TA checks the message containing the pseudonym, on whether or not a real ID is assigned with respect to the pseudonym. If it has, then TA replies RSU with a {verified} message, else TA replies RSU with a {not verified} message. In a similar manner, RSU with the verification message from TA validates authentic vehicles and thereby provides digital signature to the authentic vehicles. The vehicles with the help of the provided digital signature by an RSU can communicate with other vehicles (or RSUs) within its region. Although the scheme is built to satisfy many of the privacy requirements, but it has not considered unlinkability of the pseudo IDs. In

[54], using group key agreement and Chinese Remainder Theorem (CRT), Cui et al. proposed a privacy-preserving authentication scheme for VANET. The scheme consists of following phases: 1.System initialization phase, where TA generates system parameters. 2.RSU registration phase, where RSU registers in VANET environment. 3.Vehicle registration phase, where the vehicle sends its ID to TA for receiving the parameters for exchanging information in VANET. 5.Authentication message generation phase, where a vehicle generates anonymous ID to exchange messages. 6.Authentication message verification phase, where TA and RSU validates the received messages from the vehicles. 7.Group-key generation phase, where the TA generates the group key using Chinese Remainder Theorem (CRT). TA later sends the newly generated group key with its current timestamp to each vehicle. 8.Vehicle joining phase, where the TA updates the group key and sends the newly updated group key to all the vehicles, and 9.Vehicle leaving phase, where TA updates the group key when a vehicle leaves the group. It can be observed from the mentioned steps that TA needs to authenticate and verify the messages before they can be exchanged by the OBU. During verification, the scheme do not follow batch verification mechanism, which can delay the availability of services in VANET. Moreover, the group key is generated by the TA, using which the vehicles communicate among itself. Thus, it can be stated that TA individually needs to tackle the dynamic nature of VANET with many tasks, which is not practical in real life scenarios. In [55], Islam et al. developed a conditional privacy-preserving authentication scheme. The protocol consists of nine phases, which are: (i) System initialization phase, where TA initiates the VANET services by generating the system parameters; (ii) RSU registration phase, where the user (vehicle) selects its real ID and password to compute a hash value. The vehicle then sends hashed value to TA. TA further utilizes the ID, received hash value and its secret key to compute another hash value. TA stores the hashed value and credentials in the OBU of the vehicle; (iii) Vehicle registration phase, where vehicle requests TA using its unique ID and password to avail its service for exchanging message in VANET. TA after receiving the request, inspects the information and embeds its credentials in the OBU. The OBU is then delivered to the owner of the vehicle using a secure communication medium; (iv) Authentication message generation phase, where the vehicle generates authentication message using the information from the TA. The generated message is then sent to RSU over public channel by adding its timestamp. The RSU after receiving the message from vehicle, forwards the message to the TA by adding its ID and timestamp; (v) Authentication message verification phase: After the authentication message of the vehicle is sent to the RSU, which in turn is sent to TA, verification of the received message takes place. In this phase, TA checks the authenticity of both the RSU and the vehicle. After the authentication of both RSU and vehicle has been done by TA, it provides the group key to the vehicles within the region of the RSU; (vi) Group-key generation phase: In this phase, a vehicle initially sends authentication message to the RSU, which is forwarded to TA. Then the TA unicast the group key

to the newly arrived vehicle; (vii) Vehicle leaving phase; (viii) Vehicle joining phase; and (ix) Vehicle password change phase. In the authentication message generation phase, the vehicle generates an anonymous ID using the credentials provided by TA. Gupta et al. proposed authentication protocol for VANET called A-MAC, which is 5G based [56]. The novel authentication based secure data dissemination protocol that use lightweight encryption mechanism with few parameters and thereby achieves minimal computational overhead.

