Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 9878739, 1 page
https://doi.org/10.1155/2023/9878739

Retraction

Retracted: A Survey on Location Privacy Attacks and Prevention Deployed with IoT in Vehicular Networks

Wireless Communications and Mobile Computing

Received 12 December 2023; Accepted 12 December 2023; Published 13 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] N. Ahmed, Z. Deng, I. Memon, F. Hassan, K. H. Mohammadani, and R. Iqbal, "A Survey on Location Privacy Attacks and Prevention Deployed with IoT in Vehicular Networks," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 6503299, 15 pages, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6503299, 15 pages
https://doi.org/10.1155/2022/6503299

Review Article

A Survey on Location Privacy Attacks and Prevention Deployed with IoT in Vehicular Networks

Nadeem Ahmed,[1] **Zhongliang Deng**,[1] **Imran Memon**,[2] **Fayaz Hassan**,[1] **Khalid H. Mohammadani**,[1] **and Rizwan Iqbal**[3]

[1] *School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *Department of Computer Science, Bahria University, Karachi Campus, Karachi, Sindh, Pakistan*
[3] *Department of Computer Engineering, Bahria University, Karachi Campus, Karachi, Pakistan*

Correspondence should be addressed to Nadeem Ahmed; nadeempitafi@yahoo.com

Received 16 December 2021; Accepted 2 April 2022; Published 26 April 2022

Academic Editor: Ali Kashif Bashir

Vehicular ad hoc networks (VANETs) connect two or more vehicles wirelessly to enable data exchange in an Internet of Things (IoT) environment. In VANETs, location privacy is the most crucial piece of information, and its protection is the top priority. However, the location privacy threats have not been adequately addressed in positioning for IoT in VANETs. This paper provides an overview of location privacy attacks and their solutions to address the problems caused by attacks in any IoT environment. Secondly, we have analyzed specific solutions based on anonymity (pseudonym) and cryptographic solutions using a digital signature technique. This enables to improve user privacy and security of location-based services for IoT in VANET. Moreover, we have proposed a faster 5G solution for the VANETs as it rapidly disseminates the data in fast-moving vehicles.

1. Introduction

VANET helps to ensure traffic safety through improved traffic flow and significantly reduces car accidents within the IoT environment [1–3]. VANET provides many valuable tools and advantages for VANET clients and requires implementation operations. Due to the personal transport trend, the number of vehicles has increased in the last few years. This has resulted in high density and over speeding of vehicles causing a significant rise in road accidents [4, 5].

VANET technology is aimed at equipping vehicle technology to reduce these factors by transmitting informative messages to each other [6–8]. Significant traffic problems like road accidents and congestion require new and more efficient transport systems [3, 9]. The Intelligent Transport System (ITS) for the IoT environment tackles critical issues such as the safety of the public and road congestion. It combines information and communication technology into the transport and vehicle infrastructure. VANET includes different communication modes: vehicle to vehicle (V2V), infrastructure to vehicle (I2V), and the hybrid mode. In V2V, the connectivity media used are short-delayed and have a higher transmitting rate. This network infrastructure is used in various broadcast warning situations (emergency, reduced speed, crash, and slowing down the vehicle's speed) [10]. In I2V, the vehicle network considers the application of road-side unit (RSU) infrastructure points that multiply services in communication through Internet portals. Hybrid mode is the amalgamation of V2V and I2V techniques [11, 12].

VANET is intended to raise public awareness by broadcasting and aggregating current information on current or imminent transportation-related occurrences. The nodes of VANET are mostly segregated into two types: the first is an on-board unit (OBU), a radio device is mounted in automobile, and the other is road-side unit (RSU), therefore to ensure the protection of all passengers of vehicles and riders. Although ad hoc often connects vehicles in the network topology in VANETs, it can be inadequate and ineffective to extend existing communication methods intended for traditional mobile ad hoc networks directly to massive VANETs with quick-moving vehicles [13].

The entire communication in VANETs is open access, which makes VANETs more prone to attacks. The attacker can intercept, alter, insert, and delete vehicular ad hoc network messages [14–16].

The intruder can control the traffic messages used to direct the road vehicles. The attacker can alter these messages and spread false road information causing traffic congestion and road hazards.

Many researchers have addressed the security and privacy issues associated with VANET. There is already much literature on addressing privacy issues in various aspects of vehicular communication. To the best of our knowledge and based on searches in different well-known databases, we have found that just a few attacks on VANETs have been discussed to date. This research has covered almost all attacks that severely affect privacy and security. Table 1 shows the types of attacks, security service breached, and its countermeasures. The main contribution of this paper is that the security countermeasures are defined by different problem-solving methods. Table 2 shows the Abbreviations used in the paper.

Figure 1 shows the overall VANET structure. We can see all entities involved in the connectivity of VANET nodes. Below are the entities of the VANETs with some details of their working principles.

1.1. Entities of VANET. Road-side units (RSUs). The RSUs are installed in the VANET: RSUs are positioned along the road and serve as radios for DSRC communications. The main functions of RSUs are as follows: (i) to expand the communication range of VANETs by transferring messages to other OBUs and RSUs, (ii) enable running protection applications, such as reporting traffic conditions or accident warnings, and (iii) provide OBUs with Internet access [3, 17].

On-board unit (OBU). In the automobile, OBUs are installed, which are radio devices that will constantly be in moving conditions, although OBUs link the vehicles with RSUs. For an intrinsic part of VANET and effective communication, nodes require such functionalities to help them receive information, notify their neighbors, and make decisions by analyzing all their collected data.

Trusted authority (TA). This is accountable for the confidence and safety management of all VANETs, including the authenticity verification of vehicles and the removal of nodes for vehicles that convey false messages or malicious behavior [18]. The TA, therefore, requires high computing capabilities and adequate storage space [19].

Radar. Radar is used on different moveable objects, including vehicles, to detect the direction, speed, and distance.

Computing platform. A computing platform for the VANETs is required for the drivers to see the data received during driving, like the details of the VANET environment, i.e., position, distance of the vehicle, and the hazard information, and it is a digital platform on which any software or app can be executed.

Event data recorder. The event data recorder is an intelligent part of the VANET; it can be said that it is the "black box" of the vehicle. Any unusual event in the vehicle is recorded so that the issue can be appropriately addressed, and the transport authorities will identify the reason.

1.2. Communication Patterns with IoT Environment in VANETs. Dedicated short-range communications. Its normal transmission range is between 300 m and 1,000 meters. The DSRC system has a maximum speed of 200 km/h and a 6 to 27 megabits per second (Mbps) data rate range. DSRC operates in the 5.9 GHz frequency range. It is a short- to medium-range communication technology that can be used for public safety and private purposes. The IEEE standard for vehicular networks is IEEE 802.11p WAVE (Wireless Access in Vehicular Environments). Some of the applications for which DSRC is deployed in VANET include emergency vehicle warning systems, Cooperative Forward Collision Warning, transit or emergency vehicle signal priority, and an approaching emergency vehicle warning.

Vehicle-to-vehicle (V2V) communication. V2V communication is established between vehicles as an ad hoc network. Vehicles can transmit or share helpful information in V2V, such as traffic conditions, i.e., traffic jams and accidents [20–22].

Vehicle to infrastructure (V2I). V2I communication is used to disseminate information between the network infrastructure and vehicles [12]. In V2I, a vehicle can connect to RSUs to provide and communicate with the Internet.

Figure 2 shows the internal and external components of a smart car; the components are required to connect the vehicle smartly with VANETs to exchange the information between the drivers. Smart cars are enabled with features, which include Global Positioning System (GPS), omnidirectional antennas, sensors, alarms, camera, on-board processors, and event data recorder (EDR) [23].

This paper is categorized into six sections; a graphical paper organization is shown in Figure 3.

1.3. Importance of Location Information. From the privacy point of view, location information is the most crucial part for a vehicle and its driver. Since VANET gathers the location information, this information must remain confidential; otherwise, the attackers can quickly gain access to the driver and attack the driver's privacy, and attackers can promptly attack the VANET to disturb the efficiency of the network. Different types of attacks target the other areas of a VANET. However, attacks on confidentiality are hazardous for the privacy of location information. In a secured VANET, the data must be exchanged securely for smooth operation, and messages should be transferred between the authorized parties. However, if the attackers' targets against attacks like eavesdropping, then the data of VANET can be compromised, and the attacker can easily access the location information.

Table 1: Classification of attacks and goals achieved after implementation of different algorithms.

