Wireless Personal Communications (2022) 123:31–68
https://doi.org/10.1007/s11277-021-09118-3

Secure Authentication Schemes for Vehicular Adhoc Networks: A Survey

J. Jenefa[1] · E. A. Mary Anita[1]

Accepted: 5 September 2021 / Published online: 15 September 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract
Vehicular Adhoc Network (VANET) is based on the principles of Mobile Adhoc NETwork (MANET) where vehicles are considered as nodes and secure communication is established to provide a safe driving experience. Due to its unique characteristics, it has various issues and challenges. These issues can be resolved by ensuring security requirements like authentication, privacy preservation, message integrity, non-repudiation, linkability, availability etc. Authentication plays a vital role since it is the first step to establish secure communication in the vehicular network. It also distinguishes malicious vehicles from legitimate vehicles. Different authentication schemes have been proposed to establish secure vehicular communications. A survey of the existing authentication schemes is given in this paper. At first, the existing authentication schemes are broadly classified based on message signing and verification methods. Then, each category is clearly explained with its sub-categories. At last, the existing schemes in each category are compared based on security requirements, security attacks and performance parameters.

Keywords Authentication · Availability · Linkability · Message integrity · Non-repudiation · Privacy-preservation

1 Introduction

Ensuring safe driving experience to the users is the main goal of the vehicular ad hoc network, [1–3] which creates a temporary network among the vehicles to establish secure exchange of messages between them. VANET comes under the class of MANET and hence it follows all the principles of mobile ad hoc networks. Vehicles will be considered as nodes and communication will be established between them. Communication established between vehicles will last only for a few seconds since vehicles will be moving from one place to another at a very high speed. VANET consist of vehicles, Road-Side Units (RSU) and Trusted Authorities (TA). Each region will be separated into many domains. Each domain will be controlled by an assigned TA. Domains further divided into sub-domains

✉ J. Jenefa
jenefa.j@christuniversity.in

[1] Present Address: Department of Computer Science and Engineering, Christ University, Bangalore, India

and RSU in that sub-domain controls vehicles in its range. The TA will be responsible for all the RSUs in its domain and RSUs will be responsible for all the vehicles in its subdomain. TA is fully trusted since it cannot be compromised. System initialization will be done by TAs. It selects the system public parameters and pre-loads it into all vehicles and RSUs.

RSUs will act as service providers. It provides value added services like multimedia services, web access, etc. to the vehicles. On the other hand, it also helps vehicles to communicate with one another. It is partially trusted because it can be compromised by the attackers. It is the responsibility of the TAs to monitor the RSUs within its domain. It will identify the compromised RSUs and takes necessary steps as soon as possible to reduce impact caused by the attackers. Vehicles will be furnished with On-Board Units (OBU) [4] in which pseudo ID generation, signature generation and verification process will be carried out and all the system parameters will be stored. Vehicles will register itself to the TA before it enters into a particular domain. This process will be done manually in which vehicles will register its original information, like vehicle's license plate number, drivers name, contact number etc. By using this information TAs will generate IDs for vehicles and it will load the system parameters which will be used to generate signatures and sign messages.

Generally, two types of communications are carried out in the vehicular network. They are communication between vehicles and RSUs and inter-vehicle communications. Communication between vehicles and RSUs has Vehicle-to-RSU (V2R) & RSU-to-Vehicle (R2V) communications [5]. V2R communication involves requesting value-added services to RSUs by vehicles and in some cases requesting parameters from RSUs to generate pseudo-IDs and signatures. R2V communication involves providing requested services to vehicles and sending requested parameters. V2R, R2V and V2V communications are wireless communications, whereas communication between RSUs and TAs, vehicles and TAs are established through secure wired connections. VANET has unique characteristics [6–10] like dynamic topology, wireless communication, the frequent transmission of messages, large network, etc. Vehicles will be travelling from one place to another at a high speed and the topology will be changing from time to time depending on the speed of vehicles. Hence it does not have stable topology. The communication between vehicles will be established only for a few seconds and hence temporary wireless network will be formed among the vehicles. Unlike other network, VANET is a large network with large number of vehicles. During peak hours, the number of vehicles will be very high which affects the performance of the network. Due to these characteristics, it has many challenges and it is prone to many attacks.

The architecture diagram of vehicular networks is given in Fig. 1. As shown, vehicles and RSUs will communicate with TA through secure wired connections. Vehicles and RSUs will communicate with one another through wireless communications. Vehicles will broadcast messages to its nearby vehicles through V2V communications. RSUs will broadcast messages to all the vehicles within its sub-domain through R2V communications. Vehicles on the other hand, request services from RSUs through V2R communications. Applications of vehicular networks are classified as safety-related and commercial applications. Safety related applications includes transmission of traffic-related messages, crash avoidance system, cooperative driving, etc. These applications focus mainly on safe driving whereas commercial applications are based on value added services. Some of the examples are multimedia services, navigation services, internet services, etc. Hence vehicular network has wide varieties of applications to ensure safe and comfortable driving experience for users. The rest of the paper is organized as follows: Sect. 2 describes about the challenges and security requirements in vehicular network and Sect. 3 lists some attacks based

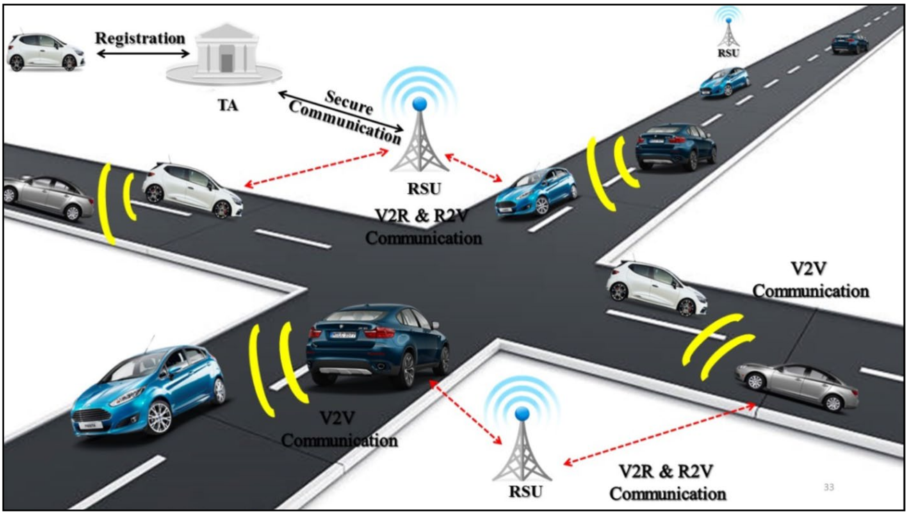

Fig. 1 Vehicular Network

on the authentication and privacy preservation. Section 4 classifies different authentication schemes. The classified schemes are reviewed and compared in further Sects. 5, 6, 7 and 8. Section 9 concludes this paper.

2 Challenges and Security Requirements

Since critical information are exchanged in vehicular network, security plays a vital role. VANET has aforementioned issues due to its unique characteristics. These issues can be resolved by ensuring all the security requirements in the vehicular network. Challenges as well as security requirements are briefly explained in this section.

2.1 Challenges

VANET is a subclass of MANET and hence it inherits almost all issues of the MANET. In addition, it also has other challenges which are described below.

Mobility Vehicles will be moving at a high speed from one place to another. Hence the mobility of nodes in the vehicular network will be very high. Establishing secure communication among the those vehicles will be a tedious process which is the main issue in the vehicular network.
Volatile Communication The communication established between vehicles in the vehicular network will last for only a short duration of time because of the high mobility of vehicles in the network. Hence it results in frequent disconnections.

Network Congestion During peak hours the number of vehicles at a particular region will be very high. In such cases, the messages which are exchanged will be very high which in turn reduce the performance of the network.

Scalability The process of providing a requested service for the vehicles will be difficult if there are a large number of vehicles in a particular region. Hence maintaining a scalable performance in the vehicular network is another major challenge.

Dynamic Topology Since the topology of the vehicular network is not stable, establishing secure communication will be difficult.

Security VANET is prone to many attacks because of its characteristics. Security has to be ensured in the vehicular network in order to improve trustworthiness of the vehicles.

2.2 Security Requirements

In order to deal with the above mentioned challenges the following security requirements have to be ensured in the vehicular network.

Authentication It helps vehicles to identify legitimate vehicles. Hence, through authentication vehicles can distinguish between attackers and legitimate vehicles.

Conditional Privacy Preservation Users private details should not be disclosed to other vehicles while exchanging messages. It avoids the misuse of private data of a legitimate vehicle. On the other hand, in case of violations attackers original ID should be traced back to identify the attackers.

Non-Repudiation It make sure that vehicles cannot deny their actions after commiting violations. It also helps in identifying malicious nodes in the network.

Message Integrity The messages exchanged between vehicles should not be altered by other nearby vehicles/attackers. It guarantees that the message received is same as that of the message sent without any modifications.

Confidentiality The messages exchanged should be disclosed only to the legitimate vehicles. It provides access control to the vehicles in the network.

Availability It makes sure that the provided services are available to all the vehicles, even if the number of vehicles at a particular region is very high.

Unlinkability The sender vehicle cannot be identified by linking its transmitted messages.

Traceability Even though vehicle's original identity should be preserved from other vehicles, in case of any violations it has to be traced back to identify the malicious vehicle.

3 Security Attacks

Among all the requirements specified in the previous section, authentication and privacy preservation plays a vital role. Attacks based on authentication and privacy preservation are listed and described in this section.

3.1 Attacks Based on Authentication

If authentication is not ensured in a network, then vehicles cannot verify sender vehicle's identity. It results in accepting and forwarding false messages throughout the network. Hence authentication has a major role in the vehicular network. If the authentication is not established in a proper way then the following attacks are possible.

Impersonation Attack An attacker can act as a legitimate vehicle. This is possible by using the parameters of legitimate vehicle during communication. In such case, the legitimate vehicle will be misjudged for commiting violations and their access for services in the network will be rejected.

Sybil Attack An attacker will use multiple identities at the same time and pretend to be different users. It will use the identities of different vehicles which it acquires while establishing communication to its nearby vehicles in the network. Hence it will pretend like different vehicle and forwards false information to its nearby vehicles in the network.

3.2 Attacks Based on Privacy Preservation

Vehicle's original details have to be protected from other users in order to avoid misuse of private data. It is done by achieving privacy preservation. Pseudo IDs are used instead of original IDs to ensure privacy preservation in a network. Pseudo IDs are usually generated by TAs, RSUs or self-generated by vehicles. If the user's private data are not preserved then the following attacks are possible.

Identity Revealing Attack An attacker will try to extract the original ID of a vehicle from its pseudo ID. By achieving it, the attacker will misuse the private data of other vehicles while establishing communication with other legitimate vehicles in the network.

Location Tracking Attack Location details of a particular vehicle should be hidden from other vehicles in the network. Attackers will try to find the location information of a vehicle for a period of time by which attackers can track the vehicles and can maintain profiles for vehicles based on its location.

Some other attacks possible in a vehicular network are listed below.

Fabrication Attack An attacker will send false information to its nearby vehicles. It will be forwarded throughout the network, which in turn reduces the performance of the network and confuses the legitimate users with false information. Since the false information will be forwarded throughout the network, identifying the sender will be difficult.

Modification Attack An attacker will try to alter the messages which are exchanged between two legitimate vehicles. As a result fake information will be forwarded throughout the network. It makes the legitimate vehicles to take wrong decisions during its journey.

