Location Privacy Schemes in Vehicular Networks: Taxonomy, Comparative Analysis, Design Challenges, and Future Opportunities

Ikram Ullah[1], Munam Ali Shah[1], Abid Khan[2], Mohsen Guizani[3]

Department of Computer Science, COMSATS University Islamabad, Pakistan[1]

College of Science and Engineering, School of Computing, University of Derby, DE22 1GB, United Kingdom[2]

College of Engineering, Qatar University, Doha, Qatar[3]

ikram.comsats.cs@gmail.com, mshah@comsats.edu.pk, a.khan3@derby.ac.uk, mguizani@ieee.org

Abstract: Vehicular networks (VANETs) revolutionized the world with smart traffic management, utilizing a road environment, and providing safety and convenience to the vehicle driver. Despite the useful features of vehicular networks, there are some privacy issues, which hinder their way toward achieving a smart world. Location privacy is one of the critical research challenges for the efficient deployment of VANETs. This challenge can be solved using a pseudonym instead of an actual vehicle identity in the beacon messages. For this purpose, many location privacy schemes are introduced in the literature. In this paper, we thoroughly review the existing location privacy schemes and present their comprehensive taxonomy. We discuss the design challenges for the development of an efficient location privacy scheme. Moreover, the existing location privacy techniques are critically analyzed based on diverse road network environments and parameters. Various issues and challenges regarding the pseudonym-changing process are elaborated in detail. Finally, we discuss the future trends for the implementation of location privacy in a vehicular network.

Keywords: VANETs, location privacy, pseudonym, mix zone, silent period, group signature, path perturbation, anonymous authentication.

I. INTRODUCTION

The transportation system is an integral part of human life and contributes to developing the social and economic order of a country. The growing number of vehicles creates difficulty for the transportation system to provide various services and facilities to the vehicles. The flux environment of transport produces various traffic congestion problems, road accidents, safety, energy consumption, maintenance cost, [1], etc. That is why, the idea of an Intelligent Transportation System (ITS) was introduced. ITS is a transportation management system that incorporates information technology, computers, communication, and other related technologies. This provides road environment information and various services to the vehicle driver to decrease congestion and improve road safety [2], [3]. One of ITS's essential components is Vehicular Ad-hoc Networks (VANETs) that make it possible for vehicles to share road environment information. It is the subfield of Mobile Ad-hoc Networks (MANETs) that uses various communication technologies to produce spontaneous networks on the road. The vehicles are equipped with wireless technologies and processing abilities to create an ad-hoc network on the road.

Vehicles in a network periodically broadcast beacons or Basic Safety Messages (BSM) to inform other vehicles about road and traffic conditions for safety and facilitation purposes. The terms beacon and BSM are considered the same in this article. The BSM is one of the significant messages in the SAE J2735 standard [4], which broadcasts the state information of vehicles such as vehicle position, status, size, and dynamics. All V2V safety applications are supported by the BSM. There are two parts of the BSM, the first part contains critical state information which highlights compactness and efficiency. The second part is optional which contains extra data elements and frames. The contents of the BSM first part are MessageID, MsgCount, TemporaryID, Dsecond, Latitude and Longitude, Elevation, PositionalAccuracy, TransmissionAndSpeed, Heading, SteeringWheelAngle, AccelarationSet4Way, BrackSystemStatus, and VehicleSize. The most discussed data items of the BSM second part are EventFlags, PathHistory, PathPrediction, and RTCMPackage [5]. The safety message is generated periodically and transmitted to one-hop neighbors. It is the main concern of various safety applications. The local road network information is collected and broadcast via the BSM to contain a local view of the neighborhood for safety services. Also, it holds sensor readings of vehicle state such as vehicle identity, velocity, location, etc. The information provided during vehicle communications can prevent vehicle collisions and reduce accidents, and can also inform drivers to select alternative strategies on the road [6]. These messages improve road safety and help

to inform vehicles about the road environment. The beacon messages are not in encrypted form as encryption increases latency [7]. The unencrypted beacon message creates severe privacy issues for the vehicle driver. The adversary may listen to messages in the network and identify various location spots visited by the target vehicle (a vehicle that an adversary desires to locate and identify) during a specific period, which may breach the vehicle driver's location privacy. For example, an adversary may capture the broadcast message in the network. These messages contain vehicle identity and location information. With the help of obtained data, the adversary may be able to identify the behavior and specific activities of a driver at different visited locations. It may create several threats to the driver, i.e., loss of social reputation, physical harassment, money loss, etc. [8]. It raises the idea of location privacy in the context of VANETs. Location privacy concept is receiving importance nowadays in vehicular network implementation. Breach of the location information may hurt the vehicle driver with certain types of dangers, as discussed earlier.