Homomorphic encryption based schemes: In homomorphic encryption based schemes, computations can be done over the encrypted data. With Fully Homomorphic Encryption (FHE) Prema et al. proposed a data aggregation scheme that preserves information of the users and minimizes rush hour traffic [62]. The scheme is also built utilizing the benefits of pseudonyms; i.e., using the pseudonym re-encryption mechanism, FHE is achieved. The entities involved in the scheme are Infrastructure Node (IN), RSU and Vehicle Unit (VU) with its OBU installed in it. The entities are interconnected to each other and thereby exchange information among themselves. The public key is shared by the RSU when a new pseudonym is created by the vehicle. The RSU also timely broadcast credentials to all the vehicles within a confined area. However, a vehicle can generate and update its own pseudonym. Using the pseudonym, a VU can preserve its identity and thereby achieve anonymity. Other than the OBU for performing the computational task of the VU, there are entities like Data Service or DS (which performs the computation and provides intercommunication among the nodes of VANET), Access Servers or AS (which performs computation on the data that are exchanged among the vehicles) and Data Encrypts or DE (which analysis the message exchange and encrypts the pseudonym of the vehicle), that are included on the system design for providing secure communication among the vehicles. Similarly, in [63], Kang et al. proposed an authentication scheme for VANET using homomorphic encryption. In the scheme, the vehicle registers itself with the Registration Server (RS), where it attains an anonymous authentication ID and secret key. The vehicles can then generate its own pseudo ID, which is confirmed by the Verification Server (VS). After the verification of the pseudo ID from the VS, a vehicle can communicate with other vehicles through a secure channel. However, on any malicious act by a user, the RS and VS can reveal the real ID. During the communication, the messages that are exchanged among the entities are encrypted using the Pallier Encryption mechanism. However, if large number of vehicles are deployed in the road, the resultant computation overhead becomes extremely large [86]. In [64], Farouk et al. proposed a privacy-preserving scheme for location services in VANET. The scheme is built to preclude noise associated with data that are related to Location Based Services (LBS). Moreover, the scheme is based on FHE and Advanced Encryption Standard (AES). But computing homomorphic operation over a cipher-text accumulates noise component, which can eventually make decryption of cipher-text difficult. In [65], Tan et al. developed a homomorphic encryption based privacy-preserving authentication scheme for cloud assisted VANET. To monitor the route information of

the VANET users, decentralized blockchain is used. But the authors did not consider the scalability of the exchanged messages and the Vehicle-to-Vehicle connectivity.

Blockchain based schemes: The blockchain based authentication schemes are efficient and secure considering the distributed and dynamic nature of the vehicles in VANET. Lu et al. proposed a privacy-preserving authentication scheme for VANET that is base on VANET. The scheme is considered to have a Law Enforcement Authority (LEA) that registers vehicles and monitors the messages exchanged among the vehicles. Moreover, the LEA authorizes Certifying Authority (CA) to distribute certificates among the vehicles. The CA under the supervision of LEA generates and sends the block to all the RSUs for verification. The real ID of all the vehicles is known only to the LEA. Furthermore, with the secret key of the LEA, the real ID and its corresponding certificate of a vehicle is encrypted. The activities performed by CA and LEA can be verified by all the entities of the VANET environment. LEA provides public/private key to RSU and its task is to add information in the block-chain that are verified by the CA. The RSU then sends updated information to each vehicle. The performance of all the involved entities of the scheme is evaluated using Hyperledger Fabric (HLF) platform and is found that the receivers can authenticate the information within 1 milliseconds. However, a vehicle is assumed to possess multiple certificates. This would eventually increase the computation overhead of the CA when there are large number of vehicles in VANET. Another work on VANET that uses blockchain was proposed by Ali et al [70]. The work is based on bilinear pairing operation and do not use certificates for verifying the messages that are exchanged. The entities involved in the scheme are OBUs, RSUs, Application Server (AS) and Trusted Authority (TA). The AS is assigned to send verified information to the RSUs so that it can broadcast the provided information to OBUs within its coverage area. The TA that monitors the entire VANET, is divided into two and they are Tracing Authority (TRA) and Key Generation Centre (KGC). The TRA registers the RSUs and vehicles and provides pseudo-IDs to the vehicles. The KGC, on the other hand, creates and assigns partial private key to the vehicles. However, the receiving vehicle verifies the partial private key by using a bilinear pairing operation. The RSU also verifies the receiving information from vehicle(s) using complex bilinear pairing operations.The scheme also supports batch and aggregate signature verification and hence, considering there are large number of vehicles on the road, the scheme has the capability to minimize the computation time. The robustness of the scheme is proved using Random Oracle Model (ROM), where the authors have successfully shown the scheme to withstand Type 1 and Type 2 adversary. In [71], Ma et al. proposed a lightweight authentication and key agreement scheme for VANET. For increasing security during V2V and V2I communication, the scheme uses bivariate polynomial for providing the session keys among the VANET entities. The entities involved in the scheme are Vehicle Service Provider (VSP), Block-chain Network (BN) and vehicles. The issuance of the block-chain, smart contracts and other data

transaction for the users are established by the VSP. The RSUs provide public keys and avails services to the vehicles. RSUs also acts as a miner and thereby create new blocks when required. Each vehicle in VANET is equipped with a OBU that can communicate with other vehicles within a particular range. Furthermore, a Hardware Security Model (HSM) that stores cryptographic credentials is installed in each of the VSPs, RSUs and vehicles. Similarly, in [72], Dwivedi et al. devised blockchain based authentication protocol in VANET. The protocol uses IPFS and blockchain for recording the events of the VANET entities. The entities involved in the scheme are Network Administrator (NA), RSU and vehicles. Initially the RSUs visits and registers themselves to the NA. Each RSU acquires the common key from NA. Later, one of the RSU updates the common key and distributes it to the other RSUs. However, the task of RSU is to register the vehicles. With the registration credentials obtained from NA, the RSU creates the block and performs the block validation procedure. After successful verification, the RSU provides the index block to the vehicle. The vehicle after a successful challenge response with the RSU, avails the VANET services. But the scheme did not mention about the vehicle to vehicle communication.