Man-In-Middle Attack An attacker will overhear the communication between vehicles and tries to alter them before the messages get delivered to its corresponding receiver. It can either eavesdrop or alter the messages which are being exchanged between the legitimate vehicles.

Replay Attack An attacker will resent the previous messages again to confuse the other legitimate vehicles. It will save all the previous messages and reuse it again for its benefit.

Denial of Service Attack An attacker will send frequent messages to its nearby vehicles to affect the network performance. On the other hand, it tries to use all the network resources and make the services unavailable for other legitimate users. It has a major impact in case of emergency situations. Because of the congestion created by the attacker in the wireless channel, emergency messages cannot be transmitted in the network.

Repudiation Attack An attacker will deny its violated actions. It will not accept its violations and tries to act as a legitimate vehicle.

4 Authentication

The first step to establish secure communication is a network is to ensure authentication. When a vehicle receives a message from its neighbor node, if first checks the legitimacy of the sender vehicle and then accepts/forwards the message if it is a legitimate vehicle. Hence authentication comes first in establishing a secure communication between vehicles, without which verifying the legitimacy of the sender vehicle will be impossible. It helps in distinguishing between the attackers and the legitimate vehicles. It also helps in creating trustworthiness between vehicles. Authentication scheme used in a network has to be strong and secure in order to avoid attacks. If it is weak, then the vehicles cannot verify the legitimacy of the sender vehicle accurately which result in accepting false messages from the attackers. Hence it has to be strong enough to identify the attackers accurately in the network. Thereby secure communication can be established between vehicles in the network.

Authentication comprises of two phases: signing and verification phase. These two phases have to be executed in a proper way to satisfy the security requirements. The method used for signing a message should not be simple. The parameters used to sign should be known only to the legitimate vehicles. Thereby attackers cannot alter and transmit false information in the network. In addition, the signing process should not be more complex since it will increase the overheads in the network. Verification on the other hand, should verify the legitimacy of the vehicles accurately. Verification process has to be simple and secure. It also should have the ability to verify multiple messages at the same time to improve efficiency. Overheads for signature verification should be less in order to improve the performance of the network. Message authentication is the process of verifying the correctness of the received messages. It helps the vehicles to accept the valid messages from the sender vehicles. It also checks the integrity of the received messages to make sure that the received messages are not altered. Hence it plays a main role in establishing secure communication among vehicles in the network.

Researchers proposed different authentication schemes to establish secure communication in the network by ensuring all the security requirements. These schemes are classified and reviewed in this section. They are also compared based on security requirements, attacks and performance parameters. Security requirements include all the requirements stated in Sect. 2.2. Security attacks include attacks like impersonation attack, sybil attack, modification attack, replay attack, etc. The performance of the existing schemes is compared based on computation and communication overheads. Computation overhead is based on the time taken to generate and verify the signature. It will be measured in milliseconds and the time taken is classified under three categories: high, medium and low. Communication overhead includes the time taken to establish communication between the vehicles in the network. It includes the size of the messages as well as the delay. Communication overhead in the existing schemes is also classified into three categories: High, medium and low based on the size of the message (bytes).

4.1 Classification of Authentication Schemes Based on Message Signing

Classification of the existing authentication schemes based on signing is given in Fig. 2. As shown, the existing authentication schemes are classified based on message signing as: Key Based Authentication, Certificate Based Authentication, Signature Based Authentication and Hybrid Approach. These schemes are explained in detail along with its sub-categories in further sections.

Key Based Authentication Key based authentication schemes use keys to encrypt the messages which are transmitted. Both symmetric and asymmetric key schemes are used to authenticate vehicles. Group Key is used to establish secure communication between group of vehicles in vehicular networks. Some of the key based authentication schemes are discussed in Sect. 5.

Certificate Based Authentication Certificate based authentication schemes use certificates to authenticate vehicles. Certificates will be generated with the private data of vehicles.

*Signature Based Authentication*Signature based authentication schemes use signatures to authenticate vehicles. Signatures are generally generated by using system parameters and the message to be transmitted. Two types of signatures single and group signatures are used for authentication purpose.

Hybrid Approach The hybrid approach is the combination of the aforementioned authentication schemes. Authentication techniques are combined to acquire the merits

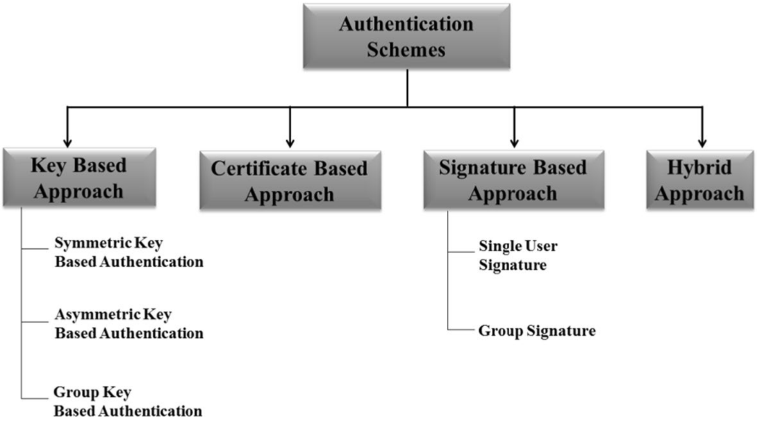
Authentication Schemes
Key Based Approach
Certificate Based Approach
Signature Based Approach
Hybrid Approach
Symmetric Key Based Authentication
Asymmetric Key Based Authentication
Group Key Based Authentication
Single User Signature
Group Signature

Fig. 2 Classification of Authentication schemes

Table 1 Comparison between different authentication schemes

Key based authentication	Certificate based authentication	Signature based authentication
Symmetric/Asymmetric keys are used for signing and verification	Certificates are used to authenticate vehicles	Signatures are used for signing and verification of messages
It provides less security than certificate and signature based schemes	It provides better security than key based authentication schemes	It provides better security than certificate based authentication schemes with less overheads
Key management will be difficult	Certificate generation and verification has overhead issues	Generated signatures cannot be duplicated
It has scalability issues	It is more scalable than key based authentication	It is more scalable than key based authentication

of both techniques and to overcome issues in a technique by using another technique. The difference between these schemes are tabulated in Table 1.

4.2 Classification of Authentication Schemes Based on Verification

Based on verification the existing authentication schemes are classified as: Schemes with pairing operations and schemes without pairing operations, which further classified into single message verification, batch verification, batch verification by using proxy vehicles and cooperative message verification. It is given in Fig. 3. These schemes are explained in detail below.

4.2.1 Schemes with Pairing Operations

In schemes under this category, expensive pairing operations are used to verify the received messages accurately. Bilinear, Weil and Tate pairings are some of the pairing operations, which are used for verification. Among which Bilinear pairings are commonly used pairing operations in many authentication schemes. A brief description about bilinear pairing operation is given below.

Let G_1 and G_2 be the additive and multiplicative group of order q. e: $G_1 \times G_1 \rightarrow G_2$ is the bilinear map with the generator point P for $G_{1.}$ It has the following properties.

- Bilinear: For all P, Q € G_1 and a, b € Z_q^*, we have e (cP, dQ) = e (P, dQ)^c = e (cP, Q)^d = e (P, Q)^{cd} and so on.
- Non-degeneracy: e (P,P) is the generator point of G_2 where p is the generator point of G_1.
- Computability: e is computed efficiently.

By using these pairing operations vehicles will verify received messages. Even though it is expensive, it is used for its accuracy in order to establish secure communication in vehicular networks.

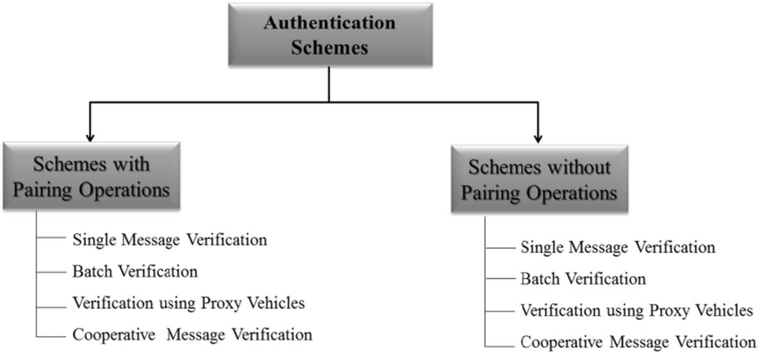
Authentication Schemes
Schemes with Pairing Operations
Single Message Verification
Batch Verification
Verification using Proxy Vehicles
Cooperative Message Verification
Schemes without Pairing Operations
Single Message Verification
Batch Verification
Verification using Proxy Vehicles
Cooperative Message Verification

Fig. 3 Classification of Authentication Schemes Based on Verification

4.2.2 Schemes Without Pairing Operations

Pairing operations used to verify signatures are very expensive. It takes around 8.12 ms to execute a pairing operation [11] which is very expensive. Hence authentication schemes are proposed without pairing operations to reduce overheads. It verifies efficiently without pairing operations and with less overheads. Recently, researchers have proposed different schemes without pairings to provide efficient authentication in the vehicular network. Based on the number of messages a vehicle can verify at a time, authentication schemes are classified as single message verification schemes, batch verification schemes, batch verification using proxy vehicles and cooperative message verification schemes. These schemes are explained briefly below. The comparison between these schemes are given in Table 2.

Single Message Verification Vehicles or RSUs can verify only one message at a time. It is a simple message verification technique. But it is time consuming since messages will be verified one by one. It has high computation and communication overheads.

Batch Verification Vehicles/RSUs can verify 'n' number of messages at the same time. It has less communication and computation overhead when compared to single message verification schemes. Hence vehicles/RSUs can verify 'n' number of messages simultaneously and with the result, it can authenticate 'n' number of vehicles at the same time. Thereby overheads can be reduced in an efficient way.

Proxy Vehicle Based Batch Verification Even by using batch verification, RSUs have efficiency issues since it receives messages from the large number of vehicles at the same time during peak hours. In order to deal with this issue, proxy vehicles are used to verify 'd' number of messages from its neighbor vehicles. It then sends the result of the verified 'd' messages to RSU which will be cross checked and accepted by RSU if it is valid. This in turn reduces the overheads to a greater extent and also overcomes efficiency issues in RSUs.

Cooperative Message Verification Vehicles/RSUs will cooperate with other vehicles/RSUs to verify 'n' number of messages at the same time. It avoids independent verification of messages by vehicles/RSUs which in turns reduces the computation overheads. It also reduces communication overheads but it is insecure against DoS attacks which is its main drawback. In this way, authentication schemes are classified based on message verification.

5 Key Based Authentication

It uses keys to sign a message before transmitting it to other vehicles. Both symmetric and asymmetric keys are used. Key based authentication schemes are classified into symmetric key based authentication, asymmetric key based authentication and group key based authentication as shown in Fig. 2. They are explained in detail below. Based on verification it is classified as schemes with pairings operations and without pairing operations, which further classified into batch verification and cooperative message verification. Symmetric key based authentication is also known as private key cryptography where similar secret keys will be shared between vehicles. These keys should be protected in a secure way to avoid misuse of data. It is simpler than asymmetric key based authentication since only one

Table 2 Comparison between authentication schemes based on verification

Single message verification	Batch verification	Proxy vehicle based verification	Cooperative message verification
Verifies single message at a time	Verifies ‘n’ number of messages at a time	Verifies [n/d] messages at a time with the help of proxy vehicles (verifies ‘d’ messages)	Verifies ‘n’ number of messages by cooperating with other vehicles
High computation overhead	Less computation overhead than single message verification schemes	Less computation overhead	Less computation overhead
High communication overhead	Less communication overhead than single message verification schemes	Less communication overhead	Less communication overhead
Affects the efficiency of RSUs	Affects the efficiency of RSUs	Efficiency problems are resolved	Efficiency problems are resolved, but it is insecure against DoS attack

secret key is used between vehicles to establish secure communication. It is also faster in signing and verification process. However, it has various issues. If a secret key is disclosed to an attacker, then the attacker can alter as well as can impersonate as legitimate vehicle. Protecting the secret key is also a difficult task.

