Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 45 No. 7
July 2024

A Study of Authentication and Privacy-Preserving Schemes for Vehicular Networks

Kamal Kumar[1], Vinod Kumar[2,*] and Renu[1]
[1]Department of Mathematics, Baba Mastnath University, Rohtak - 124021, India
[2]Department of Mathematics, Shyam Lal College, University of Delhi, New Delhi 110032, India
*: Corresponding author

Abstract
Vehicular networks (VNs) enhance vehicle efficiency, passenger safety, and comfort by communicating traffic and infotainment information. Their acceptance hinges on message speed, accuracy, privacy, and safety. Vehicle authentication ensures communication accuracy, necessitating an effective privacy-preserving system. Security and privacy concerns must be addressed within the communication protocol architecture. Despite the development of various privacy-preserving authentication systems, many methods do not fully resolve threats, vulnerabilities, computing costs, and communication issues. This survey focuses on cryptographic techniques, including symmetric key cryptography, public key cryptography, identity-based cryptography, pseudonym-based cryptography, group and ring signature-based schemes, and blockchain-based schemes, for authentication and privacy in VNs. The analysis reveals reliance on opaque trusted authorities and significant computational overhead, impacting message delivery. Further improvements in lightweight, efficient authentication systems are needed.
Keywords: Authentication, Cryptography, Security, Privacy, Vehicular network

1. Introduction

Lorem A vehicle-associated network (VANET) connects automobiles, buses, trucks, and other roadside infrastructure [1]. Every car is fitted with a transmission device, which facilitates communication between the vehicle and adjacent vehicles as well as infrastructure [2]. The trusted authority (TA), roadside unit (RSU), and on-board unit (OBU) aboard automobiles make up a vehicular network. Using RSUs to verify vehicles, the TA is a third-party device that registers RSUs and uses them to monitor the entire network [3]. Positioned beside the road, the RSU is a fixed wireless device (such as WiFi or WiMAX) that serves as an intermediary between the vehicle's OBU and TA, relaying safety directives to neighboring vehicles [4].

The vehicle to vehicle (V2V) and vehicle to infrastructure (V2I/I2V) communication modes are used in VANETs, as seen in Fig. 1. The protocol used for dedicated short-range communication (DSRC) is employed in both V2V and V2I communications [5]. Subsequently, the IEEE 802.11p standard for wireless communication is used by the DSRC protocol, which is now known as WAVE, or wireless access in automotive environments [6]. Every 100–300 ms, a car broadcasts messages of information to other vehicles or RSUs. The maximum communication range of VANETs is up to 1 kilometer, and the transmission speed ranges from 6 to 27 Mbps, according to the DSRC standard. Communications are divided into two categories: non-safety and safety. The vehicle uses V2V communication to process, exchange, transmit, or receive critical messages regarding traffic situations to or from other vehicles. Similar to how automobiles and RSUs communicate with one another, RSUs use V2I/I2V communication to deliver real-time services to drivers, including internet connectivity, navigation, and live streaming of incidents [7, 8].

Through the assistance of another vehicle in its vicinity, a vehicle relays safety messages to the distant car. The message can still be sent using other active cars if any intermediate vehicle is unable to do so. Therefore, all of the vehicles are given enough power and storage by the vehicular network to broadcast information to nearby members about accidents, crises, and traffic congestion [9, 10]. Vehicles can communicate not only safety signals but also informational messages about road conditions, allowing the recipient to respond to information from other members or drive to a safer route to avoid accidents [11, 12]. Using an open wireless channel, an attacker can intercept, change, duplicate, or remove messages as they are transmitted. To affect drivers of automobiles, the attacker can, for instance, change safety-related messages to ones that cause accidents. Additionally, it might fabricate a misleading impression of traffic congestion to impede the network's regular operation [13, 14]. To meet an

attacker's challenge, a suitable mechanism must be built within the vehicle network and communication protocol. Prior to the deployment of automotive networks, these security challenges take the form of privacy and authentication problems that need to be resolved. Table 1, shows that the comparison with comparable, currently conducted surveys with an eye toward security measures and proposed approach.

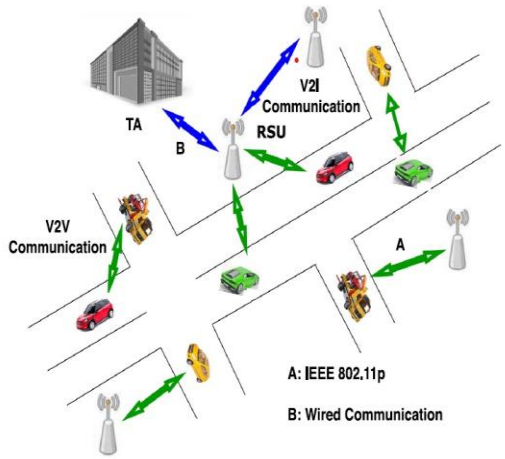

Fig. 1: The vehicular network's basic architecture [21]

1.1 Contribution of the paper

The primary goal of this work is to evaluate, assess, and discuss the shortcomings of various privacy-preserving and authenticating techniques that have been put out during the past ten years. The fundamentals of vehicle network security are also covered in this article. The following sums up the primary contributions of the current survey:

- In order to develop effective and dependable communication between the network members, we have comprehensively supplied the details of various security and privacy needs in vehicle networks in this study.
- The fundamental design and characteristics of the vehicular network, as well as the many standards and messages that are employed, have also been briefly discussed.
- We offer a thorough analysis of the current safe authentication and privacy-maintaining protocols in automobile networks. In order to comprehend their successes as well as shortcomings, this article also provides a quick description of their approaches and strengths.
- A brief overview of the current literature on authentication and privacy-preserving techniques has been provided. We have also included a comparison between the current paper and other surveys that take into account the security techniques in use.