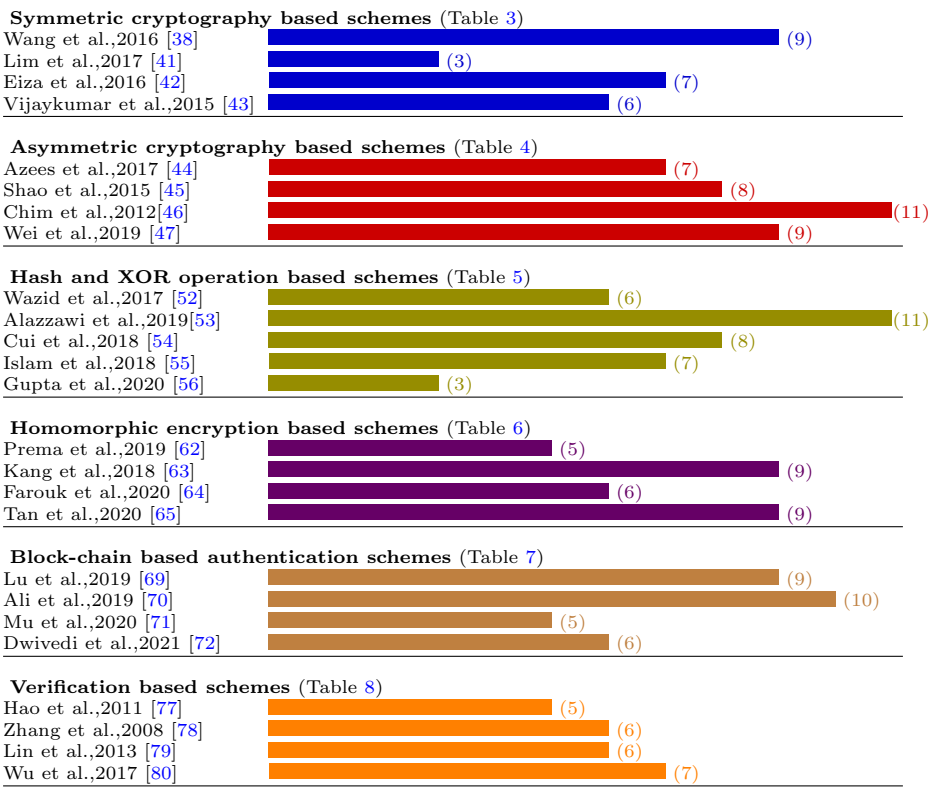
Verification based schemes: In verification based authentication schemes, the messages are simultaneously verified by the receiver. With large number of vehicles plying on the road, verifying messages from each vehicle is a tedious job, leading to multiplication of the computation overhead. In [77], Hao et al. proposed a co-operative message authentication protocol for VANET. The protocol leverage short signature for its smaller communication overhead. In the short group signature protocol there is a generator for availing group private key to key distributors. This provides any third party other than the sender and the receiver to act as a key distributor. Moreover, the short group signature possess a tracing key which allows authorities to retrieve group private key from the signature. The short group signature has the following working stages: 1. Key setup, 2. Membership distribution, 3. Signing and verification, 4. Key retrieve. In the scheme, bilinear pairing is used for generating the keys in the key setup phase, membership registration phase and key retrieve phase, which is time consuming. Furthermore, the scheme facilitates large scale exchange of message with the Cooperative Message Authentication (CMA) protocol and at the same time minimizes the computation overhead of a verifier in VANET. The CMA protocol contains two processes that are maintained by the vehicles and they are: 1. Verifier selection process and 2. Cooperative authentication process. In the verifier selection process, a vehicle verifies other vehicles, maintains a list of nearby vehicles. The cooperative authentication process is in charge of message authentication and alert messages. The messages that are exchanged can be categorised as Regular Broadcast Message (RBM) and Cooperative Authentication Message (CAM). When a vehicle receives a regular message or RBM, it verifies the received data like speed, location, acceleration and direction. If the received data are not valid, then the vehicle prepares a one