In asymmetric Based Authentication two keys, private and public keys are used for authentication purpose. It is also known as public key cryptography. The private key is used to prove its identity to other vehicles. Hence it is kept hidden from other vehicles. Messages will be encrypted by using private keys which can be decrypted only by using its public key. The public key will be broadcast to all, whereas private key is not disclosed to other vehicles. Public/Private key pairs used are not related to one another. It provides better security than symmetric key based authentication since it uses key pairs to sign and verify messages. But it has key management issues. Group Key is a symmetric key shared among the vehicles in the same group. It helps to achieve confidentiality in the vehicular network. The messages transmitted will be encrypted using the group key which can be accessed only by the vehicles in the group. Group keys will be computed by using TAs. In some schemes, RSUs are also used to generate group keys. Group keys are updated whenever a vehicle leaves or enters into a group. Since vehicles will be moving at a high speed it leads to frequent updating of group keys which is its major drawback. Both symmetric and asymmetric key based authentication schemes has key management issues. It will be very difficult in asymmetric key based authentication because vehicles should manage its public/private key pairs and public keys of all its neighborhood vehicles. It also arises memory management issues. Assigning keys to vehicles is also a difficult task since VANET is a large network with large number of vehicles. Hence it is not scalable when compared to other authentication schemes. Key based schemes are also used to generate signatures, it is discussed in Sect. 7. It is also combined with other authentication schemes to provide better security which is discussed in Sect. 8. Some of the existing key based authentication schemes are reviewed and compared in this section.

Vijayakumar et al. [12] proposed a dual authentication and key management techniques for vehicular network (DAKMT). Here the vehicles are prioritized as primary, secondary and unauthorized users. The dual authentication scheme will distinguish between the legitimate and malicious vehicles. Group key management is then used to distribute group keys to the vehicles in the group and provide access only to the members of the group. An efficient group key updating technique is proposed to reduce computation overheads. Group keys will be updated whenever a vehicle enters or leaves a group, hence the group keys will be updated frequently. Messages will be encrypted by using a vehicles secret key and messages to a group of vehicles is encrypted by using group key. Single message verification is carried out without pairing operations.

Wazid et al. [13] proposed a key agreement protocol for vehicular network (DLAKAP). Three types of authentication are proposed in this scheme: V2V authentication, V2CH (Vehicle-to-Cluster Head) authentication and CH2RSU (Cluster Head-to-RSU) authentication. In addition, authentication between RSUs (RSU2RSU) is also established securely in this scheme. Initially vehicles/RSUs will register itself to TA. Then the vehicles will authenticate with its cluster heads and other vehicles. Vehicles can communicate with RSUs through cluster heads. Authentication is established by using symmetric key based schemes. Only one message can be verified at a time. It provides privacy preservation, anonymity and traceability.

Mahagaonkar et al. [14] proposed a simple scheme based on asymmetric key based cryptography (TEAC). It uses TESLA + + along with asymmetric key based authentication. Initially, vehicles will generate their pseudo IDs with the help of RSUs. It generates their own public/private key pairs and registers all the public keys to RSUs with its pseudo ID. During authentication, it signs the message with its private key, the receiver requests RSU for the sender's public key by using the sender's pseudo ID. RSU will send the public key of the sender and thereby the receiver can verify the message. It has high computation and communication overheads since each V2V communication is established with the help of the RSU.

Xiong et al. [15] proposed an authentication scheme (CPPAP) by using the Chinese Reminder Theorem (CRT). This scheme is proposed to address the dynamic membership challenges in VANET. CRT is used for key distribution for all the vehicles within the range. The vehicles in the same domain use domain key for establishing communication which is generated by using one modulo division operation. It is simple and secure. It provides authentication and privacy-preservation, but other essential security features like message integrity, unlinkability and non-repudiation are not ensured which is the main drawback in this paper.

5.1 Comparison Between Key Based Schemes

The above discussed schemes are compared based on message signing/verification, security requirements, security attacks and performance parameters. It is given in Tables 3, 4, 5 and 6. As shown in Table 3, the schemes are compared based on communication pattern, message signing and verification. As shown, all schemes use single message verification (without pairing operations) to verify messages. CPPAP [4] use batch verification forvrifying multiple messages. Table 4 compares the schemes based on security requirements like privacy preservation, non-repudiation, message integrity, traceability, unlinkability and confidentiality. As shown, all schemes provide privacy preservation & message integrity and no scheme ensures unlinkability and confidentiality.

Table 5 compares the schemes based on resistance against security attacks like impersonation, Sybil, ID revealing, modification, man-in-the-middle, replay and DoS attack. As shown, all schemes are secure against impersonation, ID revealing and modification attacks. It is also shown that all the schemes are not secure against DoS attacks. A vehicular environment is simulated in NS2 with one TA, three RSUs and one hundred and twenty five vehicles. Vehicles moves in the operating space of about 5000 × 5000 m. Table 6 compares the schemes based on performance parameters (communication & computation overheads). These overheads are categorized as high, medium and low where the range of values for computation overheads (ms): Low–less than 5 ms, Medium–5 to 15 ms and High–greater than 15 ms. The range of values for communication overheads (bytes): Low–less than 70 bytes, Medium–70 to 150 bytes and High– greater than 150 bytes.

As shown in Table 6, DAKMT [12] scheme has medium computation and communication overheads, DLAKAP [13] scheme has medium computation and high communication overheads. TEAC [14] scheme has high computation and communication overheads. Other key based schemes used to generate signatures are discussed in Sect. 7. It is also combined with other authentication techniques for better performance, such hybrid schemes are discussed in Sect. 8. The main drawback in the key based authentication scheme is the key management process which leads to increase in communication overhead. In Group Key based schemes, [12, 13] the key or domain key will be updated each time a vehicle enter or leaves the network which in turns increases the overheads.

Table 3 Comparison of key based schemes based on message signing and verification

Schemes	Communication pattern	Message signing method	Message verification method
DAKMT [12]	V2R, R2V, V2V	Group Key Based Scheme	Single Message Verification (without pairing operations)
DLAKAP [13]	V2V, V2CH, CH2RSU, RSU2RSU	Symmetric Key Based Scheme	Single Message Verification (without pairing operations)
TEAC [14]	V2V, V2R, R2V	Asymmetric Key Based Scheme	Single Message Verification (without pairing operations)
CPPAP [4]	V2R, R2V, V2V	Group Key Based Scheme	Batch Verification (without pairing operations)

Table 4 Comparison of key based schemes based on security requirements

Schemes	Privacy-preservation	Message integrity	Non-repudiation	Traceability	Unlinkability	Confidentiality
DAKMT [12]	✓	✓	✓	✓	✗	✗
DLAKAP [13]	✓	✓	✓	✓	✗	✗
TEAC [14]	✓	✓	✗	✗	✗	✗
CPPAP [4]	✓	✓	✓	✓	✓	✗

Table 5 Comparison of key based schemes based on resistance against security attacks

Schemes	Impersonation Attack	Sybil Attack	ID Revealing Attack	Modification Attack	Man-in-Middle Attack	Replay Attack	DoS Attack
DAKMT [12]	✓	✓	✓	✓	✗	✓	✗
DLAKAP [13]	✓	✗	✓	✓	✓	✓	✗
TEAC [14]	✓	✗	✓	✓	✗	✗	✗
CPPAP [4]	✓	✓	✓	✓	✗	✓	✗

Table 6 Comparison of key based schemes based on performance parameters

Schemes	Computation overhead (ms)	Communication overhead (Bytes)
DAKMT [12]	Medium	Medium
DLAKAP [13]	Medium	High
TEAC [14]	High	High
CPPAP [4]	Medium	High

6 Certificate Based Authentication

Certificates will be used for authentication purpose. Certificate Authority (CA) will be responsible to generate certificates for vehicles. Certificate generation includes private/public key pairs as well identity of the vehicles. Hence it is more secure than key based authentication schemes. These certificates will be added in the messages which is transmitted to other vehicles. It helps to authenticate the legitimacy of the sender vehicle. It is also more scalable since CA can generate certificates for a large number of vehicles. However, it has overhead issues. The computation and communication overhead will be high when compared to other authentication schemes. It is the main drawback in certificate based authentication schemes. Even though it offers better security, due to its overhead issues it is more complex than other schemes. Certificate based schemes used to generate signatures are discussed in Sect. 7. Certificate based schemes are usually combined with key based or signature based schemes for better performance. Such schemes are discussed in Sect. 8.

7 Signature Based Authentication

Signatures will be used to establish authentication between vehicles. Signatures will be generated by using system parameters and the identity of the vehicles. It is more secure than other authentication schemes. The message which is transmitted is also used as a parameter to compute signatures. Hence, in addition to authentication it also provides other security features like message integrity, non-repudiation etc. The generated signatures cannot be duplicated by other vehicles or attackers which is the main advantage of this scheme. Signatures will be generated by vehicles whenever a vehicle wants to send messages to its nearby vehicles/RSUs. Hence it is scalable when compared to other authentication schemes. It is further classified as single user signature and group signature. Signature based authentication schemes are more efficient than other authentication schemes since it has less overheads and better performance. Different techniques are used for signature generation and verification. As shown in Fig. 2, signature based authentication schemes are further classified into single user signature based authentication schemes and group signature based authentication schemes. The existing signature based authentication schemes are categorized based on this classification and reviewed in this section. At last, comparison between the schemes under each category is done based on security requirements, attacks and performance parameters.

7.1 Single User Signature Based Authentication

In single user signature schemes, each vehicle will use its own signatures to authenticate with other vehicles. These signatures are either generated by TAs or self-generated by vehicles. The major issue in this scheme is the communication and computation overhead. Researchers proposed different single user signature schemes with other security requirements to achieve secure communication with less overheads in the vehicular network. One among the efficient single user signature based authentication scheme is Identity Based Signature (IBS) schemes. Existing IBS schemes are reviewed and compared in this section.

7.1.1 Identity Based Signature (IBS) Schemes

The identity of the vehicles will be used as a main parameter to generate signatures. It is the simple and secure signature based authentication scheme since it generates signatures by using IDs of the vehicle. These IDs will be assigned by TAs during the registration process. In order to ensure the privacy preservation, pseudo IDs are used instead of original IDs. Pseudo IDs are generated either by TAs/RSUs or self-generated by vehicles. Each identity based signatures generated by using pseudo IDs will be used only once and in most schemes pseudo IDs are not reused to avoid linkability issues. IBS schemes are further classified into subcategories based on signature generation and verification, which is explained in this section.

7.1.1.1 Classification Based on Signature Generation Based on signature generation IBS based authentication schemes are classified as ECC based schemes, key based schemes and threshold based schemes. These schemes are explained in detail with its related works.

ECC Based Schemes Identity based signatures are generated by using Elliptic Curve Cryptography (ECC). It is the efficient and secure way for generating signatures because of its light weight key. Hence, many researchers proposed different ECC based IBS schemes. It provides better security than RSA schemes and has less overheads. It is also fast and needs less storage space since it has the light weight key. Some of the existing ECC based schemes are reviewed in this section. The basic initialization steps for ECC based schemes are described below.