Table 1: Comparison of comparable current security mechanism works

Security mechanism	**[15]**	**[16]**	**[17]**	**[18]**	**[19]**	**[20]**
Symmetric key cryptography	Y	Y	N	Y	N	N
Blockchain	N	N	N	N	N	N
Public key cryptography	Y	Y	N	Y	Y	Y
Group signature	Y	Y	N	Y	Y	Y
Ring signature	N	N	N	N	N	N
Pseudonyms	Y	Y	Y	N	Y	Y
Certificateless signatures	N	N	N	Y	N	N
Identity-based cryptography	Y	Y	N	Y	Y	Y

2. Background of vehicular network

In this section, we provide a brief explanation of the system paradigm, security features, message formats and standards, and some basic information about vehicular networks.

2.1 System model

Typically, a vehicular network consists of the following components, which are shown in Fig. 1 as the basic system model [22].

- **OBU:** An onboard unit that can connect with RSUs and the OBUs of other vehicles is installed in every vehicle in the network. Storage devices, systems, processors, and sensors are all included. After the information from the sensors is processed, the processing unit creates messages. Eventually, wireless channels are used to send these signals to nearby members.
- **RSU:** The roadside units are often stationary objects that are placed beside roadways, at intersections, or in parking lots. RSUs have a transmission mechanism that facilitates both infrastructure communication and DSRC. Providing internet access to OBUs is one of

RSUs' main goals. (2) To send messages to additional RSUs and OBUs in order to extend the transmission range of vehicular networks. (3) To report unintentional incidents or traffic conditions.

- **TA:** A wired channel is used to connect RSUs and the trusted authority. It oversees the whole network and serves as an administrator. Additionally, TA is in charge of creating, disseminating, and routinely upgrading the network's system settings. Additionally, it verifies the authenticity of cars and takes them out if they are spreading fraudulent information or engaging in criminal conduct. As a result, TA has much more processing power and storage capacity than OBU and RSUs.

2.2 Properties of vehicular networks

The fundamental characteristics that set vehicular networks apart are as follows [23]:

- **Computation and storage capacity:** It is essential to process the data that is received, compute the required outcomes, store them, and send them to other participants. As a result, one of the difficult problems in VNs is data calculation and storage.
- Mobility: Generally speaking, vehicles in VNs move quickly. In V2V communication, even a slight transmission delay can therefore cause serious issues.
- **Network topology:** Vehicle topology fluctuates quickly as a result of their high speeds. This makes a vehicle more likely to be malicious and raises network susceptibility.
- **Unpredictability:** Two members only create a connection once while traveling due to the great mobility of automobiles. As such, maintaining one's true identity or private information in VNs is challenging.

3. Security requirements in VNs

To ensure the authenticity of cars, a VNs possesses two distinct features [24]. Two factors contribute to this transient connection between vehicles: first, cars are always changing their immediate neighborhood; second, vehicle-to-vehicle (V2V) communication allows information transmission between vehicles without the need for infrastructure participation or intervention. cars must, however, also have faith in the data that other cars provide in order for V2V communication to occur. Vehicle authentication is required to lessen this inclination. Nonetheless, the vehicle verification procedure can disclose the identification of the automobiles. Drivers whose identities are revealed by their vehicles may be seriously threatened by the privacy breach. This danger can make joining a VN less appealing than the benefits it offers and discourage car owners from doing so. Therefore, for VN to be viable and accepted, privacy-preserving authentication is required. These fundamental security standards must be met in order for a VN to be utilized.

3.1 Authentication in VNs

When installing VNs, the main problem is with V2I and V2V communication security. Any successful attack by a car might have a major impact on network services and operations. To disrupt the network, the attacker might erase, alter, follow, or replicate communications. It has the potential to modify the important data sent by the government or automobiles through communications [25]. The transmission of phony messages into the network by a vehicle needs to be stopped. It is therefore crucial for the authority to identify and eliminate any malicious vehicles from VNs. Additionally, it's necessary to authenticate the vehicle's actual identity. Determining whether or not the legitimate member has delivered the message is made possible through vehicle authentication, which is a crucial security need in VNs [26]. Message authentication is also required for VNs, just like identity authentication. It is necessary to immediately eliminate and prevent fraudulent communications from being sent into the network. It makes sure that throughout transmission, the message is neither copied or altered. If an attacker alters the contents of the received message, TA may transmit the incorrect decision or command, leading to a chaotic traffic condition [27, 28]. When attempting to identify and distinguish between the actions of authorized and unauthorized members, the administrator must overcome numerous challenges. In order to serve a personal purpose, a car may transmit malicious information across the network [29, 30]. As a result, message authentication is crucial in VNs, and a car needs to confirm the message's legitimacy.