To protect the location of a vehicle driver, several privacy-preserving techniques have been introduced. The existing privacy schemes take the help of the pseudonyms-changing process. In beacon, pseudonyms are used instead of the genuine identity of the vehicle. Pseudonyms are issued by Trusted Authority (TA), i.e., government authority. TA has the power to track vehicles based on the given pseudonyms to achieve conditional privacy. For the preservation of the location privacy of the vehicle, the pseudonym needs to be changed synchronously to guard against the pseudonym linking attack. Several pseudonym-changing strategies are introduced for the location protection of the vehicle. The existing research takes the change of pseudonyms in various areas and defines some criteria for it. Such as the pseudonym must be changed in the mix zone area or in the form of a group or during the silent period. The abbreviations used in the paper are given in Table 1. The terms, vehicular network, vehicular communication network, and VANETs are used alternatively and considered to have the same meaning as vehicular ad-hoc networks throughout this paper.

Table 1 Abbreviations used in the paper

Abbreviations	Definition	Abbreviations	Definition
ASS	Anonymity Set Size	NMF	Nonnegative Matrix Factorization
AOSA	Anonymous Online Service Access	VSN	Vehicular Social Network
ALUM	Autonomous Location Update Mechanism	OBU	OnBoard Unit
AU	Application Unit	PACP	Pseudonym Authentication based Conditional Privacy
BSM	Basic Safety Message	PCP	Pseudonym Changing at Proper location
CA	Certificate Authority	PPV	Pseudonym Provider Vehicles
CMIX	Cryptographic Mix Zone	POI	Point of Interest
CADS	Context Adaptive Privacy Scheme	REP	Random Encryption Period
CRL	Certificate Revocation List	RPC	Pseudonym Change
DSRC	Dedicated Short Range Communication	RS	Reported Server
EPZ	Endpoint Protection Zone	RSU	Road Side Unit
GPA	Global Passive Adversary	TA	Trusted Authority
LBS	Location-Based Server	TAPCS	Traffic-Aware Pseudonym Changing Strategy
LPG	Location Privacy Gain	SLOW	Silent at Low speed
MOP	Multiple Obfuscation Path	VANETs	Vehicular Adhoc Networks
MSN	Mobile Social Network	V2I	Vehicle to infrastructure
NMF	Nonnegative Matrix Factorization	V2V	Vehicle to Vehicle
TDMA	Time Division Multiple Acces		

A. Relation with previous surveys

Various surveys have been conducted in the literature concerning security issues for the vehicular network. The existing surveys only consider one or other security aspects of vehicular communication networks. In [9], first, the general security and its requirements are discussed; after that, some of the location privacy schemes based on anonymous authentication are reviewed. It has not included details about location privacy taxonomy as well as privacy threats during vehicular communication. Petit et al. [10] describe only the challenges of the V2X (vehicle-to-everything) communication model: vehicle-to-everything is a communication system in which multiple entities in an environment communicate with each other for road safety and traffic efficiency, they give a summary of pseudonym-changing approaches based on an authentication mechanism. The general security issues and privacy are reviewed in [11] for the vehicular network. Little interest has been shown in privacy schemes and their categorization. A useful survey on location privacy in the field of Mobile Social Networks (MSN) and Vehicular Social Networks

(VSN) is conducted in [12]. The technical privacy metrics are highlighted in [13] systematically. They discussed over 80 different privacy metrics. In [14], a survey is conducted on pseudonym-changing approaches for VANETs and divided into two classes, i.e., mix zone-based techniques and mixed context-based schemes. Also, have details on the adversary model for location privacy. A summary of general security, trust, and privacy problems is given in the paper [15]. The anonymous authentication schemes are discussed; however, lacking the detailed categorization of location privacy schemes. In [16], only location privacy schemes based on the creation of mix zone concepts are reviewed. Talat et al. [17] provide a summary of location privacy schemes in the case of VANETs but do not critically analyze the existing strategies, limited categorization, lack of research challenges, and future direction. Some of the authentication and privacy systems are analyzed in [18] and compared with their merits and demerits, security requirements, security attacks, and performance factors. The focus of the survey conducted in [19] is to discuss only cryptographic-based techniques for achieving location privacy and authentication. Location privacy is discussed in [20] from the perspective of social networks, which is different from other location privacy preservation mechanisms in a vehicular network. A survey of privacy and security issues is presented in [21], however, it only discussed the main security features and attacks in VANETs. In [22], limited location privacy schemes are discussed that are divided into three categories including location privacy, identity privacy, and data privacy mechanism. Table 2 contains information about some of the existing security and location privacy surveys in the vehicular network.