Let F_n be the finite field over n, where n is a large prime number which is the size of the finite field, F_n. The elliptic curve E ($y^2 = x^3 + ax + b$ (mod n), where $4a^3 + 27b^2 \neq 0$) has parameters (a, b) € F_n. Let P be the generator point of E, $P \neq O$ where O denotes infinity and q be the prime order of P. TA will choose secret key 's' and computes its public as $P_{pub} = sP$. It also other system parameters which will be used by vehicles for signature generation and verification purpose. Even though it is complex it provides better security than other schemes. Public/Private keys of vehicles will be self-generated by vehicles in order to avoid key management issues. In this way ECC based schemes are used to generate identity based signatures.

Key Based Schemes In key based schemes, identity based signatures are generated by using signing keys. Signing keys will be assigned by TAs to vehicles. IDs of vehicles will be encrypted with the signing key to generate signatures. It doesn't use any complex operations like ECC based schemes. It is a simple and secure scheme to generate signatures. It has key management issues since TAs assign many signing keys to vehicles for signature generation. With the signing key 'k', the signature is generated with the ID as, SIG (ID). In this way key based schemes generate identity based signatures.

Threshold Based Schemes In threshold based schemes, the information 'I' to be transferred will be divided into 'n' parts. The original information can be regenerated only if a vehicle has knowledge of 'k' or more parts of the information 'I'. If the vehicle has knowledge of $k-1$ or less than that then it cannot regenerate the original information 'I'. This is known as (k, n) threshold scheme. The divided parts will be shared between the vehicles which will be kept in a secure way. Signatures will be generated for messages by using the secret share of the information. It will be used to sign the messages to be transmitted. It has high communication and computation overheads which is the main drawback of this scheme. In this way threshold based schemes generate identity based signatures.

7.1.1.2 Classification Based on Signature Verification IBS based authentication schemes are classified based on verification as Schemes with pairing operations and Schemes without pairing operations. It further classified based on the number of messages it can verify simultaneously as single message verification, batch verification and verification by using proxy vehicles. Researchers proposed different IBS based scheme to achieve efficient authentication. Some of the existing IBS schemes are reviewed and compared based on the security and performance parameters in this section.

Lo et al. [11] proposed a new ECC based IBS authentication scheme (ECPAS). Authentication is achieved without using expensive pairing and MapToPoint operations to reduce overheads. It uses two TAs: Tracing Authority (TRA) & Private Key Generator (PKG) which is used for pseudo ID generation and private key extraction. Vehicles computes a signature by using a pair of pseudo ID and private key. Batch verification is used to increase the computation capability in RSUs. It provides privacy-preservation, traceability and message integrity. Secure V2R and R2V communications are mathematically proposed in this paper. V2V authentication is not achieved, which is the main drawback in this paper.

In order to overcome the aforementioned drawbacks, Jenefa et al. [16] proposed a new ECC based IBS scheme (ESAV). In order to reduce the overhead, two trusted authorities in Lo et al. [11] scheme is replaced by a single trusted authority, TA which is responsible for initialization and key generation of vehicles and RSUs. The communication and computation overheads are reduced by simplifying the signature generation and verification process. Hence secure authentication scheme is proposed with less overheads but the proposed scheme is not efficient when the signatures of large number of vehicles are to be verified at the same time which is its main drawback.

He et al. [17] proposed a new Conditional Privacy-preserving Authentication (EIC-PAS) scheme without pairings. Since pairing operations are expensive, both pairing and MapToPoint hash operations are not used in this scheme to reduce overheads. It uses ECC based IBS scheme for signature generation. Single message as well as batch verifications is used for signature verification. It provides authentication, privacy-preservation, message integrity, tracability, unlinkability and non-repudiation. It has less computation and communication overheads because of the omission of pairing operations.

Liu et al. [18] proposed an efficient IBS scheme using proxy vehicles, PBAS. Proxy vehicles are used to reduce the computational issues in RSUs. Here the messages received from the vehicles will be verified by proxy vehicles and the results will be sent to the RSU for further verification. At first, TA will generate its system parameters and assigns IDs to vehicles & RSUs. Vehicles by using the system parameters, generate pseudo IDs and its respective private keys. It then generates signature, which will be broadcast to all its nearby vehicles. Proxy vehicles on receiving messages from its neighbors verifies the signatures by using batch verification and sends the results to the RSUs. RSU will authenticate the proxy vehicles and will accept the messages after cross checking the result sent by proxy vehicles. Each proxy vehicle can verify ‘d’ messages and hence RSUs can verify [d/n] messages at the same time. Proxy vehicles are selected efficiently by using a proxy vehicle selection algorithm. It uses bilinear pairings for verification. It provides confidentiality to the requested vehicles by assigning session keys. Even though it overcomes efficiency issues in the RSU, it has high overheads because of pairing operations and MapToPoint hash operations which is the main drawback of this scheme.

Yong et al. [19] proposed (ESASCP) a new Conditional Privacy-preserving Authentication (CPPA) with less overheads than other existing CPPA schemes. The ECC based IBS scheme is used to generate signatures with bilinear pairings for verification purpose. Tamper-Proof devices (TMP) are secured with a password to avoid disclosure of private details even when it is compromised by attackers. Single message as well as batch verification is possible by using pairing operations. It provides authentication, privacy-preservation and non-repudiation. It has high communication and computation overheads because of pairing operations.

Tzeng et al. [20] proposed an enhanced ID based batch verification for vehicular networks (ESPIBV). TMPs will be responsible for pseudo ID and signature generation and hence it is protected with a password. It generates pseudo IDs and private keys to sign a message to be transmitted. During verification it uses constant pairing and point multiplication operations, which remains same irrespective of the number of messages. It provides authentication, privacy-preservation, non-repudiation, message integrity, traceability and unlinkabilty. Secure V2V and V2R communications are established by using this scheme. The computation and communication overheads are reduced to a certain extent but still it is higher than schemes without pairing operations.

Cui et al. [21] proposed a privacy-preserving scheme using cuckoo filter for vehicular network (SPACF). It does not rely on any hardware devices and purely based on software. It uses cuckoo filter and binary search methods for verification purpose. Vehicles will generate its signature by using its pseudo ID and transmit it to nearby RSU. RSU will verify the received messages by using batch verification. It then notifies the results to the vehicles in its range, which will be used as a reference to establish secure communication between vehicles. If a vehicle receives signature from nearby vehicles it checks it with the notification messages received from the RSU and accepts it if it is valid. It provides authentication, privacy-preservation, non-repudiation, message integrity and traceability. It has less overheads because of the pairing-free operations.

Asaar et al. [22] proposed a proxy vehicle based authentication by using an IBS scheme without pairing operations (ID-MAP). Liu et al.'s [18] has high overheads because of pairing operations. Hence pairing operations are not used in this scheme to reduce overheads and to deal with the efficiency issues in RSUs. Vehicles will generate two signatures and sends it to proxy vehicles. Proxy vehicles will verify the signatures without using pairing operations and forwards the result to the RSU which will authenticate the proxy vehicle and accepts the messages if the received results are valid. It provides authentication, non-repudiation, traceability and unlinkability. Even though it avoids pairing operations to reduce computation overheads, the cost of signature generation is high and it influences the performance of a vehicle to act a proxy vehicle.

Jenefa et al. [23] proposed a new IBS scheme using proxy vehicles (IMAS) to overcome the drawbacks in ID-MAP [22]. ECC based authentication is used without pairing operations. Proxy vehicles reduce the burden of RSUs by verifying the messages from vehicles using batch verification. RSUs verify the result from the proxy vehicles after authenticating the identity of proxy vehicles. Hence, with the help of proxy vehicles, RSUs can verify a large number of messages. The proposed scheme has less computation overhead than ID-MAP, it also provides security against privacy preservation attacks. Even though it provides efficient R2V and V2R communication, the inter-vehicle communication cost is not less when compared to other schemes.

Zhong et al. [24] proposed a new ID based conditional privacy-preservation and authentication scheme (ECPASP). TMPs are protected with passwords to avoid original ID disclosure. Vehicles computes its pseudo IDs and private keys by using the system parameters. Each time a pair of pseudo ID/private key is used to generate signatures. It verifies 'n' number of messages at the same time by using batch verification without pairing operations. It provides authentication, privacy- preservation, non-repudiation, message integrity and traceability. It has less overheads since it verifies signatures without using pairing operations.

Li et al. [25] proposed an ID based authentication scheme (ACPN) with privacy-preservation and non-repudiation. Secure V2R, R2V, V2V and cross-RSU communications are established in this scheme. Identity Based Signature (IBS) is used for secure authentication between vehicles and RSUs. Identity Based Online/Offline Signature (IBOOS) is used for secure V2V communications. Initially vehicles will self-generate its pseudo IDs by using RSUs. It then communicates with its nearby RSU for offline signature generation. Online signature is computed from offline signature and it is broadcast to neighbor vehicles to establish secure communication. After authentication the traffic-related messages are transmitted in a secure manner. Offline/online signatures are generated by using offline/online signing keys by RSUs and vehicles. It uses bilinear pairings to verify one message at a time. Cross-RSU V2V authentication is also proposed in this scheme which helps to establish secure communication between RSUs.

Sun et al. [26] proposed conditional privacy-preserving mutual authentication framework (MADAR) to provide resistance against Denial of Service (DoS) attack. It uses Li et al.'s [25] IBS and IBOOS scheme for secure V2R, R2V and V2V communications. A weak authentication mechanism is proposed to provide security against DoS attack. In order to provide weak authentication, the one-way key chain is used. It is done by computing the last key value and then repeatedly using a one-way key chain to find its previous values. The weak authentication is based on message-specific puzzle [27]. Thereby resistance against DoS attack is achieved in the proposed scheme.

Jenefa et al. [28] proposed a new ID based authentication scheme vehicular communications (SVCIBS). Modified IBS and IBOOS schemes are used for authentication of V2R, R2V and V2V communications. Secure emergency communication is also established without RSUs by using RSA algorithm. Authentication is done by the exchange of authentication messages, whereas the actual traffic-related messages are not transmitted. Hence, after successful authentication, traffic related messages will be transmitted which will increase the communication cost due to the increase in the iterations to transmit a message. It is the main drawback in this paper. On the other hand, it provides authentication, privacy-preservation and non-repudiation.

Sun et al. [29] proposed a threshold based IBS scheme (IBSSUP). It uses (k,n) threshold technique to generate signatures. It provides authentication, privacy-preservation, non-repudiation, message integrity and confidentiality. Privacy-preserving defense technique for vehicular network is also proposed in this paper. Trusted Dealer (TD) will be used to share the secrets to all the vehicles. Vehicles generates signatures by using its secret share. It uses bilinear pairings for verification and it verifies one message at a time. It has high computation and communication overheads which is the main drawback of this scheme.

Jalawi et al. [30] proposed an IBS scheme (CPPAS) which is based on ECC without point multiplication operations. Point multiplication operation is omitted in the proposed scheme to increase the performance efficiency. Authentication is achieved just by using the point addition operation of the ECC. Vehicles will be initialized and broadcast the message to the nearby vehicles through joining phase. Single message verification is used in the proposed scheme for verification of messages. Signing and verification is done by using hash functions and simple XOR operations. Hence this scheme is simple and it has less computational & communication overhead.