3.2 Privacy in VNs

During the authentication process, the sender's privacy must be protected by the authority or recipient. While the approved vehicle's identity is kept hidden from the network, an attacker may use it to send malicious information. It might potentially reveal confidential information about the permitted car. As an alternative, the attacker can attempt to track down the car's owner

by utilizing its route or navigation data [31]. The VNs must thus guarantee its users' location and identity privacy. An authorized vehicle may occasionally attempt to obstruct lawful traffic in order to engage in fraud. Therefore, in order for the authority to reveal the vehicle when needed, it must possess the necessary information on it. In VNs, protecting the true identity of a genuine vehicle while simultaneously identifying and removing a malicious vehicle from the network is a crucial but challenging task. For this reason, the authority needs to guarantee conditional privacy-preserving authentication for every vehicle connected to the network.

In addition to privacy and authentication, some fundamental needs in VNs are as follows [32]:

- **Availability:** This characteristic guarantees that even in the event of an adversary conducting an attack within the network, the hardware or software will continue to function as intended. Under all circumstances, the network's components must remain operational and accessible.
- **Confidentiality:** This feature makes sure that the information or safety message is sent in the original format to the appropriate recipient or members. Viewing or reading the message's contents is restricted to the specified members only. If this attribute is broken, confidential information about the sender or recipient may be revealed.
- **Integrity:** This characteristic guarantees that data or messages are sent over the network unaltered or updated. In order to cause havoc on the network, the attacker could add or update content in the message. In order to be confident, the message was not altered or distorted during transmission, the recipient must confirm it.
- **Non-repudiation:** Its attribute guarantees that the sender wouldn't dispute the ownership of the communication. Due of the network's transmission of fraudulent communications, this characteristic is necessary in the event of an accident or mishap. As a result, the sender is accountable for the messages it sent during transit.
- **Scalability:** With this feature, network productivity and efficiency are guaranteed to remain constant even in the event of a persistent fluctuation in the number of registered members. VNs have a high vehicle density because of the frequent travel of their cars. Scalability makes sure that the RSUs, authorities, or vehicles won't be impacted by this abrupt fluctuation in performance.
- **Unforgeability:** By virtue of this feature, the legitimate network member can be sure that an attacker cannot fake the signature of a message that is sent. A duplicate signature could be made by an attacker by replaying or reusing the correct message.
- **Unlinkability:** This feature makes sure that the sender of the message or signature cannot be connected to the driver of the car or its true identity by an attacker. In spite of analysis of the message, its contents, or its signature, this attribute aids the VANET in keeping the vehicle's secret information hidden.
- **Traceability and member revocation:** With this feature, the malicious vehicle's true identity can be ascertained and disclosed to the tracing manager or other trusted authority upon request. Finding the same is occasionally necessary to keep the network's order in place, even while the vehicle's true identity must be kept secret. Also, the malicious vehicle needs to be taken out of VNs by the authority quickly to prevent further network harm. Revocation of the membership is necessary to prevent the malicious vehicle from interfering with the regular operation of the network and the other cars.
- **Transparency:** This attribute guarantees the credibility and dependability of the trusted authority's or administrator's operations. To enable each network member to trust the actions taken by the authority or other members, the VNs must satisfy this need.

4. Categorization of privacy-preserving and authenticating protocols

We categorize the current authentication and privacy-preserving techniques in this area. The methods used in symmetric key cryptography, public key cryptography, identity-based cryptography, group and ring signatures, blockchain, and pseudonyms are the foundation of this classification.

4.1 Schemes based on symmetric key cryptography

This category is based on symmetric key cryptography schemes, where the primary function of a symmetric key in VN security methods. The symmetric key can be quickly computed by the sender and the recipient, who can then utilize it to maintain communication privacy. Furthermore, under these schemes, communications are also authenticated using the message authentication code (MAC).

Table 2: Schemes based on SKC

Scheme	Advantages and properties	Limitations
[33]	In order to provide secure data transmission throughout the network, this technique offers member authentication and guarantees effective key distribution.	The packet loss rates and end-to-end latency in VNs are not disclosed.
[34]	This technique accomplishes message integrity and privacy preservation by proposing an anonymous authentication and key distribution protocol.	Resilience against replay and impersonation attacks is not offered by it.
[35]	This technique is based on two-factor authentication using a biological password and the decentralization of CA. It lowers the overhead of calculation and key updating.	Batch message verification is not offered.
[36]	Through the use of binary pairing, this methodology suggests an anonymous batch authentication technique. Because it uses a group-based scheme and HMAC, it does away with the need for CRLs.	The transmission latency has grown, and as speed increases, so does packet loss.

Using the shared secret key, the sender generates a MAC for every communication. The MAC received with the message can be verified by a network member who has the same key. These techniques are utilized in VNs because they can be quickly verified and have lower computing and communication costs. A summary of systems based on symmetric key cryptography is provided in Table 2.

4.2. Public key cryptography-based (PKC) protocols

This type of method relies on public key cryptography, where the distribution of public-private key pairs to authorized participants for communication is managed by TA. For authentication, this infrastructure includes the digital signature of the CA and the vehicle's public key. For authentication, this infrastructure includes the digital signature of the CA and the vehicle's public key. Utilizing these approaches, a reliable and safe technique for vehicle authentication that protects privacy is implemented. Certificates issued by the CA are used to achieve traceability. A summary of the public key cryptography-based techniques is provided in Table 3.