Reference	Type of attack	Security service	Goals and targets achieved by implementation of algorithms
[58]	Eavesdropping	Availability	Solving attack problems by asymmetric cryptography technique To improve the wireless security, enhance the efficiency
[80]	Multiple types	Availability	The framework can reduce the cost and gain outperformed results.
[81]	Jamming	Availability	Blowfish cryptosystem is used for encryption and decryption to make secure routes in MANET.
[51]	Malware	Availability	To protect location privacy and improve the quality of service in the network
[82]	Greedy behavior attack	Target availability	To improve the GSM security via CL-PKC while the handshaking procedure is being done
[70]	Blackhole	Availability	To improve the MANET security using fixed slot length, the attacker cannot continue the attack on the network.
[83]	Multiple	Availability	Present multiple challenges and solutions for preventing IoT overcloud.
[4]	Multiple	Confidentiality	Use encryption technique. Use VIPER technique for V2I communications.
[23]	Sybil attack and DoS	Confidentiality	Present multiple solutions to prevent an attack on smartphones.
[84]	Sybil attack	Confidentiality	Use a distributed and robust approach
[85]	Impersonation attack	Authentication	Make use of SPECS (secure and privacy enhancing communication schemes). Make use digital certificates.
[28]	Spoofing attack	Authentication	Present some open challenges in hybrid network of cloud and 5G.
[52]	Repudiation attack	Nonrepudiation	Make use of digital signatures. Use PKC-based pseudoidentities.
[71]	Sybil attack and DoS	Availability	By the use of signature-based authentication and bit commitment, the impact of DoS attack is reduced.
[72]	Sybil attack	Authentication availability	A central authority for validation (VA) deployment validates the network's components in real time. The working principle of validation will be direct and indirect. By cryptographic technique, nodes that want to establish a direct link authenticate VA indirect validation. VA can use temporary certificates. By using the validation technology, VA is a protected option for attacks.
[86]	Jamming	Availability	Change the transmission channel and use FHSS frequency hop technology to produce pseudorandom hopping numbers for the algorithm by using cryptographic algorithms. This strategy needs improvement to the existing OFDM standard.
[87]	Certificate and or key replication	Authentication and confidentiality	For certificate and key replication, cross-certification among the various VANET certification authorities CRL (revocation certificate) real-time validity test for digital certificates Use validated and certified disposable keys.
[88]	Greedy Malware Wormhole Tunneling Blackhole Spamming	Availability Nonrepudiation Authentication Confidentiality Integrity	The cryptographic technique does not provide practical solutions for these attacks, but specific recommended methods can minimize adverse effects such as digital software signatures.

2. Location Privacy Challenges in VANET

Attacks on privacy are linked to unauthorized access to sensitive vehicle information. There is a direct relationship between the driver and vehicle. If the intruders gain unauthorized access to some data, the driver's privacy will be compromised [24–26]. In most cases, the car owner is also its driver; if an attacker obtains the owner's identity, the vehicle's privacy may be risked; this form of privacy assault is known as identity disclosing. One of the most well-known privacy threats is known as location tracking. In this attack, the vehicle's position or the path taken by the car at a specific point in time is considered personal data.

VANETs are dynamically complex ad hoc networks with limited network latency and multiple facilities. The communication modes are categorized as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and hybrid, as shown in Figure 4. Hybrid mode is a merger of the former two approaches, already discussed earlier.

Table 2: Abbreviations used in the paper.

Abbreviation	Definition
ABAKA	Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks
CRL	Certificate revocation list
DDoS	Distributed denial of service
DoS	Denial of service
EDR	Event data recorder
GPS	Global Positioning System
I2V	Infrastructure to vehicle
IoT	Internet of Things
ITS	Intelligent Transport System
OBU	On-board unit
OTP	One-time password
PKC	Public key cryptography
PKI	Public key infrastructure
RSU	Road-side unit
SNR	Signal-to-noise ratio
TA	Trusted authority
V2V	Vehicle to vehicle
VANET	Vehicular ad hoc network
5G	5th generation network

In VANETs, protection must ensure that communication messages exchanged are not intercepted or manipulated by assailants. Furthermore, the drivers' responsibility is to accurately notify the traffic situation under a time limit [4, 27]. The security threats occur due to the unique characteristics of VANETs. The exploitation of these security issues leads to other restrictions.

Here are a few of the security challenges:

2.1. Characteristics of VANETs

(i) Network topology and communication mode

(a) *Unbounded and Scalable Networks*. For one or more towns and nations, VANETs can be implemented. It needs coordination and management of security requirements.

(b) *Wireless Communication*. The connection of nodes and their data exchange is made through wireless channels. There is a need to establish communication.

(c) *High Mobility and Rapidly Changing Network Topology*. Nodes travel at fast and unpredictable speeds that make it harder to determine their location and the network's topology.

(d) In data security, the privacy of the node causes repeated disconnections, instability, and inability of the handshake. Its failure is a reasonably long-term situation (for example, a password) and is inefficient to secure vehicle communication. Under these conditions, the delay in disseminating warnings should be acknowledged. Quick cryptographic algorithms or entity authentication and timely message delivery require good delay performance. For all this, prioritizing data packets and preventing congestion should prioritize traffic safety [28] and productivity data more quickly than others. Real-time and multimedia technologies are proposed compared to the efficiency and cross-layer across transport and network layers [29, 30]

(ii) Automobiles and driver mode in IoT environment

(a) *Heavy Processing Power and Optimal Energy*. VANET nodes have no energy and computing resource problem. The vehicles are equipped with their battery and fast computational capabilities to perform complex cryptographic calculations.

(b) *Improved Physical Safety*. In VANETs, nodes are physically strengthened. It is tougher to compromise physically and can minimize the impact of infrastructure attacks.

(c) *Recognized Moments and Positions*. Utmost vehicles are packed with GPS because many applications depend on location and area. A leak-proof GPS is often used to protect the position of nodes against attackers in protected localization.

(d) *Most Members Are Trustworthy*. Most motorists are considered successful and helpful in locating a challenger.

(e) *Existing Law Enforcement Infrastructure*. They capture the adversary who attacked the device through law enforcement officers.

(f) *Interior Registration with Routine Inspection and Maintenance*. Automobiles are listed on the central registration authority and have a specific ID (licensing plate). Periodical updating of vehicles is for software and hardware upgrades. In the PKC (public key cryptography), maintenance is undertaken to update the certificate credentials and to acquire a renewed CRL (certificate revocation list). In short, the network of vehicles (VANETs) is an interface between drivers' actions, networks, and infrastructure cooperation. Proving a security solution must find a way to include both groups.

(g) In VANETs, safety must ensure that messages transferred are not manipulated or altered by the adversaries

2.2. VANET Security Challenges. VANETs have recently introduced a new safety concern, deemed a significant

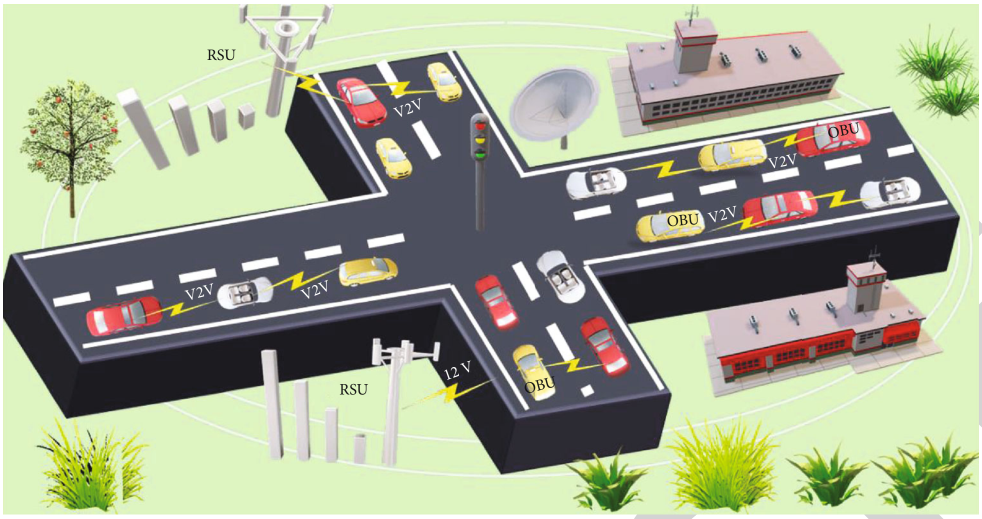

Figure 1: The illustrative architecture of VANET.