7.1.1.3 Comparison Between IBS Schemes These IBS schemes are compared based on security requirements, security attacks and performance parameters. It is given in Tables 7, 8, 9 and 10. In Table 7, the schemes discussed are compared based on signature generation and verification. As shown [11, 17–22, 24] use Elliptic Curve Cryptography to generate signatures. These schemes use batch verification (with/without pairings to verify signatures. PBAS [18] and ID-MAP [22] uses proxy vehicle to verify signatures, hence it has V2P (Vehicle-to-Proxy vehicle), P2R (Proxy vehicle-to-RSU) communications. ACPN [25], MADAR [26], SCVIBS [28] are key based schemes which use offline/online signatures for authentication and single message verification with bilinear pairings is used for signature verification. IBSSUP [29] scheme is a threshold based scheme which uses (k,n) threshold technique to generate signatures. It uses single message verification with pairings for verification purpose.

Table 8 compares schemes based on security requirements: Privacy-preservation, message integrity, non repudiation, traceability, unlinkability and confidentiality. As shown all ECC based schemes provides privacy-preservation, Message integrity, non-repudiation,

Table 7 Comparison of IBS scheme based on signature generation and verification

Schemes	Communication pattern	Signature generation method	Signature verification method
ECPAS[11]	V2R, R2V	Elliptic Curve Cryptography Based Schemes	Batch Verification (without pairing operations)
EICPAS [17]	V2V, V2R		Batch Verification (without pairing operations)
ESAV [16]	V2V,V2R, R2V		Batch Verification (without pairing operations)
PBAS [18]	V2P, V2R, P2R		Batch Verification using Proxy Vehicles (with pairing operations)
ESASCP [19]	V2V, V2R		Batch Verification (with pairing operations)
ESPIBV [20]	V2R, V2V		Batch Verification (with pairing operations)
SPACF [21]	V2R, V2V, R2V		Batch Verification (without pairing operations)
ID-MAP [22]	V2P, P2R, V2R		Batch Verification using Proxy Vehicles (without pairing operations)
IMAS [23]	V2P, P2V, P2R, V2R		Batch Verification using Proxy Vehicles (without pairing operations)
ECPASP [24]	V2V, V2R		Batch Verification (without pairing operations)
CPPAS [30]	V2V, V2R, R2V		Batch message Verificition (without pairing operations)
ACPN [25]	V2V, V2R, R2V	Key Based Schemes	Single Message Verification (with pairing operations)
MADAR [26]	V2V, V2R, R2V		Single Message Verification (with pairing operations)
SCVIBS [28]	V2V, V2R, R2V		Single Message Verification (with pairing operations)
IBSSUP [29]	V2V, V2R, R2V	Threshold Based Scheme	Single Message Verification (with pairing operations)

Table 8 Comparison of IBS scheme based on security requirements

Schemes	Privacy-preservation	Message Integrity	Non-repudiation	Traceability	Unlinkability	Confidentiality
ECPAS [11]	✓	✓	✓	✓	✓	✗
EICPAS [17]	✓	✓	✓	✓	✓	✗
ESAV [16]	✓	✓	✓	✓	✓	✗
PBAS [18]	✓	✓	✓	✓	✓	✓
ESASCP [19]	✓	✓	✓	✓	✓	✗
ESPIBV [20]	✓	✓	✓	✓	✓	✗
SPACF [21]	✓	✓	✓	✓	✓	✗
ID-MAP [22]	✓	✓	✓	✓	✓	✗
IMAS [23]	✓	✓	✓	✓	✓	✗
ECPASP [24]	✓	✓	✓	✓	✓	✗
CPPAS [30]	✓	✓	✓	✓	✓	✗
ACPN [25]	✓	✗	✓	✓	✗	✗
MADAR [26]	✓	✗	✓	✓	✗	✗
SCVIBS [28]	✓	✗	✓	✓	✗	✗
IBSSUP [29]	✓	✓	✓	✓	✓	✓

Table 9 Comparison of IBS scheme based on resistance against security attacks

Schemes	Impersonation attack	Sybil attack	ID revealing attack	Modification attack	Man-in-middle attack	Replay attack	DoS attack
ECPAS [11]	✓	✓	✓	✓	✓	✓	✗
EICPAS [17]	✓	✓	✓	✓	✓	✓	✗
ESAV [16]	✓	✓	✓	✓	✓	✓	✗
PBAS [18]	✓	✗	✓	✓	✓	✓	✗
ESASCP [19]	✓	✗	✓	✓	✗	✓	✗
ESPIBV [20]	✓	✓	✓	✓	✗	✓	✗
SPACF [21]	✓	✓	✓	✓	✓	✓	✗
ID-MAP [22]	✗	✗	✓	✓	✗	✓	✗
IMAS [23]	✓	✓	✓	✓	✓	✓	✗
ECPASP [24]	✓	✗	✓	✓	✓	✓	✗
CPPAS [30]	✓	✓	✓	✓	✓	✓	✗
ACPN [25]	✓	✓	✓	✓	✓	✓	✗
MADAR [26]	✓	✓	✓	✓	✓	✓	✓
SCVIBS [28]	✓	✓	✓	✓	✓	✓	✗
IBSSUP [29]	✓	✓	✓	✓	✓	✓	✗

traceability and unlinkability. In case of violations, original IDs can be traced back by TAs and the signatures are unlinkable. Only two schemes (PBAS [18] and IBSSUP [29]) provide confidentiality and hence IBSSUP [29] scheme has all security features.

Table 10 Comparison of IBS scheme based on performance parameters

Schemes	Computation overhead (ms)	Communication overhead (Bytes)
ECPAS [11]	Low	High
EICPAS [17]	Low	Medium
ESAV [16]	Low	Low
PBAS [18]	High	Medium
ESASCP [19]	High	High
ESPIBV [20]	High	Low
SPACF[21]	Low	Medium
ID-MAP [22]	Medium	High
IMAS [23]	Medium	Low
ECPASP [24]	Low	Medium
CPPAS [30]	Low	Low
ACPN 25]	Low	Medium
MADAR [26]	Low	Medium
SCVIBS [28]	Low	Medium
IBSSUP [29]	High	Low

Table 9 compares the schemes based on security attacks based on authentication (Impersonation & Sybil attack), privacy-preservation (ID revealing attack), message integrity (modification attack) and other attacks like Man-In-Middle attack, Replay attack & Dos attack. As shown all schemes are secure against impersonation attack and only MADAR [26] scheme is secure against DoS attack. Since all the schemes provide privacy preservation it is secure against ID revealing attack. All schemes generate signatures by using the timestamp and the message to be transmitted as one of the parameters and hence it is secure against modification and replay attack. Table 10 compares the schemes based on performance parameters (communication and computation overheads). These overheads are categorized as high, medium and low. As shown no scheme has low communication and computation overhead. Hence, for V2R and R2V communications, Proxy vehicle based authentication is more suitable since it reduces the burden of RSUs. In case of inter-vehicle communication, authentication scheme without proxy vehicles are more suitable since it has less communication and computation overheads when compared to proxy vehicle based schemes.

7.1.2 Other Schemes

Some other single user signature based schemes are discussed and compared in this subsection. Other single user signatures are classified based on the signature generation as: Key Based Schemes and ECC Based Schemes. Based on signature verification, it is classified as Schemes with pairing operations and Schemes without pairing operations, which further classified into: Single Message Verification and Batch Verification schemes.

Horng et al. [31] proposed (b-SPES +) an improved version of SPECS [32] (Secure and Privacy Enhancing Communication Schemes). Initial handshake is established between vehicles and RSUs to acquire system parameters to generate signatures. A signature is generated by signing messages with signing key. Hence it is one among the key based schemes for signature generation. It uses bilinear pairings to verify ‘n’ number of messages at the same time. In addition to bilinear pairing operations, MapToPoint operations are used for signature verification, which in turns increases the computation overhead. After verification RSU sends the notification message of all legitimate vehicles to all the vehicles in its range. It helps the vehicles to establish secure V2V communications. It provides authentication, privacy-preservation, non-repudiation and traceability.

Chim et al. [33] proposed a navigation scheme for vehicular networks (VSPN). It uses the information from other vehicles to guide a vehicle to reach its destination. A vehicle will send the traffic-related information to RSU by generating signature with the message. This signature will be verified and the navigation guide will be created based on the information. When a vehicle request a navigation request to RSU, it guides the vehicle to reach its destination through fastest route. ECC based signatures are generated which will be verified by RSU using bilinear pairing operations. A batch verification approach is also proposed which helps RSU to verify 'n' number of signatures from vehicles at the same time. It provides authentication, privacy- preservation, non-repudiation, traceability, unlinkabilty, message integrity and confidentiality. Since it uses pairing operations for verification, it has high overheads.

Zhong et al. [34] proposed (CPAURL) a new conditional privacy-preserving authentication scheme with registration list. Registration list is used instead of the revocation list to reduce overheads. In addition expensive bilinear pairing operations are not used for signature verification to reduce overheads. Two passwords are used for OBUs to avoid disclosure of private data even when it is compromised. Initially mutual authentication is established between vehicles and RSU. Two signatures will be generated by vehicles and verified by RSUs and added into the registration list. The traffic-related messages send by vehicles are verified by checking the registration list. If it is valid then the RSU will send the notification message to vehicles in its range. Vehicles can also verify messages from other vehicles by using notification messages from RSUs. It has less computation and communication overheads and it provides privacy-preservation, message integrity, non-repudiation, traceability and unlinkability.

Cui et al. [35] proposed (EMASEC) an efficient edge computing based message authentication scheme for vehicular networks. The repeated authentication problem is resolved in this scheme by using edge computing concept in message authentication. RSUs will authenticate the messages from the nearby vehicle and broadcasts the result to all the vehicles in its range. This avoids the repeated authentication of the same messages from nearby vehicles. Cuckoo filter and fuzzy logic control system are used to deal with repeated authentication issue. ECC based signatures are generated by vehicles which will be verified by RSU using the batch verification approach without pairing operations to reduce overheads. It provides authentication, privacy-preservation, message integrity and traceability.

Gayathri et al. [36] proposed an efficient certificate less and pairing free authentication scheme (EPCABV) for vehicular network. It is one among the ECC based scheme which generates ECC based signatures. It uses batch verification without pairing operations to verify 'n' number of messages. It provides privacy-preservation, message integrity, non-repudiation, traceability and unlinkability. It is secure against impersonation, ID revealing, modification and reply attack. It has high computation and communication overheads.

7.1.2.1 Comparison These schemes are compared based on signature generation/verification, security requirements, resistance against security attacks and performance parameters. It is given in Tables 11, 12, 13 and 14. In Table 11, the schemes discussed are compared based on signature generation and verification. As shown VSPN [33], CPAURL

Table 11 Comparison of other single user signature schemes based on signature generation and verification

Schemes	Communication pattern	Signature generation method	Signature verification method
b-SPECS + [31]	V2R, R2V, V2V	Key Based Schemes	Batch Verification (with pairing operations)
VSPN [33]	V2R, R2V	Elliptic Curve Cryptography Based Schemes	Batch Verification (with pairing operations)
CPAURL [34]	V2V, V2R, R2V		Single Message Verification (without pairing operations)
EMASEC [35]	V2V, V2R, R2V		Batch Verification (without pairing operations)
EPCABV [36]	V2V, V2R, R2V		Batch Verification (without pairing operations)

Table 12 Comparison of other single user signature schemes based on security requirements

Schemes	Privacy-preservation	Message Integrity	Non-repudiation	Traceability	Unlinkability	Confidentiality
b-SPECS + [31]	✓	✓	✓	✓	✗	✗
VSPN [33]	✓	✓	✓	✓	✓	✓
CPAURL [34]	✓	✓	✓	✓	✓	✗
EMASEC [35]	✓	✓	✗	✗	✗	✗
EPCABV [36]	✓	✓	✓	✓	✓	✗

Table 13 Comparison of other single user signature schemes based on resistance against security attacks

Schemes	Impersonation attack	Sybil attack	ID revealing attack	Modification attack	Man-in-middle attack	Replay attack	DoS attack
b-SPECS + [31]	✓	✗	✓	✓	✓	✓	✗
VSPN [33]	✓	✓	✓	✓	✗	✓	✗
CPAURL [34]	✓	✗	✓	✓	✓	✓	✗
EMASEC [35]	✓	✓	✓	✓	✗	✓	✗
EPCABV [36]	✓	✗	✓	✓	✗	✓	✗

Table 14 Comparison of other single user signature schemes based on performance parameters

Schemes	Computation overhead (ms)	Communication overhead (Bytes)
b-SPECS + [31]	High	Low
VSPN [33]	High	Low
CPAURL [34]	Low	Low
EMASEC [35]	Low	Medium
EPCABV [36]	High	High

[34], EMASEC [35] and EPCABV [36] schemes use Elliptic Curve Cryptography whereas b-SPECS + [31] scheme uses signing keys to generate signatures. These schemes use batch verification (with/without pairings) and single message verification (with/without pairings) to verify signatures. Table 12 compares schemes based on security requirements. As shown all schemes provide privacy-preservation and Message integrity. Only VSPN [33] scheme provides confidentiality and it provides all security requirements.