Table 3: PKC-based protocols

Scheme	Advantages and properties	Limitations
[37]	By utilizing distributed computing, this technique reduces the workload on RSUs and TA. To guarantee conditional privacy, the TA can eliminate rogue cars from the network.	There is question about the procedures used to choose proxy cars and eliminate rogue vehicles from the network.
[38]	To enable hierarchical aggregation and quick reaction, this approach makes use of short-term pseudonyms. Furthermore, the aggregation protocol and signature generation are utilized to guarantee secure vehicular communications.	There is no comparative study offered to demonstrate the efficacy of this strategy in comparison to others.
[39]	This approach offers network participants anonymous authentication that protects their privacy while being computationally efficient. Additionally, it stops the opponent from revealing the	Maintaining and revoking pseudonym certificates takes a lot of time and is not an efficient process.

	sender's true identity to the public.	
[40]	Bilinear pairing is used in this technique to enable anonymous conditional privacy-preserving authentication. Without TA, RSUs and vehicles authenticate one another.	The cost of calculation and transmission is significantly increased by managing and rescinding anonymous certificates.
[41]	Using the local identity, this technique suggests message authentication. It guarantees non-repudiation, traceability, and message integrity and authenticity.	Increasing the computation and communication expenses are the certificate distribution, CRL administration, and member revocation.
[42]	This method does away with the need for CRL checking time by using Merkle hash trees and fog computing.	Keeping each member's copy of the Merkle tree up to date and maintained is challenging.
[43]	Private certificate linking and revocation are provided by this scheme. Without linkage authority, it utilizes the public key infrastructure for vehicles.	Its efficiency and cost-effectiveness are not demonstrated by comparison with current solutions.

4.3. Identity-based cryptography (IBC) protocols

Identity-based cryptography techniques provide the basis for this category. This generates the public key for the car using the required data (such the phone number and email address). Therefore, there is no longer a need for certificate distribution and management. Certificates are not used in these schemes to authenticate messages. As a reliable third-party member, the KGC provides each member with a private key. The identity-based cryptography schemes are summarized in Table 4.

Table 4: IBC based protocols

Scheme	Advantages and properties	Limitations
[44]	The anonymous identity used in this technique allows for privacy-preserving authentication. Transparency, non-repudiation, traceability, and integrity are all guaranteed.	The lack of a graph or mathematical evidence proving its superior performance over alternative strategies is evident.
[45]	In order to maintain anonymity, this technique offers id-based online and offline signing. Both cross-region and cross-RSU V2V authentication are included.	A distinct mutual authentication technique for cars and RSUs contributes to the high level of complexity.
[46]	To provide source and message authentication, this system makes use of a one-way hash function. It can withstand an adaptively selected message attack.	As the density rises, the message loss ratio is not provided.
[47]	The cryptographic mix-zone protocol and the identity-based authenticated asymmetric group key agreement protocol have been proposed by this approach. It runs with effective key updating and completely depends on reliable vendors.	In order to encrypt and decrypt the messages, vehicles must use the same group private key. A hacker could simply obtain the private data transmitted over messages if they manage to obtain this key.

[48]	This system makes use of bilinear pairing, multiple Diffie-Hellman assumptions, and anonymous identity. It offers unforgeability and message authentication.	The complexity and computational burden are increased by the bilinear pairing operation.
[49]	To accomplish privacy-preserving authentication, this system makes use of the cuckoo filter, binary search, and ECC. The collection of signatures from numerous vehicles can all be verified simultaneously by an RSU.	The entire network can be destroyed by the key escrow issue since the TA is able to calculate every private key for every vehicle.
[50]	Identity-based batch verification is used in this technique to address privacy and security concerns. Preloading the password, private keys, and true identity into each vehicle's TPD is done by the TA.	Due to the intricate process of generating an anonymous identity and completing message signing and verification, there is a significant computing overhead.

4.4. Certificateless signature (CLS)-based protocols

This type of technique relies on certificateless signature-based systems, which do not require certificates. The CRL management problem in conventional PKC-based schemes and the key-escrow issue in IBC schemes are resolved by these schemes. Furthermore, these schemes do not call for the distribution of certificates to cars and the removal of those certificates from the network. The schemes based on certificateless signatures are compiled in Table 5.

Table 5: CLS based protocols

Scheme	Advantages and properties	Limitations
[51]	This signature technique does not utilize bilinear pairing and is based on elliptic curves. The private key is used by a vehicle to sign the message, and the public key is used by the recipient to confirm the signature.	It does not include the network's cost for processing and communication.
[52]	There is only one group element in the signature, and the scheme is based on bilinear pairings, certificateless short signatures, and does not employ the Map to Point hash operation.	As the density of vehicles grows, the effectiveness of communication diminishes.
[53]	This approach for aggregating signatures without a certificate offers conditional privacy, enabling law enforcement to ascertain the true identity of a malicious vehicle.	As the number of vehicles increases, so does the complexity and computation of the certificateless aggregate signature, causing it to suffer from scalability issues.
[54]	This approach for certificateless aggregate signatures has been enhanced. In order to boost efficiency and expedite the verification process, RSUs perform batch message verification.	In comparison to the current certificateless aggregate signature systems, the complexity is substantial.
[55]	Conditional privacy is achieved by this system through the	Compute and communication costs are greatly

	employment of a pseudo-identity technique. Message authentication is carried out and the burden on computing and transmission devices is decreased using the signature aggregation technique.	increased by the intricate signature aggregation, pseudonym formation, and verification process.