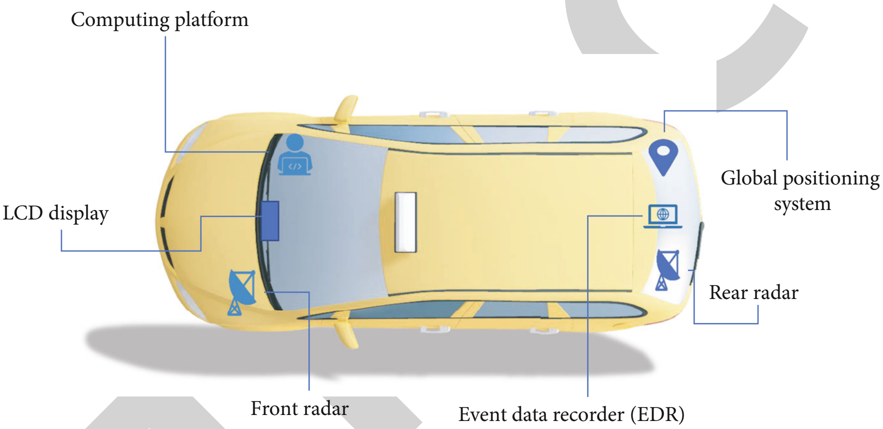

Figure 2: VANET enabled smart car [2].

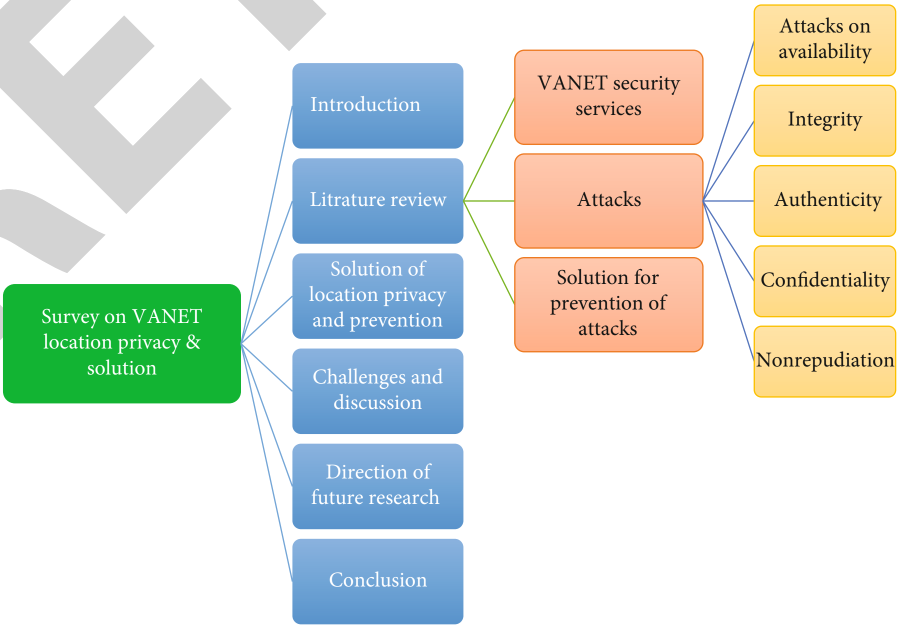
Survey on VANET location privacy & solution
Introduction
Litrature review
Solution of location privacy and prevention
Challenges and discussion
Direction of future research
Conclusion
VANET security services
Attacks
Solution for prevention of attacks
Attacks on availability
Integrity
Authenticity
Confidentiality
Nonrepudiation

Figure 3: Organization of the survey paper.

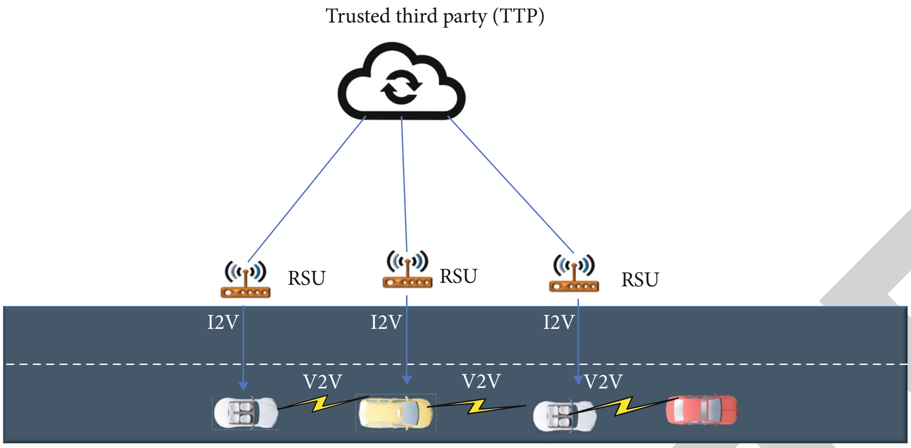

Figure 4: V2X connectivity through VANET architecture.

problem for researchers to tackle safety purposes, including a small number of major central points, mobility, inadequate wireless communication, and the issue of drivers. VANET protection ensures that the messages sent are not inserted or amended by the attackers. In addition, the motorist is accountable for providing detailed information on traffic conditions within a specific time frame. Due to their distinctive features, VANETs are more susceptible to attack. Several restrictions are created for securing VANET communications [23, 31].

(iii) Some more challenges are given below

(a) Volatility

VANET lacks the relatively long-lived context but contacting user devices to hot-spot demands a lifetime secret code. An attribute like this is unrealistic for secure intercommunication [32].

(b) Low tolerance for error

As VANETs deal with human life, there is an extremely low tolerance for error. If there is any delay in information dissemination due to attacks like DoS and DDoS [33–35], it can be harmful.

(c) High mobility and network scalability

Because of high mobility and network scalability, the network should work at its optimal level; if attackers target the VANETS, this can be disastrous for human life.

2.3. Encryption of User Information. Concern, the introduction of VANET privacy is one of the biggest challenges. Nonetheless, most drivers want to protect their data and do not want to share their confidential details [36, 37]. Personal information such as driver identification, driving behavior, the vehicle's history, and the present location is given. The critical problem is how do we build a program that respects users' privacy while concurrently defending them against malicious nodes. To avoid circumstances in which each movement can be traced, the program must guarantee users' privacy. Therefore, the users' privacy in the correspondence exchanged must be guaranteed, thus maintaining the trustworthy VANET-based framework [38].

Besides, information can be received by any network node as it is transmitted through wireless broadcasts. The information is subject to confidentiality (vehicle location, time, original ID, speed, and time) and car sensor data internally [39, 40]. It is easier to monitor the online identity of malicious people such as terrorists and lawbreakers.

VANET privacy attacks specifically relate to the unlawful collection of confidential vehicle information. Given the relationship between a vehicle and its driver, it could affect the driver's privacy by obtaining some data on the conditions of a vehicle. Then, such attacks can lead to identity disclosure. The identity of the owner of a particular vehicle may jeopardize its privacy. Typically, the car owner is also the driver, making it easier to collect personal data. The location or route of a vehicle at a specific time is known as personal data. It enables the creation of the profile for this vehicle and its driver [40, 41] through the transmission of middle nodes.

The recipient message verifies that the message is complete and authentic through the corresponding public key. It is difficult for a node to imitate since it is just private. The message sent in a VANET should be encrypted with safety or warning messages, particularly. Those messages that act as inputs for the protection framework may also be signed. Now, the critical advantage is that digital signature requirements are minimal, i.e., nodes need to have the capability to obtain/generate and store pairs of cryptographic keys. To build and verify signatures, they need computational capacity. The key problem is imitation and DoS (denial of service) attacks. In [42–46], the proposed method uses pseudonymous certificates that can hide users' true identities. Even though there is no known relationship between anonymous certificates and the true identities of key holders, the messages that have a given a key, by logging that message, the privacy can be violated [3, 26], group signature, and ID-based signatures [47, 48] are the conditional privacy protocol. The significant advantage of using

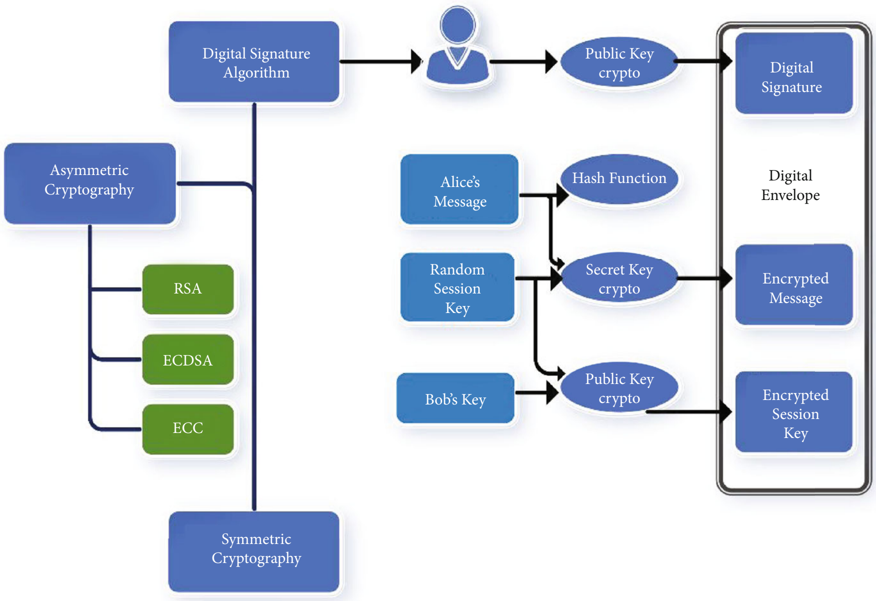

Figure 5: Digital signature algorithm.

a group signature is that they guarantee message unamiability as group members can sign incognito on behalf of the group [39, 47].