Table 13 compares the schemes based on security attacks based on authentication (Impersonation and Sybil attack), privacy-preservation (ID revealing attack), message integrity (modification attack) and other attacks like Man-In-Middle attack, Replay attack and Dos attack. As shown no scheme is secure against DoS attack. All schemes are secure against impersonation, ID revealing and modification attacks since they all provide privacy preservation and message integrity. Table 14 compares the schemes based on performance parameters (communication & computation overheads). These overheads are categorized as high, medium and low. As shown most of the schemes has high computation and less communication overhead.

7.2 Group Signatures

Group Signature is one among the signature based authentication schemes. It has three entities: group manager, group tracer and group members. Group manager manages the group, it is responsible for adding and removing group members. Group tracer is the only one who can trace back the identity of a group member. Group members can sign a message on behalf of the group by using a group certificate without revealing its identity. Verification of this message is done by using the group public key to identify whether the message is signed by a group member or not. It is also impossible to find whether the messages are from same group member or not. It provides traceability, unforgeability and anonymity. It is also scalable and the main drawback is that it increases computation overheads during the verification process. Group signature schemes are classified based on the signature generation as certificate based schemes, key based schemes and algorithm based schemes (the algorithm used for signature generation). Based on verification, it is classified as Cooperative message verification (with/without pairing operations), batch verification (with pairing operations) and single message verification (with/without pairing operations). Some of the group signature schemes are reviewed in this subsection.

Hao et al. [37] proposed a group signature based distributed key management framework (DKMFC). Distributed key management is used since it has better performance than centralized key management scheme. RSUs act as key distributor, it distributes keys to the vehicles when it joins the group. Since RSUs are semi-trusted, it can be compromised, which can be easily identified by using the proposed scheme. To reduce overheads cooperative message authentication is used. It does not provide privacy preservation and non repudiation which are the main drawback in this paper.

Zhu et al. [38] proposed a group signature based privacy-preserving scheme for vehicular network (EPPA). To avoid overhead caused by the Certificate Revocation List (CRL), HMAC is used. Cooperative message authentication is also used to reduce the verification burden of the RSU. Each vehicle will cooperate with one another and verify only a small number of messages to reduce overheads. Schnorr signature algorithm is used for signature generation. TA will generate and issue certificates for RSU/vehicles. Vehicles will join the group and acquire group certificate after authentication. It then uses it to communicate with other vehicles. It still has high overheads because of pairing operations.

Shao et al. [39] proposed a new group signature scheme for vehicular network (TAAP). It generates signatures by using certificates and verifies it by using the threshold based technique. It provides efficient revocation of certificates, unforgeability, anonymity and traceability. Batch verification with pairing operations is used for verification purpose. Group certificate will be generated by using the group manager's private key and any group members public key. Group members will generate signatures by using its private key and group certificate. Signature verification is done by using the public key of group manager and sender (group member). Whenever a vehicle enters into the range of an RSU, it sends join request to RSU and acquires a certificate from it for signature generation. Verification of signatures is done by using the threshold based technique. It has high computation and communication overhead.

Lu et al. [40] proposed an efficient conditional privacy preservation protocol (ECPP) using group signatures for vehicular network. It uses on-the-fly short time anonymous key to generate group signatures. It is used to fast authentication and privacy tracking with less storage space. Vehicles will send requests for this short- time anonymous key by using its location information. RSU will verifies the request and send the anonymous key and certificates for secure V2V communication. The received certificates will be verified and accepted by the vehicles if it is valid. It provides three levels of privacy, but it does not ensure traceability, non-repudiation and linkability. Single verification of certificates with bilinear pairings are used for verification purpose. It has high computation and communication overhead.

Jung et al. [41] proposed a robust and efficient anonymous authentication scheme using group signatures (REAP) for vehicular network. The drawbacks in the Lu et al. [40] ECPP scheme is discussed and a new group signature based scheme to overcome these drawbacks is proposed in this paper. Group signatures are generated by using certificates. These certificates are distributed by RSUs to the vehicles in its range after verifying vehicles legitimacy. Multiple anonymous certificates are generated which will be used by vehicles to establish secure V2V communication. Since multiple anonymous certificates are distributed to vehicles frequent request for certificates is reduced, which in turns reduces the system overheads. By using these certificates, vehicles will generate its signature and establish communication with other vehicles. Single message verification is done without using pairing operations. It provides privacy preservation, traceability, unlinkability and anonymity.

Chen et al. [42] proposed a new scheme for updating private reputation scores of public (PRRP). It uses Boneh-Boyen-Shacham short group signature scheme. It has the following properties: Group key will be accessed by all group members and each group member has its own secret key. Members can sign messages by using its secret key. Verification is done by using group public key, but the member's identity which sends the message cannot be traced and the two messages received cannot be linked. Single message verification is done without pairing operations. It provides privacy preservation, anonymity and unlinkablity. It has high computation and communication overheads.

7.2.1 Comparison

The above discussed schemes are compared based on signature generation/verification, security requirements, attacks and performance parameters in Tables 15, 16, 17 and 18. As shown in Table 15, most of the group signatures are generated by using certificates. Cooperative message verification (with/without pairing operations), batch verification (with pairing operations) and single message verification (with/without pairing operations) are used for verification purpose.

Table 16 compares the group signature schemes based on security requirements. As shown, all schemes provide anonymous message authentication. Confidentiality is not achieved in all schemes. Table 17 compares schemes based on security attacks and as shown, all schemes are secure against impersonation attack and based on the ensured security requirements, each scheme is secure against different attacks. As shown in Table 18, no scheme has low computation and communication overhead.

8 Hybrid Approach

The hybrid approach combines any two authentication technique to acquire the advantages of both the techniques. Different schemes are proposed by combining key based and certificate based authentication techniques, certificate based & signature based authentication techniques and key based and signature based authentication techniques. Hence message signing is done by using any one of these combined techniques. Message verification is

Table 15 Comparison of group signature schemes based on signature generation/verification

Schemes	Communication pattern	Signature generation method	Signature verification method
DKMFC [37]	V2R, R2V, V2V	Key Based Scheme	Cooperative Message Verification (without pairing operations)
EPPA [38]	V2R, R2V, V2V	Certificate/Schnorr algorithm	Cooperative Message Verification (with pairing operations)
TAAP [39]	V2V, V2R, R2V	Certificate Based Scheme	Batch Verification (with pairing operations)
ECPP [40]	V2V, V2R, R2V	Certificate Based Scheme	Single Verification (with pairing operations)
REAP [41]	V2V, V2R, R2V	Certificate Based Scheme	Single Verification (without pairing operations)
PRRP [42]	V2V, V2R, R2V	Boneh-Boyen-Shacham short group signature scheme	Single Verification (without pairing operations)

Table 16 Comparison of group signature schemes based on security requirements

Schemes	Privacy-preservation	Message Integrity	Non-repudiation	Traceability	Unlinkability	Confidentiality	Anonymity
DKMFC [37]	✗	✓	✗	✗	✗	✗	✓
EPPA [38]	✓	✓	✓	✓	✗	✗	✓
TAAP [39]	✓	✓	✓	✓	✗	✗	✓
ECPP [40]	✓	✗	✗	✗	✗	✗	✓
REAP [41]	✓	✓	✓	✓	✓	✗	✓
PRRP [42]	✓	✗	✗	✓	✓	✗	✓

Table 17 Comparison of group signature schemes based on resistance against security attack

Schemes	Impersonation attack	Sybil attack	ID revealing attack	Modification attack	Man-in-middle attack	replay attack	DoS attack
DKMFC [37]	✓	✗	✗	✓	✓	✗	✗
EPPA [38]	✓	✓	✓	✓	✓	✗	✗
TAAP [39]	✓	✓	✗	✓	✓	✓	✗
ECPP [40]	✓	✗	✓	✗	✗	✓	✗
REAP [41]	✓	✓	✓	✓	✓	✓	✗
PRRP [42]	✓	✗	✓	✗	✗	✓	✗

Table 18 Comparison of group signature schemes based on performance parameters

Schemes	Computation overhead (ms)	Communication overhead (Bytes)
DKMFC [37]	High	High
EPPA [38]	High	High
TAAP [39]	Medium	Medium
ECPP [40]	High	Medium
REAP [41]	High	High
PRRP [42]	High	High

done by single, batch, aggregate and cooperative message verification. Efficient way to combine authentication techniques is proposed by different researchers with better security and less overheads. Some of the existing hybrid approach schemes are discussed in this section.

Zhang et al. [43] proposed a new identity based aggregate signature scheme (DAPPA) for vehicular networks. It is proposed to deal with the challenges based on ideal tamper-proof devices (TMP). It uses realistic TMPs instead of ideal TMPs and hence the ideal TMPs issues are resolved. It uses signing keys, certificates to generate signatures. Hence it combines key based, certificate based and signature based authentication techniques. The generated signatures will be aggregated into a single signature. Hence, by verifying a single aggregate signature, it can verify many messages at the same time. Aggregate signatures are stored instead of the original messages by which it reduces the storage space of signatures. It uses pairing operations for verification. It has high overheads since it uses certificates and pairing operations.

Azees et al. [44] proposed an anonymous authentication scheme (EAAP) with conditional privacy-preservation for vehicular network. It mainly focuses on reducing the computational cost incurs in signature generation and verification. It also provides a conditional tracking mechanism to identify the compromised RSUs and attackers in the network. It uses certificate as well as signatures for message signing. It verifies one message at a time with pairings. It provides privacy-preservation, message integrity, non-repudiation and traceability. Even though it tries to reduce computation overhead, it has high overheads since it uses pairing operations.

Jo et al. [45] proposed an authentication protocol with cooperative message authentication (RCAVN) without pairings. It uses certificate based, group key based and signature based authentication techniques. Initially V2R and R2V authentication is carried out to generate and distribute group keys which will be used to establish secure V2V communications. Group keys can be easily updated whenever it is necessary with the help of RSUs. It provides message integrity, conditional privacy-preservation, traceability, unlinkability, reliability and availability. It still has high computation and communication overheads which are its drawbacks.