Table 2 Overview of various VANETs security surveys

Ref:	Publication year	Main functions	Deficiency
[10]	2015	Challenges of V2X communication model, an overview of pseudonym changing strategies, pseudonym life cycle	No detailed categorization of location privacy mechanisms and only covers authentication-based and cryptographic techniques.
[11]	2015	General security issues and some privacy issues	Only discuss privacy in one section and have no proper detail of location privacy schemes
[12]	2017	- Location privacy in MSN and VSN - Various attacks discussed - Categorization of privacy - Location-based attacks - Countermeasure for privacy attacks	Discussion about location privacy in the case of MSN and VSN. Much attention is given to cryptographic schemes.
[14]	2018	Study efficiency of pseudonym-changing strategies, privacy metrics, efficient detail on adversary model.	No comprehensive categorization of privacy schemes, required to discuss design challenges.
[15]	2019	Discussion on security services, anonymous authentication schemes, and trust models	Lacks detailed categorization of privacy schemes, missing privacy measuring metrics, and privacy model challenges.
[17]	2019	VANETs overview, discusses general threats; some of the vehicular network aspects are analyzed.	Limited categorization of the existing schemes, lack of research challenges, and future direction.
[23]	2021	Critical analysis of attacks, analysis of existing solutions, discussed location privacy metrics	Not deeply categorize the location privacy schemes, not mentioned location privacy design challenges, pseudonym distribution and management is not discussed which is the core concept of location privacy protection

The majority of the surveys conducted in the case of VANETs mostly cover security issues and attacks, limited attention is given to privacy issues. Useful surveys are carried out in [10], [14], [17], [18], [19], [24] for security and privacy issues in VANETs. The coverage of the survey in [10] is only limited to pseudonym-changing schemes based on public key, identity-based cryptography, group signatures, and symmetric authentication. Limited space is given to other location privacy schemes such as mix zones, and silent periods schemes. Paper [14] divided pseudonyms changing approaches into two classes, i.e., mix zone and mix context methods. However, there may be many more categories of privacy schemes that exist in the literature. Moreover, they discussed location privacy concerning authentication schemes. Moreover, there is also a lack of a discussion of the pseudonym issue and distribution problem concerning the pseudonym-changing process and its impact on other fields of VANETs such as the routing protocol. While the paper [17] just discusses general security threats, some of the vehicular network aspects are analyzed.

They did not comprehensively categorize the existing schemes; no research challenges or future directions were provided. The concern of [18] is to critically analyze the general security requirements (source authentication, message authentication, non-repudiation, collision resistance), security attacks (DoS, modification, impersonation, bogus information, Sybil, replay), and performance efficiency factors (computation and communication costs), there is little concern given to location privacy schemes. In the survey [24], the privacy schemes are provided in chronological order, strategies are divided into two categories i.e. triggered and trigger-free. They only provide details about general security attacks (DoS, malware, masquerade, man in the middle) not discuss the specific location privacy attacks and threats, and do not have privacy schemes designed challenges. In [19] the main focus is to discuss the cryptographic-based schemes for achieving authentication, and privacy. These schemes are based on symmetric key cryptography, public key infrastructure, identity-based cryptography, certificateless signature, and pseudonym-based authentication schemes. The pseudonym-based location privacy schemes are only discussed with respect to authentication mechanism. Not discuss the main privacy requirements such as anonymity, minimum disclosure, unlinkability, and uncertainty.