The digital signature algorithm is shown in Figure 5. Digital signatures are the public-key primitives of message authentication; this technique binds the person or entity with digital information; the receiver and the third party verify this unique binding. In the digital data exchange, the digital signature algorithm authenticates the originality of data. This technique is very efficient for the security and privacy of a VANET. Digital signatures have various advantages, i.e., message authentication, data integrity, and nonrepudiation. If the attacker hacks the system and attacks the data to modify the data integrity, the digital signature verification at the receiving end fails. Hence, the receiver can safely deny the message, assuming that the data integrity has been breached [9, 29, 40].

In [49], SeGCom (Secure Group Communications) framework introduced a simplified approach while generating and disseminating emergency messages. V2V scenario issues with only using one encryption method. Several other researchers also proposed PKI and digital signatures for VANET protection [23].

In [50], a protocol was proposed to revoke malicious vehicle certification throughout misbehaving vehicles. The biggest challenge for VANET PKI-based schemes is the heavy load of certificate creation, storage, distribution, verification, and revocation. A steady communication architecture based on a PKI and a virtual cluster-controlled network was proposed to intelligently avoid collisions caused intentionally by malicious vehicles [32]. However, this approach comes up with an incredible overhead and a cluster head building bottlenecks. In [49, 51], an ID-based cryptosystem (for security-related applications) is proposed, which imposes strong rejection and minimizes the overheads linked to the certificate management prevailing in PKI systems. The mix zone approach in [42] has been used to maximize unrecognized vehicles. This approach is based on preloading in each vehicle group of unknown certificates. Elliptic curve cryptography is designed to reduce transmission and overhead delay. The elliptic curve logarithm problem (unsolved NP problem) is defined by ABAKA's (Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Network) privacy. One of the researchers proposed a detection algorithm to deal with the invalid request problem because of the batch verification failure [52]. The researchers arranged hierarchical identity-based cryptography for location-based signature verification to provide location assurance and pseudonym-based privacy authentication. For a location-based signature generation and location assurance verification scheme, the ID-based validated vital agreement between a vehicle and an RSU, and a hierarchical ID-based signature has been used in [53]. The above system provides unconditional privacy and eliminates the need for a group manager. A signatory can generate a signature on behalf of an ad hoc group without using the ring members' public keys. This scheme has limited functionality in VANETs because it offers absolute privacy without non-repudiation [54].

2.3.1. The High Mobility of Nodes. In the VANET, the high mobility of the nodes causes enormous complexity. Classical node and message authentication techniques are challenging due to the high level of mobility. A handshake protocol cannot be proposed since some nodes communicate only once, and a lack of time restricts the validity of messages received from these nodes. Therefore, securing mobility issues is a significant concern. Although many researchers have tackled these issues, many problems still need to be

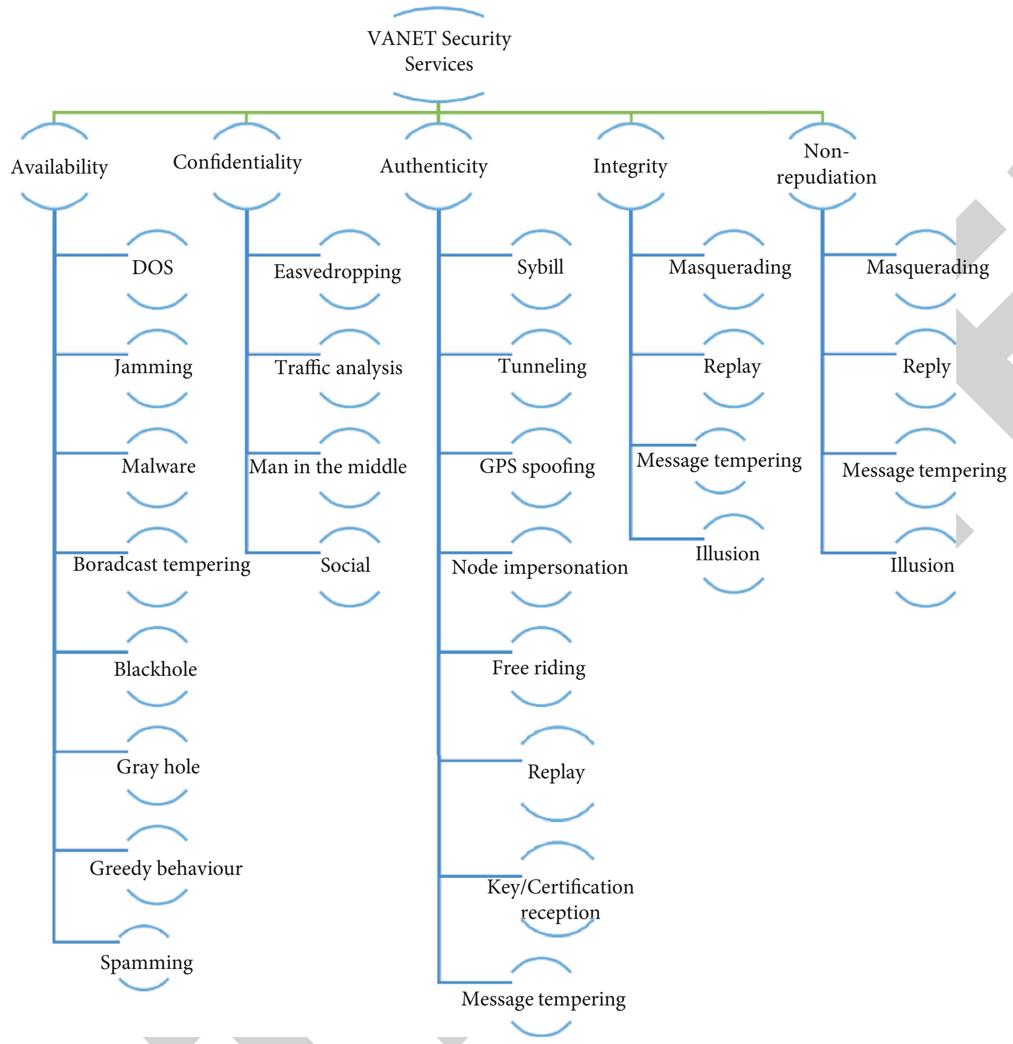

Figure 6: Attack type classified category wise.

addressed [10, 53]. This strategy does not enforce particular routes or speeds for drivers to follow [53].

Günay et al. [55] addressed several concerns of privacy, in which business organizations can use the data of their employees' cars when they are parked in the company's parking space. Police can also use the information of the driver from the beacon frames. Insurance companies can track their consumer data to evaluate their actions. Therefore, privacy violations occur when the user's confidential data is owned by third parties or by a separate node not entitled to the data [5, 56].

2.3.2. The Relationship between Security and Privacy. User hesitancy is one of the main barriers to VANET technology. Users have a negative perception, believing that a third party is monitoring them. If a hostile user changes, the message privacy can be compromised. Some potential attacks may encrypt or fake the data; hence, privacy can be breached in the VANETs.

2.3.3. Security Threats and Hazards in VANET. In this section, we address each security services' attacks and threats. There are bundles of security and privacy attacks in VANETs affecting the overall performance of a VANET. The attacker attacks on different VANET security services, i.e., availability, confidentiality, authenticity, integrity, and nonrepudiation, as shown in Figure 6.