Zhang et al. [46] proposed a new decentralized authentication scheme (SRAPS) for vehicular networks. In this scheme instead of centralized TAs, RSUs controls the vehicles within its range (group). Each RSU will maintain on-the-fly group with the vehicles within its range. Vehicles can send messages to other vehicles in its group to establish secure V2V communication. Messages from a vehicle in a group can also be verified by vehicles in another group. In case of violations, attackers ID is revoked by using a third party. It provides robust communication, if an RSU is damaged, then it affects only the vehicles in its range services to other vehicles are not affected. It is also scalable, even with large number of vehicles, the performance are not affected. It uses certificate based, key based and group signature techniques. Verification is done by using batch verification with bilinear pairings. It provides privacy-preservation, message integrity, non-repudiation, traceability, unlinkability and confidentiality. It has medium computation and low communication overhead.

Liu et al. [47] proposed a new realistic conditional privacy preserving scheme (RDC-PAS) for vehicular network using realistic TMPs. It specifies the drawbacks in Zhang et al. [46] scheme and a new scheme is proposed to overcome specified drawbacks. It uses certificate based and IBS based techniques. Signatures are generated by using IBS scheme and verification is done by using batch verification without pairings. It provides all necessary security requirements with less computation overhead.

Jiang et al. [48] proposed a HMAC based authentication scheme (ABAH) to avoid time consuming Certificate Revocation List (CRL). It uses certificate based, group key and IBS based techniques. Signatures are generated by using HMAC and verification is done by using IBS based batch verification with bilinear pairings. Initially, TA issues certificate and signatures for RSU. Vehicles then generates its pseudo IDs and private keys. It then communicates with other vehicles using group keys. Group keys will be updated periodically by RSUs. It provides privacy-preservation, non-repudiation, message integrity and traceability. It has high computation and medium communication overhead.

Saad et al. [49] proposed a light weight authentication scheme (MFSPV) by using two different factors as parameters. The two factors which are used in the proposed scheme are Physically Unclonable Function (PUF) and dynamic pseudo IDs. Each pseudo IDs are used only once and then they are discarded. Vehicle-to-Infrastructure (V2I) communication is established securely by using two-factor mutual authentication. After successful authentication, vehicles communicate with nearby vehicles/RSUs by using hash signatures. The burden of the Certificate Authority is reduced by decreasing the dependencies. Hence the situation which leads to bottleneck in CA and RSU is avoided efficiently.

Liu et al. [50] proposed a hybrid authentication scheme (HPBS) with proxy vehicles. It uses IBS and PKI-based certificate scheme for authentication. Certificates are used for V2R and R2V authentication and V2V authentication is carried out by using IBS. In addition, proxy vehicles are used to reduce the burden of RSUs. Vehicles can be authenticated anonymously as well as in a group. Certificate authority is responsible for certificate distribution to the vehicles and RSUs which is used for long duration. Certificate revocation is also done by the CAs during which all the certificates of the RSU and vehicles are stored in CRL. It doesn't provide unlinkability.

8.1 Comparison

These schemes are compared based on authentication techniques used, message signing/verification, security requirements, resistance against security attacks and performance parameters. It is given in Tables 19, 20, 21 and 22. In Table 19, the schemes discussed are compared based on message signing and verification. As shown different authentication schemes are combined to prove better security. Message signing is based on certificates, signing keys, group signature, IBS and HMAC in DAPPA [43], EAAP [44], RCAVN [45], SRARS [46], RDCPAS [47] and ABAH [48] schemes. These schemes use batch verification (with/without pairings), single message verification (with pairings), aggregate signature verification (with pairings) and cooperative message verification (without pairings) to verify messages.

Table 19 compares schemes based on security requirements. As shown all schemes provide privacy-preservation, Message integrity, non-repudiation and traceability. Only SRAPS [46] scheme provides confidentiality by using group keys and it provides all security features. Table 20 compares the schemes based on security attacks (Impersonation, Sybil attack, ID revealing attack, modification attack, Man-In-Middle attack, Replay attack & Dos attack). As shown all schemes are secure against impersonation attack, ID revealing attack and modification attack since they provides authentication, privacy preservation and message integrity. No scheme is secure against DoS attack. Table 21 compares the schemes based on performance parameters (communication and computation overheads). As shown most of the schemes has high computation overhead. Only RDCPAS [47] scheme has less computation overhead and only SRAPS [46] scheme has less communication overhead.

9 Conclusion

Life critical messages are transmitted in the vehicular network, hence security plays a vital role. The very first step to establish secure communication is authentication, since it helps vehicles to verify the received messages before accepting them. In addition to authentication, other security requirements like privacy-preservation, non-repudiation, message integrity, traceability, unlinkability, availability etc. should also be considered to deal with the challenges and issues in the vehicular network. Researchers proposed different authentication schemes with other security requirements to establish secure vehicular communication. The existing schemes are classified based on message signing and verification process in this paper. Each category is explained with its existing authentication schemes

Table 19 Comparison of hybrid approach schemes based on message signing and verification

Schemes	Communication pattern	Authentication techniques used	Message signing method	Message verification method
DAPPA [43]	V2R, R2V, V2V	A signature is generated by using signing key and certificate	Certificate Based Scheme	Aggregate Signature Verification (with pairing operations)
EAAP [44]	V2R, R2V, V2V	A signature is generated by using signing key and certificate	Key Based Scheme	Single Message Verification (with pairing operations)
RCAVN [45]	V2R, R2V, V2V	A signature is generated by using group key and certificate	Key Based Scheme	Cooperative Message Verification (without pairing operations)
SRAPS [46]	V2V, V2R, R2V	A group signature is generated by using signing key and certificate	Group Signature Based Scheme	Batch Verification (with pairing operations)
RDCPAS [47]	V2V, V2R, R2V	An IBS is generated by using certificates	IBS	Batch Verification (without pairing operations)
ABAH [48]	V2R, R2V, V2V	A signature is generated by using HMAC, certificate, group key	HMAC	Batch Verification (with pairing operations)
MSFPV [49]	V2I, V2V	Multi-factor authentication using PUF and dynamic pseudo IDs	HMAC	Single Message Verification (without pairings)
HPBS [50]	V2V, V2P, P2V, P2R	IBS and PKI-based Certificates	IBS	Batch Verification (with pairing operations)

Table 20 Comparison of hybrid approach schemes based on security requirements

Schemes	Privacy-preservation	Message Integrity	Non-repudiation	Traceability	Unlinkability	Confidentiality
DAPPA [43]	✓	✓	✓	✓	✓	✗
EAAP [44]	✓	✓	✓	✓	✗	✗
RCAVN [45]	✓	✓	✓	✓	✓	✗
SRAPS [46]	✓	✓	✓	✓	✓	✗
RDCPAS [47]	✓	✓	✓	✓	✓	✗
ABAH [48]	✓	✓	✓	✓	✗	✗
MSFPV [49]	✓	✓	✓	✓	✓	✗
HPBS [50]	✓	✓	✓	✓	✗	✗

Table 21 Comparison of hybrid approach schemes based on resistance against security attacks

Schemes	Impersonation Attack	Sybil Attack	ID Revealing Attack	Modification Attack	Man-in-Middle Attack	Replay Attack	DoS Attack
DAPPA [43]	✓	✗	✓	✓	✗	✗	✗
EAAP [44]	✓	✓	✓	✓	✓	✓	✗
RCAVN [45]	✓	✓	✓	✓	✗	✗	✗
SRAPS [46]	✓	✓	✓	✓	✓	✗	✗
RDCPAS [47]	✓	✗	✓	✓	✗	✓	✗
ABAH [48]	✓	✗	✓	✓	✗	✓	✗
MSFPV [49]	✓	✓	✓	✓	✗	✓	✗
HPBS [50]	✓	✓	✓	✓	✗	✓	✗

Table 22 Comparison of hybrid approach schemes based on performance parameters

Schemes	Computation overhead (ms)	Communication overhead (Bytes)
DAPPA [43]	High	Medium
EAAP [44]	High	High
RCAVN [45]	High	Medium
SRAPS [46]	Medium	Low
RDCPAS [47]	Low	Medium
ABAH [48]	High	Medium
MSFPV [49]	Low	Low
HPBS [50]	High	Medium

and compared based on security requirements, attacks and performance parameters. It is observed that most of the schemes have high overheads and are insecure against few security attacks since they do not provide essential security requirements. Hence, it is concluded that for infrastructure- based communications, (V2R and R2V) proxy vehicle- based authentication schemes can be used, whereas it is not suitable for inter-vehicular communication since it has high overheads. Authentication without proxy vehicles can be used for inter-vehicular communication since it has less overheads. This survey will be helpful for researchers to design secure authentication schemes for vehicular networks.

Authors' Contribution All the authors have participated in writing the manuscript and have revised the final version. All authors read and approved the final manuscript.

Funding The authors have no relevant financial or non-financial interests to disclose.

Declarations

Conflict of interest The authors have no conflicts of interest to declare that are relevant to the content of this article.

Ethics approval This article does not contain any studies with human participants and/or animals performed by any of the authors.

Informed Consent There is no informed consent for this study.

References

1. Shen, X., Cheng, X., Yang, L., Zhang, R., & Jiao, B. (2014). Data dissemination in vanets: A scheduling approach. *IEEE Transactions on Intelligent Transportation Systems, 15*, 2213–2223. https://doi.org/10.1109/TITS.2014.2313631
2. Shen, X., Zhang, R., Yang, X. C. L., & Jiao, B. (2013). Cooperative data dissemination via space-time network coding in vehicular network. *IEEE GLOBECOM, Atlanta*. https://doi.org/10.1109/GLOCOM.2013.6831599
3. Yang, L., & Wang, F. (2007). Driving into intelligent spaces with pervasive communications. *IEEE Transactions on Intelligent Transportation Systems, 22*, 12–15. https://doi.org/10.1109/MIS.2007.8
4. Anita, E. A. M., & Jenefa, J. (2016). A survey on authentication schemes of VANETs. *International Conference on Information Communication and Embedded Systems (ICICES), 2016*, 1–7. https://doi.org/10.1109/ICICES.2016.7518946
5. Mejri, M. N., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications, 1*, 53–66. https://doi.org/10.1016/j.vehcom.2014.05.001
6. Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., & Weil, T. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *Communications Surveys & Tutorials, IEEE, 13*, 584–616. https://doi.org/10.1109/SURV.2011.061411.00019
7. Raw, R. S., Kumar, M., & Singh, N. (2013). Security Challenges, issues and their solutions for VANET. *International Journal of Network Security & Its Applications (IJNSA)., 5*, 95–105. https://doi.org/10.5121/ijnsa.2013.5508
8. Samara, Gh., Al-Salihy, W. A. H., & Sures, R. (2010). Security analysis of of vehicular Ad Hoc networks (VANET). *Network Applications Protocols and Services (NETAPPS)*. https://doi.org/10.1109/NETAPPS.2010.17
9. Chauley, N. K. (2016). Security analysis of vehicular Ad Hoc networks (VANETs): A comprehensive study. *International Journal of Security and Its Applications, 10*(261), 274.
10. Mokhtar, B., & Azab, M. (2015). Survey on security issues in vehicular Ad Hoc Networks. *Alexandria Engineering Journal, 54*, 115–1126. https://doi.org/10.1016/j.aej.2015.07.011
11. Nai, L., & Jia, T. (2016). An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings (ECPAS). *IEEE Transactions on Intelligent Transportation Systems, 17*, 1319–1328. https://doi.org/10.1109/TITS.2015.2502322