4.5 Pseudonym-based schemes

Pseudonym-based systems are mandatory for this category. To begin with, the car uses the secure channel to transmit its true identification and pertinent data to TA via RSU. After confirming the information, TA sends the corresponding vehicle the pseudo-identity and its validity. During vehicle communication, the pseudo-identity is utilized to provide total anonymity and authentication. Unlinkability can be ensured in part by preventing the linking of two pseudonyms for the same vehicle in order to determine the real identity or vehicle identification. Should the car be connected to any malicious behavior, the TA can also use the pseudonym to identify the genuine owner. Schemes based on pseudonyms are summarized in Table 6.

Table 6: Pseudonym-based schemes

Scheme	Advantages and properties	Limitations
[56]	In order to provide conditional privacy, this approach offers pseudonym-based authentication. Attackers are unable to identify the vehicle's true identity.	The high burden of CRL management is causing it problems.
[57]	To achieve privacy-preserving authentication and boost efficiency, this technique makes use of ECC and a collision-resistant hash function.	The statistical analysis of the quantity of messages evaluated in a split second is not provided.
[58]	Message authentication and effective network distribution are guaranteed by this approach. Secure communication is achieved through the use of identity-based signatures and pseudo-identities.	If a vehicle is involved in a dispute, it does not offer conditional privacy.
[59]	To provide network members with privacy and authentication, this approach is based on blind signatures and hierarchical pseudonyms.	The topic of message signature verification by an RSU on received vehicles is not covered.
[60]	This is a distributed authentication mechanism that maintains privacy through the use of bilinear pairing for message aggregation and authentication.	Every time an automobile changes networks, it must undergo a new identification process.

4.6. Schemes based on Group Signature and Ring Signature (GSRS)

The group signature and ring signature-based methods are the foundation of this category. Typically, the group is made up of members and a manager. Every member of the group has their own private key in addition to their public key. There are four main algorithms in the group signature set: KeyGen, Sign, Verify, and Find. The algorithms Key-Gen, Sign, and Verify create public and private key pairs, sign the message, validate the message-signature pair, and locate the malicious vehicle. Unlinkability is the inability of an adversary to use the genuine identity of the vehicle to link two signatures generated by the same vehicle. GSRS-based techniques are summarized in Table 7.

Table 7: Ring signature-based and group signature-based methods

Scheme	Advantages and properties	Limitations
[61]	This identity-based group signature is used in an efficient signature verification system that has been presented. For effective verification, it uses the batch-scheduling technique.	It lacks the network's computation and communication overhead.
[62]	This is a safe, privacy-preserving authentication system that mainly targets location-based services in order to deliver value-added applications.	In order to demonstrate its superiority over current systems, it does not offer any comparative findings.
[63]	To increase geographic privacy in VNs, this is an accumulative pseudonym exchange system. By using the group signature, the pseudonyms are employed.	The complicated operations involved result in somewhat substantial processing and communication overheads.
[64]	This approach lessens the load of group certificate production for OBUs from TA by using a threshold anonymous authentication based on group signatures.	Since there are always moving vehicles in the network, it is challenging to build and maintain the group.
[65]	This is a secure key distribution and authentication system that uses group signatures to shift the computing load from TA to RSUs.	There is no explanation for the selection process for the L-RSU and M-RSU.

4.7 Schemes based on Blockchain

Frameworks for identity revocation and authentication based on blockchain are essential to this category. Vehicles that are kept on the blockchain are given a pseudoidentity or certificate by the CA authority. The receiver is also given access to the entry pointer information for verification. The two main benefits of using blockchain are transparency and decentralization. The data that is added to the blockchain cannot be changed once it is saved there; it is considered immutable. Furthermore, there is no burdensome CRL distribution or management for CA. A summary of authentication mechanisms based on blockchain is provided in Table 8.

Table 8: Schemes based on Blockchain

Scheme	Advantages and properties	Limitations
[66]	In order to extend a traditional blockchain using historical Merkle trees and Merkle Patricia trees, this blockchain-based privacy-preserving authentication method	The computation and communication costs increase due to the inclusion of CA in addition to LEA.
[67]	This is a public key, certificate-less blockchain signing system that makes use of bilinear pairing. To achieve transparency in the revocation of pseudo-identities, it makes use of blockchain.	Because of the batch signature verification and aggregation, there is a significant level of complexity.
[68]	This blockchain-based system verifies trust and validates traffic events. Rather than	For PoE and PoW, which take longer to complete, each member must

	taking a proof-of-work method, it suggests a proof-of-event consensus notion.	validate the transactions.
[69]	Smart contracts are used in this method to distribute data coins to the vehicles taking part in data contribution. Over the data sharing messages, it generates signatures using the elliptic curve.	In addition to blockchain, bilinear pairing contributes to an increase in complexity.
[70]	This is a blockchain-based secure authentication and key management system that uses edge computing to make sure that all network users have access to enough storage and processing capacity.	The process of creating and validating signatures is expensive.