After a careful study of the existing surveys carried out for VANETs, we developed a suitable survey for location privacy issues. The contributions of this paper are summarized as (1) we provide a comprehensive taxonomy of pure location privacy schemes and its timeline, (2) we clearly mention the important design challenges for the development of privacy protection methods, (3) we highlight the problems and issues related to the pseudonym changing process, and (4) critically analyze issues and problems with existing schemes. The comparison of the proposed survey with existing surveys in terms of location privacy protection schemes, comprehensive taxonomy, privacy techniques timeline, privacy design challenges, and pseudonym management challenges is given in Table 3.

Table 3 Comparison with related surveys concerning location privacy schemes, privacy design, and pseudonym management challenges

	[10]	[14]	[17]	[18]	[19]	[24]	Proposed survey
Location protection mechanisms							
Cryptographic mechanisms	✓	×	×	✓	✓	✓	✓
Group signature	✓	✓	×	✓	✓	×	✓
Mix zone	✓	✓	✓	×	×	✓	✓
Silent period	✓	✓	×	×	×	✓	✓
Path perturbation	×	×	✓	×	×	×	✓
Triggered based	×	×	✓	×	×	✓	✓
Anonymous authentication	×	×	×	✓	✓	×	✓
Privacy design challenges	×	×	×	×	×	×	✓
Pseudonym management challenges	×	×	×	×	×	×	✓
Comprehensive taxonomy of location privacy schemes	×	×	×	×	×	×	✓
Location privacy schemes timeline	×	×	×	×	×	×	✓

B. Contributions:

The major contributions of this research work are summarized as follows.

i. The paper consists of a new and comprehensive categorization of the existing location privacy strategies with respect to diverse road traffic conditions and environments. We provide a summarized evolution of location privacy techniques in vehicular networks shown in Figure 4.

ii. We critically analyzed side by side comparison of the privacy-preserving schemes based on various factors and parameters in tabular form. The paper also has a comprehensive analysis of various location privacy attacks and threats taken in the existing literature.

iii. This survey contains various privacy design challenges that may help the researcher in the development of effective location privacy schemes in vehicular networks.

iv. We provide a thorough overview of the challenges regarding the pseudonym-changing process in other fields of the VANETs, such as routing protocols.

The rest of the paper is planned as follows. Section II contains the necessary background information. Privacy requirements and various attacks are discussed in Section III. Section IV talked about the existing location privacy techniques. Section V contains the comparative analysis of the location privacy approaches. Open issues and considerations are argued in Section VI. Section VII contains design challenges and future directions. The useful and negative features of existing work are discussed in Section VIII. Finally, the paper is concluded in Section IX.

II. VANETS AND PRIVACY

In this section, we presented the basic concept of VANETs, privacy, wireless technologies, and motivational scenarios for location privacy. It provides a simple research background for location privacy in Vehicular Adhoc Networks for interested readers.

A. The basic architecture of VANETs

The simple structure of VANETs comprises of Road Side Unit (RSU), OnBoard Unit (OBU), and Application Unit (AU) [3]. RSUs are wireless devices fixed on the roadside or near the junction and parking lot to enable wireless communication with faraway vehicles. It extends the communicating range of the network by sending information to other RSUs and vehicles out of the transmission range. RSU acts as an information source to disseminate road information in the vehicle-working zone and provide Internet facilities to the vehicle. OBU is a WAVE device fixed in the vehicle to exchange information with RSUs and other OBUs. OBU has a memory, which contains information about the vehicle's identity, certificates, and additional related information. The primary functions of the OBU are wireless radio access, reliable message transfer, ad-hoc routing, data security, network congestion control, etc. AU device is equipped in a vehicle as a single physical unit in OBU. It is a specialized device for safety services to run on the Internet.

There are three forms of communication models used in the VANETs, i.e., Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and hybrid communication model. In the V2V communication model, the vehicles are directly connected with each other to share road safety and general information; there is no need for infrastructure support. Note that in V2I, the vehicles communicate with road infrastructure for information dissemination. The hybrid communication model combines both V2V and V2I models. In this model, the road information is reached to infrastructure directly or indirectly. In the direct communication, vehicles are in the transmission range of infrastructure, and indirect communication is done through multi-hop. Various vehicles take part in forwarding the road information to the infrastructure [25]. The basic architecture of vehicular communication is presented in Figure 1.