12. Vijayakumar, P., Azees, M., Kannan, A., & Deborah, L. J. (2015). Dual authentication and key management techniques for secure data transmission in vehicular Ad Hoc networks. *IEEE Trans on Intelligent Transportation Systems, 17*, 1015–1028. https://doi.org/10.1109/TITS.2015.2492981
13. Wazid, M., Das, A. K., Kumar, N., Odelu, V., Reddy, A. G., & Park, K. P. A. Y. (2017). Design of lightweight authentication and key agreement protocol for vehicular Ad Hoc networks. *IEEE Access, 5*, 14966–14980. https://doi.org/10.1109/ACCESS.2017.2723265
14. Mahagaonkar, S. V., Dongre, N. (2017). *TEAC: Timed Efficient Asymmetric Cryptography for Enhancing Security in VANET International Conference on Nascent Technologies in the Engineering Field* 1–5.
15. Xiong, H., Chen, J., Mei, Q., Zhao, Y. (2020). Conditional privacy-preserving authentication protocol with dynamic membership updating for VANETs. In *IEEE Transactions on Dependable and Secure Computing*, doi: https://doi.org/10.1109/TDSC.2020.3047872.
16. Jenefa, J., & Anita, E. (2019). An enhanced secure authentication scheme for vehicular Ad Hoc networks without pairings. *Wireless Personal Communications, 106*, 535–554.
17. He, D., Zeadally, S., Baowen, Xu., & Huang, X. (2015). Efficient identity based conditional privacy-preserving authentication scheme for vehicular Ad Hoc network (EICPAS). *IEEE Transactions on Information Forensics and Security, 10*, 2681–2691. https://doi.org/10.1109/TIFS.2015.2473820
18. Liu, Y., Wang, L., & Chen, H.-H. (2014). Message authentication using proxy vehicles in vehicular Ad Hoc networks (PBAS). *IEEE Transactions on Vehicular Technology, 64*, 3697–3710. https://doi.org/10.1109/TVT.2014.2358633
19. Xie Yong, Wu., Libing, Z. Y., & Jian, S. (2016). Efficient and secure authentication scheme with conditional privacy-preserving for VANETs (ECASCP). *Chinese Journal of Electronics, 25*, 950–956. https://doi.org/10.1049/cje.2016.08.027
20. Tzeng, S.-F., Horng, S.-J., Li, T., Wang, X., Huang, P.-H., & Khan, M. K. (2017). Enhancing security and privacy for identity-based batch verification scheme in VANET (ESPIBV). *IEEE Transactions on Vehicular Technology, 66*, 3535–4348. https://doi.org/10.1109/TVT.2015.2406877
21. Cui, J., Zhang, J., Zhong, H., & Yan, Xu. (2017). SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter. *IEEE Transactions on Vehicular Technology, 66*, 10283–10295. https://doi.org/10.1109/TVT.2017.2718101
22. Asaar, M. R., Salmasizadeh, M., Susilo, W., & Majidi, A. (2018). A secure and efficient authentication technique for vehicular Ad-Hoc networks (ID-MAP). *IEEE Transactions on Vehicular Technology, 67*, 5409–5423. https://doi.org/10.1109/TVT.2018.2822768
23. Jenefa, J., & Anita, E. A. M. (2021). Identity-based message authentication scheme using proxy vehicles for vehicular ad hoc networks. *Wireless Networks, 27*, 3093–3108.
24. Zhong, H., Wen, J., Cui, J., & Zhang, S. (2016). Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET (ECPASP). *Tsinghua Science and Technology, 21*, 620–629. https://doi.org/10.1109/TST.2016.7787005
25. Li, J., Huang, L., & Guizani, M. (2015). ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. *IEEE Transactions on Parallel and Distributed Systems, 26*, 938–948. https://doi.org/10.1109/TPDS.2014.2308215
26. Sun, C., Liu, J., Xinpeng, Xu., & Ma, J. (2017). A privacy-preserving mutual authentication resisting DoS attacks in VANETs (MADAR). *IEEE Access, 5*, 24012–24022. https://doi.org/10.1109/ACCESS.2017.2768499
27. Ning, P., Liu, A., & Du, W. (2008). Mitigating DoS attacks against broadcast authentication in wireless sensor networks. *ACM Transactions on Sensor Networks, 4*, 1–35. https://doi.org/10.1145/1325651.1325652
28. Jenefa, J., & Mary Anita, E. A. (2018). Secure vehicular communication using ID based signature scheme (SVCIBS). *Wireless Personal Communications, 98*, 1383–1411. https://doi.org/10.1007/s11277-017-4923-7
29. Sun, J., Zhang, C., Zhang, Y., & Fang, Y. (2010). An identity-based security system for user privacy in vehicular Ad Hoc networks (IBSSUP). *IEEE Transactions on Parallel and Distributed Systems, 21*, 1227–1239. https://doi.org/10.1109/TPDS.2010.14
30. Alshudukhi, J. S., Mohammed, B. A., & Al-Mekhlafi, Z. G. (2020). Conditional privacy-preserving authentication scheme without using point multiplication operations based on elliptic curve cryptography (ECC). *IEEE Access, 8*, 222032–222040. https://doi.org/10.1109/ACCESS.2020.3044961
31. Horng, S.-J., Tzeng, S.-F., Pan, Yi., Fan, P., Wang, X., Li, T., & Khan, M. K. (2013). b-SPECS+: Batch verification for securepseudonymous authentication in VANET. *IEEE Trans on Information Forensics and Security, 11*, 1860–1675. https://doi.org/10.1109/TIFS.2013.2277471
32. Chim, T. W., Yiu, S. M., Hui, L. C. K., & Li, O. K. (2011). SPECS: Secure and privacy enhancing communications schemes for VANETs. *Ad Hoc Networks, 9*, 189–203. https://doi.org/10.1016/j.adhoc.2010.05.005

33. Chim, T. W., Yiu, S. M., Hui, L. C. K., & Li, V. O. K. (2012). VSPN: VANET-based secure and privacy-preserving navigation. *IEEE Trans on Computers, 2*, 510–524.
34. Zhong, H., Huang, Bo., Cui, J., Yan, Xu., & Liu, Lu. (2018). Conditional privacy-preserving authentication using registration list in vehicular Ad Hoc networks (CPAURL). *IEEE Access, 6*, 2241–2250. https://doi.org/10.1109/ACCESS.2017.2782672
35. Cui, J., LuWei, J. Z., Yan, Xu., & Zhong, H. (2018). An efficient message-authentication scheme based on edge computing for vehicular Ad Hoc networks (EMASEC). *IEEE Trans on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2018.2827460
36. Gayathri, N. B., Gowri Thumbur, P., Reddy, V., & Md. Zia Ur Rahman, . (2018). Efficient pairing-free certificateless authentication scheme with batch verification for vehicular Ad-Hoc networks (EPCABV). *IEEE Access, 6*, 31808–31819. https://doi.org/10.1109/ACCESS.2018.2845464
37. Yong Hao, Yu., Cheng, C. Z., & Song, W. (2011). A distributed key management framework with cooperative message authentication in VANETs (DKMFC). *IEEE Journals on Selected Areas in Communications, 29*, 616–629. https://doi.org/10.1109/JSAC.2011.110311
38. Zhu, X., Jiang, S., Wang, L., & Li, H. (2014). Efficient privacy-preserving authentication for vehicular Ad Hoc networks (EPPA). *IEEE Trans on Vehicular Technology, 63*, 907–919. https://doi.org/10.1109/TVT.2013.2294032
39. Shao, J., Lin, X., Rongxing, Lu., & Zuo, C. (2015). A threshold anonymous authentication protocol for VANETs (TAAP). *IEEE Trans on Vehicular Technology, 65*, 1711–1720. https://doi.org/10.1109/TVT.2015.2405853
40. Lu, R., Lin, X., Zhu, H., Ho, P-H, (Sherman) Shen, X. (2008). ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. 2008 IEEE Infocom Conference. 1903–1911. https://doi.org/10.1109/INFOCOM.2008.179.
41. Jung, C. D., Sur, C., Park, Y., & Rhee, K.-H. (2009). A Robust and efficient anonymous authentication protocol in VANETs (REAP). *Journal of Communications and Networks, 11*, 607–614. https://doi.org/10.1109/JCN.2009.6388414
42. Chen, L., Li, Q., Martin, K. M., & Ng, S.-L. (2016). Private reputation retrieval in public – a privacy-aware announcement scheme for VANETs (PRRP). *IET Information Security, 11*, 204–210. https://doi.org/10.1049/iet-ifs.2014.0316
43. Zhang, L., Qianhong, Wu., Domingo-Ferrer, J., Qin, Bo., & Chuanyan, Hu. (2016). DAPPA: Distributed aggregate privacy-preserving authentication in VANETs. *IEEE Trans on Intelligent Transportation Systems, 18*, 516–526. https://doi.org/10.1109/TITS.2016.2579162
44. Azees, M., Vijayakumar, P., & Deboarh, L. J. (2017). EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular Ad Hoc networks. *IEEE Trans on Intelligent Transportation Systems, 18*, 2467–2476. https://doi.org/10.1109/TITS.2016.2634623
45. Jo, H. J., Kim, I. S., & Lee, D. H. (2018). Reliable cooperative authentication for vehicular networks (RCAVN). *IEEE Trans on Intelligent Transportation Systems, 19*, 1065–1079. https://doi.org/10.1109/TITS.2017.2712772
46. Zhang, L., Qianhong, Wu., Solanas, A., & Domingo-Ferrer, J. (2010). A Scalable robust authentication protocol for secure vehicular communications (SRAPS). *IEEE Trans on Vehicular Technology, 59*, 1606–1617. https://doi.org/10.1109/TVT.2009.2038222
47. Liu, Z.-C., Ling Xiong, Tu., & Peng, D.-Y. (2018). A realistic distributed conditional privacy preserving authentication scheme for vehicular Ad Hoc networks (RDCPAS). *IEEE Access, 6*, 26307–26317. https://doi.org/10.1109/ACCESS.2018.2834224
48. Jiang, S., Zhu, X., & Wang, L. (2016). An efficient anonymous batch authentication scheme based on HMAC for VANETs (ABAH). *IEEE Trans on Intelligent Transportation Systems, 17*, 2193–2204. https://doi.org/10.1109/TITS.2016.2517603
49. Alfadhli, S. A., Lu, S., Chen, K., & Sebai, M. (2020). MFSPV: A multi-factor secured and lightweight privacy-preserving authentication scheme for VANETs. *IEEE Access, 8*, 142858–142874.
50. Liu, H., Wang, H., & Gu, H. (2020). HPBS: A hybrid proxy based authentication scheme in VANETs. *IEEE Access, 8*, 161655–161667. https://doi.org/10.1109/ACCESS.2020.3021408

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

J. Jenefa received her Bachelor's and Master's degree in Computer Science & Engineering. She holds a Ph.D. in Information and Communication Engineering from Anna University, Chennai. She is currently an assistant professor in the Department of Computer Science and Engineering of Christ (Deemed to be University), Bangalore. Her current research focuses on Network Security and Vehicular Ad hoc Networks.

E. A. Mary Anita holds a B.E in Electrical and Electronics Engineering and M.E in Computer Science & Engineering, both from Government College of Engineering, Tirunelveli, India and a Ph.D. in Information and Communication from Anna University, Chennai. She is presently Professor in Computer Science and Engineering Department of Christ (Deemed to be University), Bangalore. She has over 30 years of teaching experience and has published more than 80 research papers in International and national journals and conferences. Her main research interests are in the field of wireless networks, security and privacy. She is a Life member of Indian Society for Technical Education (ISTE), Computer Society of India (CSI), IEEE, IAENG and ACM. She is a peer reviewer for referred International Journals. Her biography has been included in the 2014 edition of Who's Who in the World, USA. Email: maryanita.ea@christuniversity.in