5. Discussions

Different cryptographic mechanisms are used to authenticate messages and protect the identity privacy of vehicles. Each mechanism has advantages and disadvantages that vary based on the needs of network administrators and members. The following is a discussion of the VNs' current protocols:

- Schemes based on symmetric key cryptography provide reduced computational overhead and communication expenses. However, security and privacy may be jeopardized if identical keys or Message Authentication Codes (MACs) are used for both signature generation and verification. In order to obtain a group key, cars register with a Trusted Authority (TA), who then uses the vehicle's fingerprint to validate it. While maintaining message integrity, identity privacy is preserved through the use of anonymous authentication and key distribution. By removing the need for a Certificate Revocation List (CRL), Hash-based Message Authentication Code (HMAC) for message signing and authentication improves network performance.
- Every participant in a public key cryptography scheme possesses a public-private key pair and a certificate that has been issued by a Certification Authority (CA) following the verification of information obtained from vehicles and Roadside Units (RSUs). By utilizing separate keys for signing and verification, these systems improve security and performance. However, scalability is impacted by certificate distribution and revocation concerns, and CRL administration raises communication expenses.
- Identity-based cryptography (IBC) systems do away with certificate administration by using personal data to generate public keys. For source anonymity, non-repudiation, and message authentication, keys are managed by the Key Generation Center (KGC) or TA. However, by examining public keys and message-signature pairs, an attacker may be able to determine the sender's identity.
- Messages carrying certificates are not transmitted in certificateless signature methods, which rely on other cryptographic techniques to perform signature operations. Computational costs rise as a result. In order to protect privacy, pseudo-identities are used for authentication in pseudo-identity-based schemes. However, in order to identify hostile cars, numerous pseudo-identities must be stored in the vehicle and a link between the pseudo-identity and real identity must be maintained.
- Vehicles establish groups and communicate using pairs of public and private keys in group and ring signature-based protocols. While ring signatures guarantee complete anonymity, they can also result in hostile users with verified identities sending fake communications, which means that changes are needed to prevent non-repudiation.
- Blockchain-based authentication systems prohibit data tampering or deletion and offer transparency and immutability. On the other hand, cartel formation could result from depending on reliable sources for blockchain updates. Blockchain techniques also need to change in order to accommodate the dynamic nature of VNs and control the size of the blockchain.

6. Conclusion and future directions

Through the dissemination of educational information, VNs seek to improve driver safety and guarantee safe traffic conditions. The privacy of car owners is

jeopardized, though, because of the open wireless medium's vulnerability to security breaches. In this study, several privacy-preserving and authentication strategies as well as cutting-edge methods for VANETs are surveyed. It demonstrates how different cryptographic algorithms are required to suit the various security objectives of virtual networks (VNs). Certain parts of current systems are inadequate for security, and in certain instances, they do not offer complete privacy. The system's main drawbacks are its high memory requirements for revocation lists and certificates, conditional privacy clauses, dependency on centralized entities, and efficiency in computation and communication. Research on complete security and robustness against attacks is still in progress. Complementary approaches, such machine learning, are required as cryptographic techniques alone are insufficient. Innovations like as 5G and the Internet of Vehicles will bring new privacy and security problems that will force current processes to change and adapt.

Innovative cryptographic algorithms combined with machine learning for behavior analysis and anomaly detection will be the future of authentication and privacy-preserving strategies for virtual networks. Scalability, effectiveness, and resilience against a variety of cyberthreats are aspects that solutions must address. To minimize communication overhead and minimize single points of failure, a focus on decentralized techniques is necessary. For secure data management, it will also be essential to adjust to new technologies like 5G and use blockchain. Updating privacy guarantees without sacrificing system speed should be the main goal of ongoing research to make sure VNs can handle changing security requirements in dynamic automotive contexts.

Refrences

[1] J. Zhang, Trust management for VANETs: challenges, desired properties and future directions, Int. J. Distrib. Syst. Technol. (IJDST) 3 (1) (2012) 48–62.

[2] I. Ali, M. Faisal, S. Abbas, A survey on lightweight authentication schemes in vertical handoff, Int. J. Coop. Inf. Syst. 26 (01) (2017) 1630001.

[3] H. Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, A. Ksentini, Named data networking in vehicular ad hoc networks: State-of-the-art and challenges, IEEE Commun. Surv. Tutor. 22 (1) (2020) 320–351.

[4] F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV, Ad Hoc Netw. 61 (2017) 33–50.

[5] Q. Xu, T. Mak, J. Ko, R. Sengupta, Vehicle-to-vehicle safety messaging in DSRC, in: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, ACM, 2004, pp. 19–28.

[6] L.N. Balico, A.A.F. Loureiro, E.F. Nakamura, R.S. Barreto, R.W. Pazzi, H.A.B.F. Oliveira, Localization prediction in vehicular ad hoc networks, IEEE Commun. Surv. Tutor. 20 (4) (2018) 2784–2803.

[7] M. Azees, P. Vijayakumar, L.J. Deborah, Comprehensive survey on security services in vehicular ad-hoc networks, IET Intell. Transp. Syst. 10 (6) (2016) 379–388.

[8] R. Jain, I. Kashyap, An qos aware link defined OLSR (LD-OLSR) routing protocol for MANETS, Wirel. Pers. Commun. (2019) 1–14.