hop alert message to its nearby vehicle termed as CAM. Any vehicle on receiving CAM, authenticates its corresponding RBM and then decides whether the message is valid or invalid to be dropped. But the messages are verified without looking into the revocation list that is maintained by the RSU. At the same time, frequent involvement of the RSU for authenticating the messages is not practical in real life scenario. Similarly, in [78], Zhang et al. introduced privacy-preserving authentication schemes that uses RSU for verifying the messages that are being exchanged. It utilizes the k-anonymity principle for preserving privacy of the vehicles. But, if there are large number of vehicles in VANET, the k-anonymity principle becomes inefficient and time consuming. In [79], the authors proposed a co-operative authentication scheme that do not require constant monitoring of the TA. The main focus is to discourage the free riding attack. This is achieved using the ID-based signcryption (IBSC) mechanism which consists of following steps: setup, key generation, token generation, signcryption, and decryption and verification. While generating the token bilinear pairing operation is used [87] [88]. With IBSC free riding attack is shielded by exchanging tokens among the authentic users during the communication which were initially provided by TA. The TA distributes the token among the users with a validity. The authentic users can utilize the tokens only within the provided time frame. After a user has requested for a cooperative authentication, the TA verifies using bilinear pairing operation. Performance analysis shows the scheme to be efficient for its cooperative approach and can meet the challenges of the dynamic nature of VANET. In [80] utilizing the batch verification mechanism, Wu et al. have proposed a privacy-preserving authentication scheme for VANET. The scheme uses random short lived pseudonyms that are provided by RSUs. But generation of short-lived pseudonyms, is inefficient considering a vehicle communicating over long distance.

8 Analysis and Future Direction

Security features like privacy preservation and robustness to various kinds of security attacks involve complex computations and hence is always an overhead on normal communication. On the other hand, the effectiveness of any authentication scheme depends on the computational efficiency and their adaptability with the dynamic VANET environment. Therefore, there must be a balance between the number of security features/attacks fulfilled/resisted by an authentication scheme and its overall computational cost. An ideal authentication scheme must fulfil majority of the security requirements and resist majority of the security attacks with minimum computational cost. Table 9 graphically presents the security schemes considered in this article with reference to their type and number of security features/attacks that they fulfil/withstand. From this table, it is noticeable that the privacy preserving authenticating schemes that leverage asymmetric key cryptography (with an average of approximately 9 features) fulfil/withstand a greater number of security features/attacks than authentication schemes based on all the other types.

Table 9 Comparative analysis of the discussed schemes based on security features and attacks that are addressed



In spite of this, it seems that in recent times more researchers have started exploring the use of other techniques like homomorphic encryption, hash-XOR operations and blockchain for devising authentication schemes for VANET. This could be due to the resource intensive computations that are involved with asymmetric key cryptography. It is a known fact that asymmetric key cryptography is almost one thousand times slower than symmetric key cryptography. However, as evident from Table 9, symmetric key cryptography also does not give the desired result (with an average of only 6 features). Blockchain (with an average of approximately 8 features) and hash-XOR (with an average of approximately 7 features) looks to be promising solutions for devising effective authentication schemes. The effectiveness of homomorphic encryption-based schemes needs to be further explored and more research work needs to be carried out using this method as prominent works using this method in this area were carried out only in recent times between 2019 and 2020. We therefore, based on the above discussion, highlight the following future scope of work in this area.

- Asymmetric key cryptography has the potential to fulfil a large number of security requirements and has the potential to withstand a number of security attacks. However, it is computationally intensive and may not give the best results in terms of performance in the dynamic VANET environment. Therefore, use of lightweight asymmetric cryptographic techniques like Elliptic Curve Cryptography needs to be further explored.
- Use of a combination of emerging techniques like hash-XOR, blockchain, homomorphic encryption, etc., with traditional techniques like asymmetric cryptography to develop hybrid solutions, in order to reap the benefits of various techniques in a single solution, needs to be further explored.
- There is not much works with regards to privacy preservation during VANET authentication in evolving cellular technologies like 5G mobile networks. Due to commercial success of cellular technologies, implementation of VANET through cellular networks and related issues like security, privacy, etc., presents immense scope for further research.