B. Wireless technologies and standards

A set of wireless technologies and standards can be used in vehicular networks to satisfy the need for VANETs applications [26]. These technologies are Dedicated Short Range Communication (DSRC), Wireless Access in Vehicular Environment (WAVE) [27], cellular network standards, WiMax, WiFi, VeMAC protocol, etc. A cellular network (4G) is currently used by many car manufacturers to provide various services such as passenger entertainment, driver assistance, and remote vehicle diagnostics. However, the 5.9 GHz band is allocated to the cellular network by standard organizations (ETSI and FCC) which is difficult to utilize to operate on a lower frequency band. VeMAC (based on TDMA) is another wireless technology protocol proposed for VANETs that supports periodic and event-driven safety messages. VeMAC takes the help of a slot synchronization process using 1 pulse per second signal given by the GPS receiver [26]. Similarly, other wireless technologies can be utilized for wireless communications in VANETs, but here we only discuss the DSRC. Standard bodies in North America and Europe specify a family of the protocol stack from physical to application, in North America, it is called IEEE WAVE, while in Europe, it is known as ETSI ITS-G5. WAVE standard is based on the IEEE 802.11a protocol [28]. Later on, IEEE 802.11p was added by modifying the physical and MAC layers of 802.11a and adapting the vehicular networks according to the DSRC band. Generally, communication between vehicles and infrastructure is done using WAVE standards. It allows the exchange of various messages to ensure vehicle drivers' safety by updating road network information and traffic flow [3]. WAVE defines the architecture, mechanism, protocols, and

interface used for the growth of V2V and V2I communications. The WAVE standard improves road safety and increases the traffic efficacy of the vehicular network.