3. Location Privacy Attack Methods and Prevention for IoT in VANET

In location privacy, attackers target the VANET to disturb the network's performance through different types of attacks. To prevent these attacks, various researchers have proposed multiple approaches. Researchers in [19] have proposed enhanced privacy using an asymmetric cryptography scheme. Moreover, pseudonym-changing strategies [57–59] effectively prevent location attacks.

3.1. Attack on Availability. Data availability (vehicle information) is essential for VANETs to ensure that the network is operational and valuable information is always accessible; this is a necessity for VANETs to ensure the safety of users' lives [60, 61]. Table 3 shows the list of some well-known

Table 3: Basic types of attacks.

Types	Descriptions	Purpose
Counterfeit information	Adversaries modify or disburse the wrong data on the network.	To interrupt other motorists for particular illegal purposes and public order [89]
Denial of service	Adversaries insert irrelevant bulk messages to VANETs. Attackers interpose irrelevant bulk messages into the network.	To interrupt the communication process and use the computing resources of other nodes, making VANET unavailable [62]
Impersonate	Attackers claim to be valid nodes such as authenticated RSUs or cars.	To include fraudulent information across the network, not only to trick other vehicles but also to eliminate the innocent drivers whose IDs were taken out of the service [90]
Eavesdropping	Adversaries are located in vehicles or false RSUs.	It is for collecting vehicle data from overhead vehicle communications.
Message suspension	Adversaries hold messages to delay for some time	To avoid the registration and insurance authorities learning about collisions involving the attacker's vehicles. Moreover, prevent collision reports from being delivered to road-side access points [71, 91].
Hardware tampering	Adversaries exploit vehicle and RSU hardware.	It is disturbing the user for unlawful purposes [1, 92].

attacks, e.g., denial of service attack (DoS) and jamming attack.

(a) *DoS (Denial of Service Attack)*. In this attack, an attacker attempts to make the network resources and facilities inaccessible to the user. It is either by active channel jamming or sleep deprivation. DoS attacks include a family of attacks to deliver network services, particularly for VANET applications. DoS attacks are listed due to their associated risks and consequences. They can occur via deceptive explicit or implicit network nodes. Control channel floods with large numbers of purposefully generated messages [25, 62]. Network nodes (RSU and OBU) cannot accommodate the massive amount of data obtained. Distributed denial of service (DDoS) is a changed variant of DoS attacks [63]. It is an attack disseminated by the primary attacker, the "attack operator" of other agents who may be victims inadvertent. In most cases, the DDoS attacks flood the unnecessary data in the network, to produce the congestion and delay in the network, and the results are invariably disastrous. DoS attacks include both blackhole attacks and jamming.

(b) *Jamming*. Jamming is a type of denial-of-service attack that prevents other nodes from using the channel to communicate since they occupy the medium on which the communication between the nodes is established. A significant threat to wireless channel access reduces the receiver's signal-to-noise ratio (SNR). The jammer would simultaneously control the value of the jamming signal [64]. The most effective signal transmission model that best combines the receiver should also be selected if efficient jamming is accomplished in a VANET. Some researchers, including [17, 65], examined some strategies to minimize the impact of jamming on ad hoc mobile networks.

(c) *Malware*. An intruder continues to send network spam messages to waste network bandwidth and increase latency. This attack is difficult to manage due to the lack of centrally controlled infrastructure and management. Intruder broadcasts unwanted messages to a user's group. These messages act like advertisements.

(d) *Broadcast Tampering Attack*. The offender is trying to render and insert fake security warnings in the network in this type of attack. The proper security messages can be withheld from legitimate users, and network security can be seriously affected [17]. This kind of assault is usually probable for a legal node.

(e) *Blackhole Attack*. A fraudulent node determines the short-lived route to receive and then routes and reroutes the data. The fraudulent node may decrypt or preserve the data packet. The forged route is built successfully relying on the malicious node sending the packet wherever it chooses.

(f) *Gray Hole Attack*. This attack only involves deleting data packets from vulnerable applications due to packet loss [66, 67]. Gray hole is known as a variant of the blackhole attack.

(g) *Greedy-Behavior Attack*. Greedy's attack is an intrusion of the function of the MAC layer in line with the OSI model architecture. The greedy node recognizes the channel access system and still wants to connect to the media. The fundamental purpose is to prevent using other nodes of support and services. A greedy action node often reduces its time to wait for quick access to the channel and penalizes other undefeated nodes [48, 68]. Transmission congestion and collision issues are caused by greedy behavior, which causes delays in the services of authorized consumers. Greedy behavior is autonomous and is shielded from the top layers, so a mechanism designed for those layers cannot detect them.

(h) *Spam*. The spam attacks are mainly used to increase latency and bandwidth usage and decrease the overall efficiency of the network and services.

3.2. Authenticity and Identification Attacks. Authenticity is a big security problem for VANETs. Before accessing the available resources, all existing network stations must authenticate. Any infringement or attack targeting the recognition or authentication process would adversely impact the entire network. Ensure legitimate nodes in a vehicle network from outside or inside attackers with a false identity. The benefit of verification of identity is that in the majority of the time, a vehicle joins the network or service. There are several types of attacks in this category [69, 70].

(a) *Sybil Attack*. The Sybil attack is hazardous because the vehicle can act as if it has multiple identities simultaneously [71, 72]. One of the main ways that two entities can convince a third that they are independent is by performing activities that cannot be performed by a single entity alone. Many techniques such as computational testing resources, memory, and communication challenges have been recommended to protect the identity of a node. The Sybil attack is risky in VANETs because of the catastrophic consequences. The attacker can manipulate the behavior of other vehicles so that the receiving node can think that the message was sent by another vehicle. As a result, they believe that there is a traffic jam on the road, and the user changes the route to clear the road.

(b) *Tunneling Attack*. The tunneling attack imitates the wormhole attack [26]. In a tunneling attack, attackers use the identical network to communicate privately (tunnel) in this attack, while in the wormhole, the attackers use a separate radio channel (assumed external) to exchange packets. This tunneling attack joins two remote parts of the vehicle network through a communication channel such as a tunnel [73]. Therefore, the victims of two remote network parts would link as their neighbors.

(c) *Position Information Deception (GPS Spoofing)*. Secreted automobiles produce fake crash locations. GPS does not work.

(d) *Node Impersonation Usurpation*. The intruder attempts to imitate an additional node. The intruder does malicious things to gain rights and then reveals that the better one is the doer.

(e) *Free Riding*. Such attacks are highly dominant and generate an active malicious user by fake authentication when connected with cooperative message authentication. A malicious person can take advantage of several other users' authentication contributions without providing their own identity to this threat. This attack could pose a serious threat to the authentication of a cooperative message [74].

(f) *Replay or Reiteration Attack*. Malicious or unauthorized drivers try to use new frames that have been built into new connections to create legitimate RSU users [93].

(g) *Key Certification/Replication*. This attack is identified as a replay attack that arises when legitimate information is transmitted false or allows an unwanted or malicious effect to be caused by delay. The VANET needs more time with a greater cache to test the messages received to overcome this attack.

(h) *Message Tampering or Alteration*. The intruder drops packets from the network or alters the message's contents. In addition to alteration attacks, a new message is produced or repeated by displaying old messages or threats to falsify or introduce mass amounts of false vehicle emergency warnings. Broadcast tampers, where the attacker infuses fake security messages into the network to cause significant problems.

3.3. Attacks on Confidentiality. Confidentiality is an essential safety requirement for VANETs, ensuring authorized parties read the data. Failure to provide confidentiality between node communication within a vehicle network means that exchanged messages are susceptible to threats. The intruder can collect information regarding the vehicle, its route, and the user's privacy in such cases. Without a confidentiality system, the data collected would affect individual privacy. It is hard to detect such an intrusion since the user is inherently passive and does not personally know the database [5, 75, 76].

(a) *Eavesdropping Attack*. Eavesdropping is a privacy attack; listening to media is a direct attack on networks like VANET. It is also submissive, and the victim does not know that the connection is compromised. Several valuable data can be easily accessible during this attack, such as the position information used to track vehicles.

(b) *Traffic Analysis Attack*. An attack on traffic inside a VANET is a significant passive threat to privacy and anonymity. The attacker investigates the data obtained after listening to the network and retrieves as much information as possible.

(c) *Man-in-the-Middle Attack (MiM)*. The communication between various vehicles is perceived by a malicious node. It tries to pretend that they are responding to each other. It transmits false knowledge between them.