9 Conclusion

VANET is set to play an important role with regards to safety, comfort and entertainment of people travelling on the road. It will allow commuters to communicate among themselves and with the infrastructure by exchanging messages. However, since the messages in VANET are transmitted through radio signals, they are open for access to eavesdroppers; thereby making the communications vulnerable to various kinds of security attacks. Therefore, there is a need for devising effective and efficient authentication schemes for VANET. The schemes should be developed in such a way that the privacy of the users, an important security concern in modern times, is preserved. Several privacy preserving authentication schemes and protocols were proposed for VANET in recent times. We felt that there is a requirement to make a comprehensive review on these works so that an estimate of the types of works being carried out and progress made so far be made; in this paper, an effort is made in this regard. Based on the review, it is our observation that asymmetric key cryptography-based schemes have the potential to fulfil a large number of security requirements and have the potential to withstand a number of security attacks. However, they are computationally intensive and may not give the best results in terms of performance in the dynamic VANET environment. Therefore, use of lightweight asymmetric cryptographic techniques like elliptic curve cryptography needs to be further explored. It is also felt that combination of emerging techniques like hash-XOR, blockchain, homomorphic encryption, etc., with traditional techniques like asymmetric cryptography may lead to an effective solution. Work on developing privacy preserving security schemes for VANET implementations through commercially successful and emerging infrastructure-based networks like 4G/5G cellular networks also requires to be carried out, as there is not much work in this area.

Declarations

The work presented in this paper is funded by Cyber Security R&D Division, Ministry of Electronics and Information Technology (MeitY), Government of India (AAA-22/2/2021-CSRD-MeitY)

Ethical Statements

No humans or animals were involved in the research work presented in this paper.

References

[1] Singh, A., Kumar, M., Rishi, R., Madan, D.: A relative study of manet and vanet: Its applications, broadcasting approaches and challenging issues. In: International Conference on Computer Science and Information Technology, pp. 627–632 (2011). Springer

[2] Mansour, M.B., Salama, C., Mohamed, H.K., Hammad, S.A.: Vanet security and privacy-an overview. International Journal of Network Security & Its Applications (IJNSA) Vol **10** (2018)

[3] Kaushik, S.S.: Review of different approaches for privacy scheme in vanets. International Journal of Advances in Engineering & Technology **5**(2), 356 (2013)

[4] Sommer, C., Dressler, F.: Vehicular Networking. Cambridge University Press, Cambridge, UK (Dec, 2014). https://doi.org/10.1017/CBO9781107110649

[5] Biswas, S., Mišić, J., Mišić, V.: Ddos attack on wave-enabled vanet through synchronization. In: 2012 IEEE Global Communications Conference (GLOBECOM), pp. 1079–1084 (2012). IEEE

[6] Taleb, T., Sakhaee, E., Jamalipour, A., Hashimoto, K., Kato, N., Nemoto, Y.: A stable routing protocol to support its services in vanet networks. IEEE Transactions on Vehicular technology **56**(6), 3337–3347 (2007)

[7] Jindal, V., Bedi, P.: Vehicular ad-hoc networks: introduction, standards, routing protocols and challenges. International Journal of Computer Science Issues (IJCSI) **13**(2), 44 (2016)

[8] Manvi, S.S., Tangade, S.: A survey on authentication schemes in vanets for secured communication. Vehicular Communications **9**, 19–30 (2017)

[9] Sheikh, M.S., Liang, J.: A comprehensive survey on vanet security services in traffic management system. Wireless Communications and Mobile

Computing **2019** (2019)

[10] Mundhe, P., Verma, S., Venkatesan, S.: A comprehensive survey on authentication and privacy-preserving schemes in vanets. Computer Science Review **41**, 100411 (2021)

[11] Azam, F., Yadav, S.K., Priyadarshi, N., Padmanaban, S., Bansal, R.: A comprehensive review of authentication schemes in vehicular ad-hoc network. IEEE Access **9**, 31309–31321 (2021)

[12] Gao, S., Lim, A., Bevly, D.: An empirical study of dsrc v2v performance in truck platooning scenarios. Digital Communications and Networks **2**(4), 233–244 (2016)

[13] Kenney, J.B.: Dedicated short-range communications (dsrc) standards in the united states. Proceedings of the IEEE **99**(7), 1162–1182 (2011)

[14] Morgan, Y.L.: Notes on dsrc & wave standards suite: Its architecture, design, and characteristics. IEEE Communications Surveys & Tutorials **12**(4), 504–518 (2010)

[15] Bi, S., Chen, C., Du, R., Guan, X.: Proper handover between vanet and cellular network improves internet access. In: 2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall), pp. 1–5 (2014). IEEE

[16] Lai, C., Zheng, D., Zhao, Q., Jiang, X.: Segm: A secure group management framework in integrated vanet-cellular networks. Vehicular Communications **11**, 33–45 (2018)

[17] Engoulou, R.G., Bellaïche, M., Pierre, S., Quintero, A.: Vanet security surveys. Computer Communications **44**, 1–13 (2014)

[18] Biswas, S., Mišić, J.: A cross-layer approach to privacy-preserving authentication in wave-enabled vanets. IEEE Transactions on Vehicular Technology **62**(5), 2182–2192 (2013)