[9] M. Aloqaily, B. Kantarci, H.T. Mouftah, Multiagent/multiobjective interaction game system for service provisioning in vehicular cloud, IEEE Access4 (2016) 3153–3168.

[10] S.S. Manvi, S. Tangade, A survey on authentication schemes in VANETs for secured communication, Veh. Commun. 9 (2017) 19–30.

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

[12] J. Cui, L. Wei, J. Zhang, Y. Xu, H. Zhong, An efficient message authentication scheme based on edge computing for vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 20 (5) (2018) 1621–1632.

[13] M. Aloqaily, S. Otoum, I. Al Ridhawi, Y. Jararweh, An intrusion detection system for connected vehicles in smart cities, Ad Hoc Netw. (2019).

[14] S. Otoum, B. Kantarci, H.T. Mouftah, Detection of known and unknown intrusive sensor behavior in critical applications, IEEE Sensors Lett. 1 (5) (2017) 1–4.

[15] J. Petit, F. Schaub, M. Feiri, F. Kargl, Pseudonym schemes in vehicular networks: A survey, IEEE Commun. Surv. Tutor. 17 (1) (2014) 228–255.

[16] F. Qu, Z. Wu, F.-Y. Wang, W. Cho, A security and privacy review of VANETs, IEEE Trans. Intell. Transp. Syst. 16 (6) (2015) 2985–2996.

[17] A. Boualouache, S.-M. Senouci, S. Moussaoui, A survey on pseudonym changing strategies for vehicular ad-hoc networks, IEEE Commun. Surv. Tutor. 20 (1) (2017) 770–790.

[18] Z. Lu, G. Qu, Z. Liu, A survey on recent advances in vehicular network security, trust, and privacy, IEEE Trans. Intell. Transp. Syst. 20 (2) (2018) 760–776.

[19] I. Ali, A. Hassan, F. Li, Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey, Veh. Commun. 16 (2019) 45–61.

[20] D. Manivannan, S.S. Moni, S. Zeadally, Secure authentication and privacy preserving techniques in Vehicular Ad-hoc NETworks (VANETs), Veh. Commun. 25 (2020).

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

[22] S. Al-Sultan, M.M. Al-Doori, A.H. Al-Bayatti, H. Zedan, A comprehensive survey on vehicular ad hoc network, J. Netw. Comput. Appl. 37 (2014) 380–392.

[23] A. Dhamgaye, N. Chavhan, Survey on Security Challenges in VANET 1, Citeseer, 2013.

[24] H. Talat, T. Nomani, M. Mohsin, S. Sattar, A survey on location privacy techniques deployed in vehicular networks, in: 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), IEEE, 2019, pp. 604–613.

[25] M.A. Hossain, R.M. Noor, K.A. Yau, S.R. Azzuhri, M.R. Z'aba, I. Ahmedy, Comprehensive survey of machine learning approaches in cognitive radio-based vehicular ad hoc networks, IEEE Access 8 (2020) 78054–78108.

[26] A. Boualouache, S.-M. Senouci, S. Moussaoui, A survey on pseudonym changing strategies for vehicular ad-hoc networks, IEEE Commun. Surv. Tutor. 20 (1) (2017) 770–790.

[27] M. Bayat, M. Barmshoory, M. Rahimi, M.R. Aref, A secure authentication scheme for VANETs with batch verification, Wirel. Netw. 21 (5) (2015) 1733–1743.

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

[29] I. Al Ridhawi, M. Aloqaily, Y. Kotb, Y. Jararweh, T. Baker, A profitable and energy-efficient cooperative fog solution for IoT services, IEEE Trans. Ind. Inf. (2019).

[30] S. Otoum, B. Kantarci, H.T. Mouftah, On the feasibility of deep learning in sensor network intrusion detection, IEEE Netw. Lett. 1 (2) (2019) 68–71.

[31] A. Ullah, X. Yao, S. Shaheen, H. Ning, Advances in position based routing towards ITS enabled FoG-oriented VANET–A survey, IEEE Trans. Intell. Transp. Syst. 21 (2) (2019) 828–840.

[32] O.S. Al-Heety, Z. Zakaria, M. Ismail, M.M. Shakir, S. Alani, H. Alsariera, A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET, IEEE Access 8 (2020) 91028–91047.

[33] P. Vijayakumar, M. Azees, A. Kannan, L.J. Deborah, Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (2015) 1015–1028.

[34] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, B. Balamurugan, Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks, Cluster Comput. 20 (2017).

[35] F. Wang, Y. Xu, H. Zhang, Y. Zhang, L. Zhu, 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET, IEEE Trans. Veh. Technol. 65 (2) (2015) 896–911.

[36] S. Jiang, X. Zhu, L. Wang, An efficient anonymous batch authentication scheme based on HMAC for VANETs, IEEE Trans. Intell. Transp. Syst. 17 (8) (2016) 2193–2204.

[37] Y. Liu, L. Wang, H.-H. Chen, Message authentication using proxy vehicles in vehicular ad hoc networks, IEEE Trans. Veh. Technol. 64 (8) (2014) 3697–3710.

[38] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, B. Qin, Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response, IEEE Trans. Comput. 65 (8) (2015) 2562–2574.

[39] P. Vijayakumar, M. Azees, L.J. Deborah, CPAV: Computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks, in: 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, IEEE, 2015, pp. 62–67.