(d) *Social Attack*. A social attack frequently diverts the driver's focus. The attacker sends deceptive and immoral messages to the vehicles. The attackers aim to make drivers respond to these immoral messages, thereby impacting the driving of cars and the efficiency of the VANET network [2].

3.4. Data Integrity. It guarantees that the messages' quality is not altered during the interaction process. The public key infrastructure can be assured in VANETs and cryptography revocation.

(a) *Masquerading Attack*. The attacker's legitimate identity, known as a mask, attempts to build a black hole or generate false messages from an authentic node in this attack, for example, slowing down the speed of a vehicle or lane change. A malicious node claims to be a vehicle of emergency, for example, cheating other cars [26, 77].

(b) *Replay Attack*. It is a traditional attack that involves recreating (broadcasting) a message that was already sent at the time of submission. Moreover, the intruder injects this again into the previously obtained network packets. This attack can be used to replay frames for beacons [9] so that the attacker can handle the location and the routing table of nodes. Unlike many other attacks, nonlegitimate users replay attacks [8, 78].

(c) *Alteration of Message*. This attack is against credibility by changing, deleting, restoring, and changing existing information. It can happen by altering a particular part of the message to be sent [79]. Suppose the assailant fabricates the information indicating that the road is jammed and alters it to cheat users, thereby implying that congestion is not occurring and the road traffic is regular. In such an attack, the offender can also delete part of the message change or create new messages that help him reach his malicious objective.

(d) *Illusion Attack*. The illusion attack is a direct application to fabricate messages that attack integrity and data trust. It involves voluntarily putting sensors that produce false data [1]. Such data will usually be moved around the network and require drivers' involvement. Authentication mechanisms cannot detect this attack since the attacker authenticates to the network.

3.5. Attacks on Nonrepudiation. Nonrepudiation in data security indicates that the sender and recipient are people pretending to have sent or received the message, respectively [54]. Otherwise, the failure to repudiate the data sources shows that the data has been sent, and nonrepudiation of arrival proves that the data have been obtained. In the scope of VANETs, the compromised data regarding the user's safety and anonymity, confidentiality sets, and hardware, device, and software adjustments (updates, changes, and additions) should always be provable [53].

(a) Nonrepudiation and accountability attacks

Traceability of lost events: considering its significance, no critical information dealing with this attack was found in the context of VANET. Besides, such nonrepudiation attacks allow an attacker to reject one or more actions. This type of attack focuses primarily on eradicating signs of behavior and uncertainty for the auditing group. Many attacks may be used for a preventive attack against nonrepudiation, for example, Sybil and key and certificate replication.

3.6. Solution for Location Privacy Attacks in an IoT Environment. We analyze various attacks and their solutions in Table 1.

4. Discussion

As we know, a flawless VANET can make highway traffic smoother, safer, and faster. However, the attackers can gain system access to disrupt the VANET-based drivers, thus reducing the overall performance of the VANET. Consequently, user privacy and security are the main targets of attackers. User privacy must not be compromised at any cost; otherwise, it becomes difficult to attract drivers to use VANET services. All VANET-based communication contains sensitive private information such as driver identity, personal identification number, driver number, travel time, and route details. Therefore, VANET communication information must be secured to ensure the safety of user information and vehicle information for smooth operation.

Moreover, the consequences of a security breach in VANETs are serious and threatening. In a highly demanding environment characterized by vehicles arriving and frequently departing simultaneously and a short connection time, implementing a solution to protect complete privacy is challenging. There is a great need to secure data transmission paths in VANETs, and some approaches have already been proposed to address related issues. Since the main challenges discussed here are privacy and security, the solutions to improve these problems are addressed accordingly. We have thoroughly analyzed various papers and approaches for privacy and security problems. We have found solutions to overcome privacy and DoS attacks by using signature-based authentication and bit commitment. The impact of DoS and Sybil attacks is reduced by using signature-based authentication.

For jamming attacks, many techniques are used by different researchers. Our findings show that the Blowfish cryptosystem is efficient as it is used for encryption and decryption to create safe routes in VANETs. It changes the transmission channel and uses FHSS frequency-hopping technology; it is possible to develop pseudorandom hopping numbers for the algorithm using cryptographic algorithms. On the other hand, this strategy needs to be improved, especially for the existing OFDM standard.

We found cross-certification between the different VANET certification authorities for confidentiality and authentication attacks. CRL (revocation certificate) real-time validity test is for digital certificates.

Certificate and or key replication affects the services like authentication and confidentiality; this technique protects the security in a well-organized manner. For attacks like greedy malware, wormhole, tunneling, blackhole, spamming, availability, nonrepudiation, authentication, confidentiality, and integrity, we found that cryptographic technique does not provide practical solutions for these attacks. Still, specific recommended methods can minimize adverse effects, such as using digital software signatures. Existing protocols and values can be modified by using trusted hardware, which practically cannot even be approved. We also propose an OTP (one-time password) system that should maximize the security of drivers from attackers. A simplified approach is that a policy-based method is more suitable when mobile consumers prefer the service level of complete privacy. A cryptographic technique is a practical solution for users who care deeply about privacy and require a high level of confidentiality. They are less concerned about the overhead of data processing and communications.

In addition, anonymization and obfuscation techniques and spatial and temporal information would be best for a mobile user to disguise. The infrastructure is location-based services, benefits, applications, and privacy concerns. We have primarily addressed the privacy issue of LBS and analyzed several different approaches. We classify the existing mechanisms into a tree structure to evaluate the efficiency of additional security measures and study them in detail on their benefits and limitations. We have successfully analyzed various shortcomings and gaps in privacy technology. Location protection is an essential element of LBS. To benefit from the specified services, users use current locations as information. Without the necessary precautions, the lack of privacy protection in the services could hinder the regular use of this smart technology. We have highlighted the threats posed by LBS services that intentionally or unintentionally compromise the privacy of VANET users. We have outlined their basic ideas and recent developments by examining typical techniques. In the following section, we have provided a comparison and analysis. Finally, we have identified some interesting topics for future research that should be investigated in the context of privacy protection in the future. We also emphasized that the intersection of LBS and other popular technologies will lead to further scientific growth in this area to address user needs.

5. Direction of Future Research

As privacy is a core issue in VANETs, our detailed review has anticipated some potential future directions.

(i) As in the VANETs, all entities and information are placed under the shelter of TA, RSU, and drivers, so the tracking system of vehicles should have a robust mechanism of digital signature and pseudonym identity to avoid privacy attacks. A more robust and more reliable digital signature system should be introduced

(ii) There should be a dual authentication system to secure data transmission on the VANETs, as nowadays, on the Internet, all email systems and personal accounts are based on a dual authentication system. In this way, the attackers cannot cheat the drivers and the network

(iii) There is an efficient need for the VANET tracking app to double-check the security. Both ends of connectivity, i.e., TA and driver, may understand that there is no attacker or alternation in the messages

(iv) There should be a faster communication method so that privacy may not be disturbed along with speedier data dissemination

(v) VANETs should be switched to the 5G technology. VANET service providers and users can benefit from the high speed of 5G, as 5G is faster and information dissemination will be quicker

6. Conclusion

Security and privacy play a vital role in this fast-growing technological era. Modern cyber-physical technologies such as VANETs are particularly lucrative targets for fundamental information breaches. Breaching a mobile VANET node can lead to physical attacks, such as tracking delay of data dissemination, leading to severe problems. It is impossible to run a VANET in a compromised condition. We have analyzed the privacy and security-based attacks in VANETs. Various types of attacks were considered, which can halt the VANET efficiency. To resolve the problems, different beneficial techniques such as cryptography and pseudonyms were found adequate to protect the network and user's privacy from various attacks. Moreover, OTP-based system mechanism can make the network's confidentiality more secure. It is a real-time double verification for VANETs. Moreover, the incorporation of 5G is also a good option for new and innovative real-time applications via VANET. Furthermore, integration with other supporting technologies such as cloud computing and IoT will enhance the robustness of data dissemination.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] R. Hemalatha and J. A. Samath, "A survey: security challenges of VANET and their current solution," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 2, pp. 1239–1244, 2021.

[2] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: a survey," *IEEE Communication Surveys and Tutorials*, vol. 19, no. 4, pp. 3015–3045, 2017.

[3] S. Khan, I. Sharma, M. Aslam, M. Z. Khan, and S. Khan, "Security challenges of location privacy in VANETs and state-of-the-art solutions: a survey," *Future Internet*, vol. 13, no. 4, pp. 96–122, 2021.