[19] More, H.R., Digrase, A.A., Wayse, A.V.: Linear pid control technique for single wheel abs (anti-lock braking system) of motorcycle. In: 2017 2nd International Conference for Convergence in Technology (i2ct), pp. 277–281 (2017). IEEE

[20] Luckshetty, A., Dontal, S., Tangade, S., Manvi, S.S.: A survey: comparative study of applications, attacks, security and privacy in vanets. In: 2016 International Conference on Communication and Signal Processing (ICCSP), pp. 1594–1598 (2016). IEEE

[21] Sumra, I.A., Ahmad, I., Hasbullah, H., *et al.*: Behavior of attacker and

some new possible attacks in vehicular ad hoc network (vanet). In: 2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 1–8 (2011). IEEE

[22] Hasrouny, H., Samhat, A.E., Bassil, C., Laouiti, A.: Vanet security challenges and solutions: A survey. Vehicular Communications **7**, 7–20 (2017)

[23] Zhang, J., Zheng, K., Zhang, D., Yan, B.: Aatms: An anti-attack trust management scheme in vanet. IEEE Access **8**, 21077–21090 (2020)

[24] Papadimitratos, P., Gligor, V., Hubaux, J.-P.: Securing vehicular communications-assumptions, requirements, and principles (2006)

[25] Anita, E.M., Jenefa, J.: A survey on authentication schemes of vanets. In: 2016 International Conference on Information Communication and Embedded Systems (ICICES), pp. 1–7 (2016). IEEE

[26] Manivannan, D., Moni, S.S., Zeadally, S.: Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (vanets). Vehicular Communications **25**, 100247 (2020)

[27] Mishra, R., Singh, A., Kumar, R.: Vanet security: Issues, challenges and solutions. In: 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 1050–1055 (2016). IEEE

[28] Wagan, A.A., Jung, L.T.: Security framework for low latency vanet applications. In: 2014 International Conference on Computer and Information Sciences (ICCOINS), pp. 1–6 (2014). IEEE

[29] Rajput, U., Abbas, F., Eun, H., Oh, H.: A hybrid approach for efficient privacy-preserving authentication in vanet. IEEE Access **5**, 12014–12030 (2017)

[30] He, D., Zeadally, S., Xu, B., Huang, X.: An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Transactions on Information Forensics and Security **10**(12), 2681–2691 (2015)

[31] Sakai, Y., Emura, K., Hanaoka, G., Kawai, Y., Matsuda, T., Omote, K.: Group signatures with message-dependent opening. In: International Conference on Pairing-Based Cryptography, pp. 270–294 (2012). Springer

[32] Shrestha, R., Kim, S.: Integration of iot with blockchain and homomorphic encryption: Challenging issues and opportunities. In: Advances in Computers vol. 115, pp. 293–331. Elsevier, ??? (2019)

[33] Han, W., Xiao, Y.: Privacy preservation for v2g networks in smart grid: A survey. Computer Communications **91**, 17–28 (2016)

[34] Bunese, E.E., Todt, E., Albini, L.C.P.: Vanet security through group broadcast encryption. Journal of Computer and Communications **8**(8), 22–35 (2020)

[35] Kumar, N., Iqbal, R., Misra, S., Rodrigues, J.J.: An intelligent approach for building a secure decentralized public key infrastructure in vanet. Journal of Computer and System Sciences **81**(6), 1042–1058 (2015)

[36] Nath, H.J., Choudhury, H.: A privacy-preserving mutual authentication scheme for group communication in vanet. Computer Communications **192**, 357–372 (2022)

[37] Alimohammadi, M., Pouyan, A.: Performance analysis of cryptography methods for secure message exchanging in vanet. International Journal of Scientific & Engineering Research **5**(2), 912 (2014)

[38] Wang, M., Liu, D., Zhu, L., Xu, Y., Wang, F.: Lespp: lightweight and efficient strong privacy preserving authentication scheme for secure vanet communication. Computing **98**(7), 685–708 (2016)

[39] Ren, K., Lou, W., Kim, K., Deng, R.: A novel privacy preserving authentication and access control scheme for pervasive computing environments. IEEE Transactions on Vehicular technology **55**(4), 1373–1384 (2006)

[40] Liu, X., Xia, Y., Chen, W., Xiang, Y., Hassan, M.M., Alelaiwi, A.: Semd: Secure and efficient message dissemination with policy enforcement in vanet. Journal of Computer and System Sciences **82**(8), 1316–1328 (2016)

[41] Lim, K., Tuladhar, K.M., Wang, X., Liu, W.: A scalable and secure key distribution scheme for group signature based authentication in vanet. In: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), pp. 478–483 (2017). IEEE