[40] M. Azees, P. Vijayakumar, L.J. Deboarh, EAAP: Efficient anonymous authentication with

conditional privacy-preserving scheme for vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 18 (9) (2017) 2467–2476.

[41] S. Wang, N. Yao, LIAP: A local identity-based anonymous message authentication protocol in VANETs, Comput. Commun. 112 (2017) 154–164.

[42] A. Alrawais, A. Alhothaily, B. Mei, T. Song, X. Cheng, An efficient revocation scheme for vehicular ad-hoc networks, Procedia Comput. Sci. 129 (2018) 312–318.

[43] M.A. Simplicio, E.L. Cominetti, H.K. Patil, J.E. Ricardini, L.T.D. Ferraz, M.V.M. Silva, Privacy-preserving certificate linkage/revocation in VANETs without linkage authorities, IEEE Trans. Intell. Transp. Syst. (2020) 1–11.

[44] J. Sun, C. Zhang, Y. Zhang, Y. Fang, An identity-based security system for user privacy in vehicular ad hoc networks, IEEE Trans. Parallel Distrib. Syst. 21 (9) (2010) 1227–1239.

[45] H. Lu, J. Li, M. Guizani, A novel ID-based authentication framework with adaptive privacy preservation for VANETs, in: 2012 Computing, Communications and Applications Conference, IEEE, 2012, pp. 345–350.

[46] N.-W. Lo, J.-L. Tsai, An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings, IEEE Trans. Intell. Transp. Syst. 17 (5) (2016) 1319–1328.

[47] L. Zhang, OTIBAAGKA: a new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks, IEEE Trans. Inf. Forensics Secur. 12 (12) (2017) 2998–3010.

[48] A. Karati, S.H. Islam, G. Biswas, M.Z.A. Bhuiyan, P. Vijayakumar, M. Karuppiah, Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments, IEEE Internet Things J. 5 (4) (2017) 2904–2914.

[49] J. Cui, J. Zhang, H. Zhong, Y. Xu, SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter, IEEE Trans. Veh. Technol. 66 (11) (2017) 10283–10295.

[50] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, M.K. Khan, Enhancing security and privacy for identity-based batch verification scheme in VANETs, IEEE Trans. Veh. Technol. 66 (4) (2017) 3235–3248.

[51] K.-H. Yeh, K.-Y. Tsai, C.-Y. Fan, An efficient certificateless signature scheme without bilinear pairings, Multimedia Tools Appl. 74 (16) (2015) 6519–6530.

[52] J.-L. Tsai, A new efficient certificateless short signature scheme using bilinear pairings, IEEE Syst. J. 11 (4) (2015) 2395–2402.

[53] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, M.K. Khan, An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks, Inform. Sci. 317 (2015) 48–66.

[54] X. Yang, C. Chen, T. Ma, Y. Li, C. Wang, An improved certificateless aggregate signature scheme for vehicular ad-hoc networks, in: 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), IEEE, 2018, pp. 2334–2338.

[55] H. Zhong, S. Han, J. Cui, J. Zhang, Y. Xu, Privacy-preserving authentication scheme with full aggregation in VANET, Inform. Sci. 476 (2019) 211–221.

[56] Y. Sun, R. Lu, X. Lin, X. Shen, J. Su, An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications, IEEE Trans. Veh. Technol. 59 (7) (2010) 3589–3603.

[57] D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, IEEE Trans. Inf. Forensics Secur. 10 (12) (2015) 2681–2691.

[58] Q. Kang, X. Liu, Y. Yao, Z. Wang, Y. Li, Efficient authentication and access control of message dissemination over vehicular ad hoc network, Neurocomputing 181 (2016) 132–138.

[59] E.R. Agustina, A.R. Hakim, Secure VANET protocol using hierarchical pseudonyms with blind signature, in: 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), IEEE, 2017, pp. 1–4.

[60] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, C. Hu, Distributed aggregate privacy-preserving authentication in VANETs, IEEE Trans. Intell. Transp. Syst. 18 (3) (2017) 516–526.

[61] M.S.I. Mamun, A. Miyaji, An optimized signature verification system for vehicle ad hoc network, in: 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, IEEE, 2012, pp. 1–8.

[62] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, B. Liu, Practical secure and privacy-preserving scheme

for value-added applications in VANETs, Comput. Commun. 71 (2015) 50–60.

[63] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, S. Gjessing, MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks, IEEE Trans. Dependable Secure Comput. 13 (1) (2015) 93–105.

[64] J. Shao, X. Lin, R. Lu, C. Zuo, A threshold anonymous authentication protocol for VANETs, IEEE Trans. Veh. Technol. 65 (3) (2015) 1711–1720.

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

[66] Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, A blockchain-based privacy preserving authentication scheme for vanets, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 27 (12) (2019) 2792–2801.

[67] I. Ali, M. Gervais, E. Ahene, F. Li, A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs, J. Syst. Archit. 99 (2019) 101636.

[68] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, C.-C. Liu, Blockchain-based traffic event validation and trust verification for VANETs, IEEE Access 7 (2019) 30868–30877.

[69] X. Zhang, X. Chen, Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network, IEEE Access 7 (2019) 58241–58254.

[70] H. Tan, I. Chung, Secure authentication and key management with blockchain in VANETs, IEEE Access (2019).