[4] L. Sleem, H. N. Noura, and R. Couturier, "Towards a secure ITS: overview, challenges and solutions," *Journal of Information Security and Applications*, vol. 55, article 102637, 2020.

[5] C. Hu, J. Zhang, and Q. Wen, "An identity-based personal location system with protected privacy in IoT," *2011 4th IEEE International Conference on Broadband Network and Multimedia Technology*, vol. 2011, no. 2011, pp. 192–195.

[6] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: a survey," *Computer Communications*, vol. 91-92, pp. 17–28, 2016.

[7] G. Sun, Y. Zhang, D. Liao, H. Yu, X. Du, and M. Guizani, "Bus-trajectory-based street-centric routing for message delivery in urban vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7550–7563, 2018.

[8] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, and M. N. M. Bhutta, "Security in vehicular ad hoc networks: challenges and countermeasures," *Security and Communication Networks*, vol. 2021, 20 pages, 2021.

[9] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "VPPCS: VANET-based privacy-preserving communication scheme," *IEEE Access*, vol. 8, pp. 150914–150928, 2020.

[10] A. Ullah, X. Yao, S. Shaheen, and H. Ning, "Advances in position based routing towards ITS enabled FoG-oriented VANET-a survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 2, pp. 828–840, 2020.

[11] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A Comprehensive Survey : Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020.

[12] E. Farsimadan, F. Palmieri, L. Moradi, D. Conte, and B. Paternoster, "Vehicle-to-everything (V2X) communication scenarios for vehicular ad-hoc networking (VANET): an overview," *Computational Science and Its Applications – ICCSA*, no. article 12956, pp. 15–30, 2021.

[13] G. Sun, L. Song, H. Yu, V. Chang, X. Du, and M. Guizani, "V2V routing in a VANET based on the autoregressive integrated moving average model," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 908–922, 2019.

[14] R. Mishra, A. Singh, and R. Kumar, "VANET security: issues, challenges and solutions," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, vol. 2016, pp. 1050–1055, 2016.

[15] A. Yang, J. Weng, N. Cheng, J. Ni, X. Lin, and X. Shen, "DeQoS attack: degrading quality of service in VANETs and its mitigation," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4834–4845, 2019.

[16] J. Jiang, G. Han, H. Wang, and M. Guizani, "A survey on location privacy protection in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 125, pp. 93–114, 2019.

[17] S. R. Shetty and D. H. Manjaiah, "A comprehensive study of security attack on VANET," *Data Management, Analytics and Innovation*, vol. 71, pp. 407–428, 2022.

[18] S. A. Soleymani, S. Goudarzi, M. H. Anisi, M. Zareei, A. H. Abdullah, and N. Kama, "A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET," *Vehicular Communications*, vol. 29, article 100335, 2021.

[19] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in VANETs," *Computer Science Review*, vol. 41, article 100411, 2021.

[20] I. Memon, "Distance and clustering-based energy-efficient pseudonyms changing strategy over road network," *International Journal of Communication Systems*, vol. 31, no. 11, article e3704, 2018.

[21] M. M. Hamdi, Y. A. Yussen, and A. S. Mustafa, "Integrity and authentications for service security in vehicular ad hoc networks (VANETs): a review," *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, vol. 2021, 2021.

[22] F. Liu, Z. Chen, and B. Xia, "Data dissemination with network coding in two-way vehicle-to-vehicle networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2445–2456, 2016.

[23] V. Primault, A. Boutet, S. Mokhtar, and Ben; Brunie, L, "The long road to computational location privacy: a survey," *IEEE Communication Surveys and Tutorials*, vol. 21, no. 3, pp. 2772–2793, 2019.

[24] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approachesvol. 18, no. 1, pp. 163–175.

[25] T. Pavithra and B. S. Nagabhushana, "A survey on security in VANETs," in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, vol. 2020, pp. 881–889, Coimbatore, India, 2020.

[26] A. S. Mustafa, M. M. Hamdi, H. F. Mahdi, and M. S. Abood, "VANET: towards security issues review," in *2020 IEEE 5th International Symposium on Telecommunication Technologies (ISTT)*, pp. 151–156, Shah Alam, Malaysia, 2020.

[27] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2603–2611, 2020.

[28] A. Sharma and A. Jaekel, "Machine learning approach for detecting location spoofing in VANET," in *2021 International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–6, Athens, Greece, 2021.

[29] A. A. O. Affia, R. Matulevičius, and A. Nolte, "Security risk management in cooperative intelligent transportation systems: a systematic literature review," in *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems*, pp. 282–300, Cham, 2019.

[30] M. R. Schurgot, D. A. Shinberg, and L. G. Greenwald, "Experiments with security and privacy in IoT networks," in *2015 IEEE 16th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–6, Boston, MA, USA, 2015.

[31] C. Huang, R. Lu, X. Lin, and X. Shen, "Secure automated valet parking: a privacy-preserving reservation scheme for autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11169–11180, 2018.

[32] H. C. Pöhls, V. Angelakis, S. Suppan et al., "RERUM: building a reliable IoT upon privacy- and security- enabled smart objects," in *2014 IEEE wireless communications and networking conference workshops (WCNCW)*, pp. 122–127, Istanbul, Turkey, 2014.

[33] R. K. Sahu and A. M. Malla, “Security attacks with an effective solution for DOS attacks in VANET,” *International Journal of Computer Applications*, vol. 66, pp. 975–8887, 2013.

[34] Y. Kim, I. Kim, and C. Y. Shim, “A taxonomy for DOS attacks in VANET,” *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, vol. 2018, Article ID 1640167, pp. 26-27, 2014.

[35] K. Verma, H. Hasbullah, A. Kumar et al., “Prevention of DoS attacks in VANET,” *Wireless Personal Communications*, vol. 73, no. 1, pp. 95–126, 2013.

[36] M. Grissa, B. Hamdaoui, and A. A. Yavuza, “Location privacy in cognitive radio networks: a survey,” *IEEE Communication Surveys and Tutorials*, vol. 19, no. 3, pp. 1726–1760, 2017.

[37] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu, “FADB: a fine-grained access control scheme for VANET data based on blockchain,” *IEEE Access*, vol. 8, pp. 85190–85203, 2020.

[38] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, “Towards secure and practical consensus for blockchain based VANET,” *Information Sciences*, vol. 545, pp. 170–187, 2021.

[39] H. Zhong, B. Huang, J. Cui, J. Li, and K. Sha, “Efficient conditional privacy-preserving authentication scheme using revocation messages for VANET,” in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–8, Hangzhou, China, 2018.

[40] G. Sun, V. Chang, M. Ramachandran et al., “Efficient location privacy algorithm for Internet of Things (IoT) services and applications,” *Journal of Network and Computer Applications*, vol. 89, pp. 3–13, 2017.

[41] J. Daubert, A. Wiesmaier, and P. Kikiras, “A view on privacy & trust in IoT,” in *2015 IEEE International Conference on Communication Workshop (ICCW)*, pp. 2665–2670, London, UK, 2015.

[42] Y. Xu, F. Li, and B. Cao, “Privacy-preserving authentication based on pseudonyms and secret sharing for VANET,” *2019 Computing, Communications and IoT Applications (ComComAp)*, vol. 2019, pp. 157–162, 2019.

[43] Q. A. Arain, D. Zhongliang, I. Memon et al., “Privacy preserving dynamic pseudonym-based multiple mix-zones authentication protocol over road networks,” *Wireless Personal Communications*, vol. 95, no. 2, pp. 505–521, 2017.

[44] U. Rajput, F. Abbas, H. Eun, R. Hussain, and H. Oh, “A two level privacy preserving pseudonymous authentication protocol for VANET,” in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 643–650, Abu Dhabi, United Arab Emirates, 2015.

[45] U. Rajput, F. Abbas, and H. Oh, “A hierarchical Privacy preserving pseudonymous authentication protocol for VANET,” *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

[46] J. Qi and T. Gao, “A privacy-preserving authentication and pseudonym revocation scheme for VANETs,” *IEEE Access*, vol. 8, pp. 177693–177707, 2020.

[47] J. Zhang and Q. Zhang, “On the security of a lightweight conditional privacy-preserving authentication in VANETs,” *IEEE Transactions on Information Forensics and Security*, vol. 14, p. 1, 2021.

[48] J. Ni, X. Lin, and X. Shen, “Toward privacy-preserving valet parking in autonomous driving era,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2893–2905, 2019.

[49] S. S. Kaushik, “Review of different approaches for privacy scheme in VANETS,” *International Journal of Advances in Engineering & Technology*, vol. 5, pp. 356–363, 2013.