[42] Eiza, M.H., Ni, Q., Shi, Q.: Secure and privacy-aware cloud-assisted video reporting service in 5g-enabled vehicular networks. IEEE Transactions on Vehicular Technology **65**(10), 7868–7881 (2016)

[43] Vijayakumar, P., Azees, M., Kannan, A., Deborah, L.J.: Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems **17**(4), 1015–1028 (2015)

[44] Azees, M., Vijayakumar, P., Deboarh, L.J.: Eaap: Efficient anonymous

authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems **18**(9), 2467–2476 (2017)

[45] Shao, J., Lin, X., Lu, R., Zuo, C.: A threshold anonymous authentication protocol for vanets. IEEE Transactions on vehicular technology **65**(3), 1711–1720 (2015)

[46] Chim, T.W., Yiu, S.-M., Hui, L.C., Li, V.O.: Vspn: Vanet-based secure and privacy-preserving navigation. IEEE Transactions on Computers **63**(2), 510–524 (2012)

[47] Wei, Z., Li, J., Wang, X., Gao, C.-Z.: A lightweight privacy-preserving protocol for vanets based on secure outsourcing computing. IEEE Access **7**, 62785–62793 (2019)

[48] Malik, A., Pandey, B.: Asymmetric encryption based secure and efficient data gathering technique in vanet. In: 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence, pp. 369–372 (2017). IEEE

[49] Alwan, M.H., Ramli, K.N., Al-Jawher, Y.A., Sameen, A.Z., Mahdi, H.F.: Performance comparison between 802.11 and 802.11 p for high speed vehicle in vanet. International Journal of Electrical and Computer Engineering **9**(5), 3687 (2019)

[50] Goyal, A.K., Tripathi, A.K., Agarwal, G.: Security attacks, requirements and authentication schemes in vanet. In: 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), vol. 1, pp. 1–5 (2019). IEEE

[51] El-Hajj, M., Fadlallah, A., Chamoun, M., Serhrouchni, A.: A survey of internet of things (IoT) authentication schemes. Sensors **19**(5), 1141 (2019)

[52] Wazid, M., Das, A.K., Kumar, N., Odelu, V., Reddy, A.G., Park, K., Park, Y.: Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks. IEEE Access **5**, 14966–14980 (2017)

[53] Alazzawi, M.A., Lu, H., Yassin, A.A., Chen, K.: Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network. IEEE Access **7**, 71424–71435 (2019)

[54] Cui, J., Tao, X., Zhang, J., Xu, Y., Zhong, H.: Hcpa-gka: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for vanets. Vehicular communications **14**, 15–25 (2018)

[55] Islam, S.H., Obaidat, M.S., Vijayakumar, P., Abdulhay, E., Li, F., Reddy, M.K.C.: A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for vanets. Future Generation Computer Systems **84**, 216–227 (2018)

[56] Gupta, N., Manaswini, R., Saikrishna, B., Silva, F., Teles, A.: Authentication-based secure data dissemination protocol and framework for 5g-enabled vanet. Future Internet **12**(4), 63 (2020)

[57] Shamir, A.: Identity-based cryptosystems and signature schemes. In: Workshop on the Theory and Application of Cryptographic Techniques, pp. 47–53 (1984). Springer

[58] Patel, M., Patel, R.: Improved identity based encryption system (iibes): A mechanism for eliminating the key-escrow problem. Emerging Science Journal **5**(1), 77–84 (2021)

[59] Gentry, C.: "A fully homomorphic encryption scheme". PhD dissertation, Stanford university (2009)

[60] Sun, X., Yu, F.R., Zhang, P., Xie, W., Peng, X.: A survey on secure computation based on homomorphic encryption in vehicular ad hoc networks. Sensors **20**(15), 4253 (2020)

[61] Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM **21**(2), 120–126 (1978)

[62] Prema, N.: Efficient secure aggregation in vanets using fully homomorphic encryption (FHE). Mobile Networks and Applications **24**(2), 434–442 (2019)

[63] Kang, J., Lin, D., Jiang, W., Bertino, E.: Highly efficient randomized authentication in vanets. Pervasive and Mobile Computing **44**, 31–44 (2018)

[64] Farouk, F., Alkady, Y., Rizk, R.: Efficient privacy-preserving scheme for location based services in vanet system. IEEE Access **8**, 60101–60116 (2020)

[65] Tan, H., Kim, P., Chung, I.: Practical homomorphic authentication in cloud-assisted vanets with blockchain-based healthcare monitoring for pandemic control. Electronics **9**(10), 1683 (2020)

[66] Aggarwal, S., Kumar, N.: Basics of blockchain. In: Advances in Computers vol. 121, pp. 129–146. Elsevier, ??? (2021)

[67] Zachariadis, M., Hileman, G., Scott, S.V.: Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. Information and Organization **29**(2), 105–117 (2019)

[68] Xu, Y., Ren, J., Wang, G., Zhang, C., Yang, J., Zhang, Y.: A blockchain-based nonrepudiation network computing service scheme for industrial iot. IEEE Transactions on Industrial Informatics **15**(6), 3632–3641 (2019)

[69] Lu, Z., Wang, Q., Qu, G., Zhang, H., Liu, Z.: A blockchain-based privacy-preserving authentication scheme for vanets. IEEE Transactions on Very Large Scale Integration (VLSI) Systems **27**(12), 2792–2801 (2019)

[70] Ali, I., Gervais, M., Ahene, E., Li, F.: A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in vanets. Journal of Systems Architecture **99**, 101636 (2019)

[71] Ma, Z., Zhang, J., Guo, Y., Liu, Y., Liu, X., He, W.: An efficient decentralized key management mechanism for vanet with blockchain. IEEE Transactions on Vehicular Technology **69**(6), 5836–5849 (2020)

[72] Dwivedi, S.K., Amin, R., Vollala, S.: Blockchain-based secured ipfs-enable event storage technique with authentication protocol in vanet. IEEE/CAA Journal of Automatica Sinica **8**(12), 1913–1922 (2021)

[73] Lu, Z., Liu, W., Wang, Q., Qu, G., Liu, Z.: A privacy-preserving trust model based on blockchain for vanets. Ieee Access **6**, 45655–45664 (2018)

[74] Kumar, V., Mishra, S., Chand, N., *et al.*: Applications of VANETs: present & future. Communications and Network **5**(01), 12 (2013)

[75] Lin, D., Kang, J., Squicciarini, A., Wu, Y., Gurung, S., Tonguz, O.: Mozo: A moving zone based routing protocol using pure v2v communication in vanets. Ieee transactions on mobile computing **16**(5), 1357–1370 (2016)

[76] Horng, S.-J., Tzeng, S.-F., Pan, Y., Fan, P., Wang, X., Li, T., Khan, M.K.: b-specs+: Batch verification for secure pseudonymous authentication in vanet. IEEE transactions on information forensics and security **8**(11), 1860–1875 (2013)

[77] Hao, Y., Cheng, Y., Zhou, C., Song, W.: A distributed key management framework with cooperative message authentication in vanets. IEEE Journal on selected areas in communications **29**(3), 616–629 (2011)

[78] Zhang, C., Lin, X., Lu, R., Ho, P.-H., Shen, X.: An efficient message authentication scheme for vehicular communications. IEEE transactions on vehicular technology **57**(6), 3357–3368 (2008)

[79] Lin, X., Li, X.: Achieving efficient cooperative message authentication in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology **62**(7), 3339–3348 (2013)

[80] Wu, L., Fan, J., Xie, Y., Wang, J., Liu, Q.: Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks. International Journal of Distributed Sensor Networks **13**(3), 1550147717700899 (2017)

[81] Chandra, S., Paira, S., Alam, S.S., Sanyal, G.: A comparative survey of symmetric and asymmetric key cryptography. In: 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), pp. 83–93 (2014). IEEE

[82] Mantri, A., Razaque, A., Makwana, H., Parekh, P., Soomro, T.R.: Analytical comparison of rsa and rsa with chinese remainder theorem. Journal of Independent Studies and Research **14**(1), 16 (2016)

[83] Zhang, G., Liao, Y., Fan, Y., Liang, Y.: Security analysis of an identity-based signature from factorization problem. IEEE Access **8**, 23277–23283 (2020)

[84] Nandy, T., Idris, M.Y.I.B., Noor, R.M., Ahmedy, I., Bhattacharyya, S.: An enhanced two-factor authentication protocol for v2v communication in vanets. In: Proceedings of the 2020 the 3rd International Conference on Information Science and System, pp. 171–176 (2020)

[85] Bali, R.S., Kumar, N.: Secure clustering for efficient data dissemination in vehicular cyber–physical systems. Future Generation Computer Systems **56**, 476–492 (2016)

[86] Zhao, P., Zhang, G., Wan, S., Liu, G., Umer, T.: A survey of local differential privacy for securing internet of vehicles. The Journal of Supercomputing **76**(11), 8391–8412 (2020)

[87] Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Annual International Cryptology Conference, pp. 213–229 (2001). Springer

[88] Barreto, P.S., Libert, B., McCullagh, N., Quisquater, J.-J.: Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 515–532 (2005). Springer