[50] J. Serna, R. Morales, M. Medina, and J. Luna, “Trustworthy communications in vehicular ad hoc networks,” *2014 IEEE World Forum on Internet of Things (WF-IoT)*, vol. 2014, pp. 247–252, 2014.

[51] B. K. Pattanayak, O. Pattnaik, and S. Pani, “Dealing with Sybil attack in VANET,” *Intelligent and Cloud Computing*, vol. 194, pp. 471–480, 2021.

[52] W. Xiong, R. Wang, Y. Wang, F. Zhou, and X. Luo, “CPPA-D: efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 4, pp. 3456–3468, 2021.

[53] L. E. Funderburg and I. Y. Lee, “Efficient short group signatures for conditional privacy in vehicular ad hoc networks via ID caching and timed revocation,” *IEEE Access*, vol. 9, pp. 118065–118076, 2021.

[54] M. Obaidat, M. Khodjaeva, J. Holst, and M. Zid, “Ben Security and Privacy Challenges in Vehicular Ad Hoc Networks,” in *Connected Vehicles in the Internet of Things*, Z. Mahmood, Ed., pp. 223–251, Springer, Cham, 2020.

[55] F. B. Günay, E. Öztürk, T. Çavdar, Y. S. Hanay, and A. Khan, “Vehicular ad hoc network (VANET) localization techniques: a survey,” *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3001–3033, 2021.

[56] K. Xue, Q. Yang, S. Li et al., “PPSO: a privacy-preserving service outsourcing scheme for real-time pricing demand response in smart grid,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2486–2496, 2019.

[57] A. Boualouache, S. M. Senouci, and S. Moussaoui, “A survey on pseudonym changing strategies for vehicular ad-hoc networks,” *IEEE Communication Surveys and Tutorials*, vol. 20, no. 1, pp. 770–790, 2018.

[58] I. Saini, B. St Amour, and A. Jaekel, “Intelligent adversary placements for privacy evaluation in VANET,” *Information*, vol. 11, p. 443, 2020.

[59] L. Benarous, B. Kadri, and S. Boudjit, “Alloyed pseudonym change strategy for location privacy in VANETs,” in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, Las Vegas, NV, USA, 2020.

[60] A. Verma, R. Saha, G. Kumar, and T. H. Kim, “The security perspectives of vehicular networks: a taxonomical analysis of attacks and solutions,” *Applied Sciences*, vol. 11, p. 4682, 2021.

[61] S. Sharma, A. Kaul, S. Ahmed, and S. Sharma, “A detailed tutorial survey on VANETs: emerging architectures, applications, security issues, and solutions,” *International Journal of Communication Systems*, vol. 34, no. 14, 2021.

[62] M. Al-Mehdhara and N. Ruan, “MSOM: efficient mechanism for defense against DDoS attacks in VANET,” *Wireless Communications and Mobile Computing*, vol. 2021, 17 pages, 2021.

[63] F. G. Abdulkadhim, Z. Yi, C. Tang, A. N. Onaizah, and B. Ahmed, “Design and development of a hybrid (SDN + SOM) approach for enhancing security in VANET,” *Applied Nanoscience*, vol. 1, pp. 1–12, 2021.

[64] D. Xu, “Proactive eavesdropping of suspicious non-orthogonal multiple access networks,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13958–13963, 2020.

[65] H. Bangui, M. Ge, B. Buhnova, and L. Hong Trang, “Towards faster big data analytics for anti-jamming applications in vehicular ad-hoc network,” *Transactions on Emerging*

Telecommunications Technologies, vol. 32, no. 10, article e4280, 2021.

[66] N. Wisitpongphan, O. K. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, and V. Sadekar, "Broadcast storm mitigation techniques in vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 84–94, 2007.

[67] K. H. Mohammadani, K. A. Memon, I. Memon, N. N. Hussaini, and H. Fazal, "Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 16, no. 5, 2020.

[68] G. Luo, Q. Yuan, H. Zhou et al., "Cooperative vehicular content distribution in edge computing assisted 5G-VANET," *China Communications*, vol. 15, no. 7, pp. 1–17, 2018.

[69] P. Kohli, S. Sharma, and P. Matta, "Security challenges, applications and vehicular authentication methods in VANET for smart traffic management," in *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 327–332, London, United Kingdom, 2021.

[70] A. Kumar and N. Gupta, "A secure RSU based security against multiple attacks in VANET," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, pp. 1156–1163, Thoothukudi, India, 2020.

[71] P. Shah and T. Kasbe, "Detecting Sybil attack, black hole attack and DoS attack in VANET using RSA," *Algorithmica*, vol. 1–7, p. doi:10.1109/ETI4.051663.2021.9619414, 2021.

[72] B. K. Pattanayak, O. Pattnaik, and S. Pani, "A novel approach to detection of and protection from Sybil attack in VANET," *Lecture Notes in Networks and Systems*, vol. 109, pp. 240–247, 2020.

[73] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *2012 6th International Conference on Signal Processing and Communication Systems*, pp. 1–9, Gold Coast, QLD, Australia, 2012.

[74] O. E. Ojo, C. O. Iyadi, A. O. Oluwatope, and A. T. Akinwale, "AyoPeer: the adapted ayo-game for minimizing free riding in peer-assisted network," *Peer-to-Peer Networking and Applications*, vol. 13, no. 5, pp. 1672–1687, 2020.

[75] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin, and H. Wang, "Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1779–1790, 2019.

[76] W. Li and H. Song, "ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

[77] P. K. Singh, A. Agarwal, G. Nakum, D. B. Rawat, and S. Nandi, "MPFSLP: masqueraded probabilistic flooding for source-location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 11383–11393, 2020.

[78] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5535–5548, 2020.

[79] M. H. Junejo, A. A. H. A. Rahman, R. A. Shaikh, and K. M. Yusof, "Location closeness model for VANETs with integration of 5G," *Procedia Computer Science*, vol. 182, pp. 71–79, 2021.

[80] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 9, pp. 113226–113238, 2021.

[81] M. Alotaibi, "Improved Blowfish algorithm based secure routing technique in IoT based WSN," *IEEE Access*, vol. 9, pp. 159187–159197, 2021.

[82] S. Mandal, S. Mohanty, and B. Majhi, "CL-AGKA: certificateless authenticated group key agreement protocol for mobile networks," *Wireless Networks*, vol. 26, no. 4, pp. 3011–3031, 2020.

[83] G. Goel, R. Tiwari, A. Anand, and S. Kumar, "Workflow Scheduling Using Optimization Algorithm in Fog Computing," *Advances in Intelligent Systems and Computing*, pp. 379–390, 2022.

[84] X. Ma, J. Zhang, X. Yin, and K. S. Trivedi, "Design and analysis of a robust broadcast scheme for VANET safety-related services," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 46–61, 2012.

[85] T. W. Chim, S. M. Yiu, L. C. K. Hui, Z. L. Jiang, and V. O. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Networks*, vol. 9, pp. 189–203, 2011.

[86] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping-part I: system design," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 70–79, 2013.

[87] B. Aslam and C. Zou, "Distributed certificate and application architecture for VANETs," in *MILCOM 2009-2009 IEEE Military Communications Conference*, pp. 1–7, Boston MA, USA, 2009.

[88] L. Chen, S. Thombre, K. Jarvinen et al., "Robustness, security and privacy in location-based services for future IoT: a survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[89] D. An, Q. Yang, W. Yu, D. Li, and W. Zhao, "LoPrO: location privacy-preserving online auction scheme for electric vehicles joint bidding and charging," *Future Generation Computer Systems*, vol. 107, pp. 394–407, 2020.

[90] S. S. Chhatwal and M. Sharma, "Detection of impersonation attack in VANETs using BUCK Filter and VANET Content Fragile Watermarking (VCFW)," in *2015 International Conference on Computer Communication and Informatics (ICCCI)*pp. 1–5, Coimbatore, India, 2015.

[91] P. Kohli, S. Painuly, P. Matta, and S. Sharma, "Future trends of security and privacy in next generation VANET," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, pp. 1372–1375, Thoothukudi, India, 2020.

[92] N. C. Velayudhan and A. Anitha, "Sybil attack in VANET operating in an urban environment: an overview," *Advances in Communication Systems and Networks*, vol. 656, pp. 433–442, 2020.

[93] S. Kumar and V. Singh, "A review of digital signature and hash function based approach for secure routing in VANET," *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, vol. 2021, pp. 1301–1305, 2021.