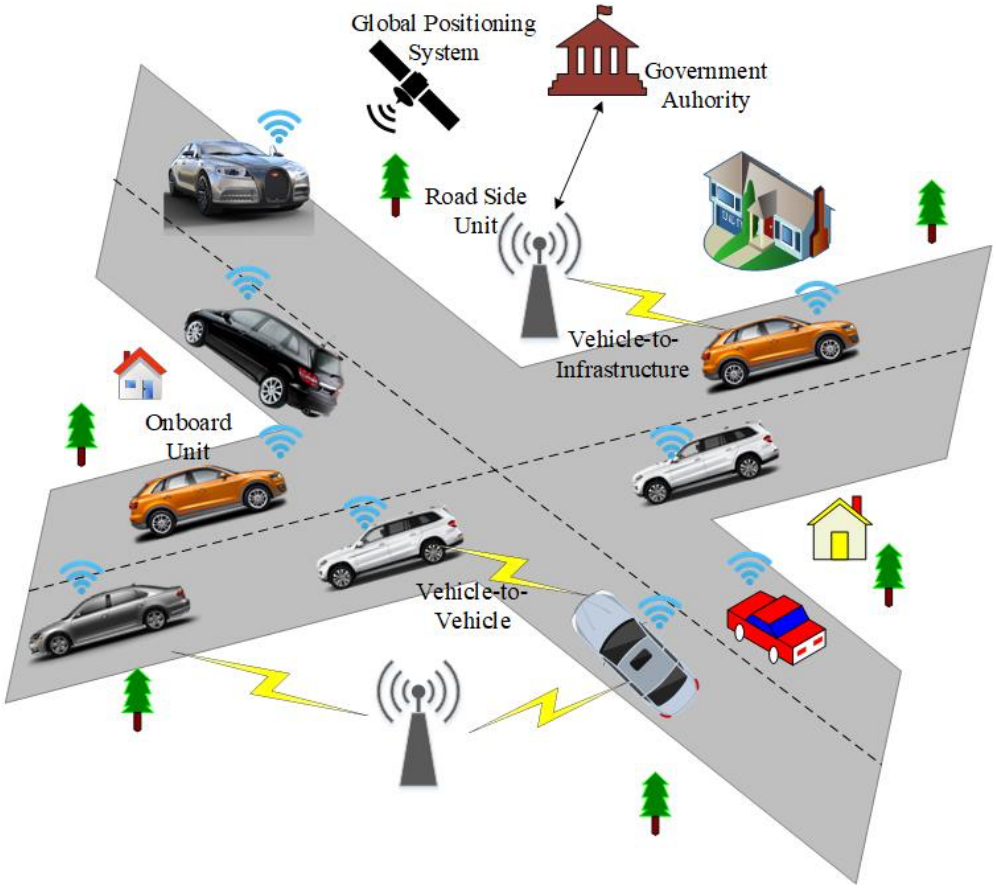

Figure 1 The basic architecture of VANETs

The DSRC is a short-range wireless technology that supports various types of vehicular communication applications [5]. The primary motivation for organizing the DSRC protocol is to permit collision preventive applications in vehicular communication, as vehicles connect with one another and with roadside infrastructure for regular information exchange. Department of Transportation of the US has estimated that vehicular communication based on DSRC may decrease traffic collapse by 82% to save millions of lives. Each DSRC equipped vehicle broadcasts safety messages in the network containing contents such as velocity, location, acceleration, and other vehicle headings. Other vehicles in the network can receive these safety messages. It is a short-range communication suite that requires low latency and high data range [26]. DSRC is defined in the IEEE 802.11p standard based on the physical layer and MAC layer. The deployment cost of IEEE 802.11p is little related to cellular technology. The US Federal Communication Commission and Europe Electronic Commission Committee assigned the spectrum for DRSC from 5.85 to 5.925 GHz [3], [29]. This band is allocated into seven channels 10 MHz each by IEEE and ETSI. These channels are further divided into one control channel and six service channels. The control channel is used to broadcast road status and emergency messages related to road safety. The remaining six channels have the responsibility of data transmission of various services [14].

C. Privacy concept

It is hard to explain privacy precisely, and the recognition of privacy consists of various dimensions. Some theorist creates a taxonomy for privacy problems. For example, the taxonomy of privacy problems is introduced in [30], i.e., information collection such as surveillance or interrogation, the problem of information processing includes data insecurity and potential identification, information dissemination consists of exposure and breach of confidentiality, an invasion that comprises of intrusion and decisional interference. Privacy is the protection of the private and confidential information of a user/person while using any communication

network. For ad-hoc networks, privacy is categorized into three kinds that may be protected from leakage to the third party, i.e., identity privacy, data privacy, and location privacy.

Identity privacy: The concealing of the actual identity of a user from an unauthorized person is called identity privacy. It is essential to conceal the identity of a person/user for privacy protection [12]. If the identity of a person is leaked, the adversary can easily know the behavior and other activities related to the concerned person.

Data privacy: Data privacy is the hiding of data transmitted during a communication network. It includes personal information of a person, i.e., home address, health condition, political connection, family information, etc. The users in the network communicate with each other for the information exchange required to be protected from an unauthorized party [30].

Location privacy: The shelter of location information of mobile users during connection within a network is considered location privacy. The user of the mobile network using the location service sends his/her actual location position to the server which may compromise the location of the user. The adversary makes a tracking route of a user, and the adversary comes to recognize the various locations visited by users during network communication. In the case of the vehicular network, the location privacy of the vehicle is sheltered with the help of using a pseudonym in place of the actual identity of a vehicle [31]. Several techniques have been proposed in the literature for the security of the location of vehicle drivers that are based on the pseudonym-changing process [32], [33], [34].

D. Motivational scenarios for location privacy

Let's explain the notion of location privacy breaches in VANETs with the help of an example. A vehicle Vi is moving on a road and broadcasts basic safety messages (beacon). The beacon contents are vehicle identity (VID), direction, speed, location, and other headings. In the beacon, the VID of the vehicle is openly broadcast within the network. The adversary on a roadside has covered a large vehicular network area listening to vehicles' beacon messages. The adversary captures beacon messages of the vehicle at various visited places. Then the adversary compares the VID of the captured beacons and tries to identify the other locations having the same VIDs and derives information about various locations visited by vehicle Vi. The adversary may easily get the different location spots of the vehicle Vi and recognize the activities and interests of a vehicle user. As shown in Figure 2, the adversary could relate the several locations visited by vehicle Vi during its trip and come to know that the vehicle is making a stop near a bank at three different locations. It provides information to the adversary that the vehicle is attached to the bank and contains money or an important person of the bank, which may produce serious threats to the driver while moving on the road network. The danger may be the snatch of money or vehicle, physical harassment, defamation, etc. Similarly, the case for a political person or company salesperson whose location privacy is essential for their organization/company.

III. LOCATION PRIVACY REQUIREMENTS AND ATTACKS

In this section, various privacy requirements are defined which are necessary for the improvement of the level of location privacy. We also discussed different types of attacks and threats to location privacy.

1. Location privacy requirements

Privacy requirements define the necessary parameters to be considered while evaluating user location privacy. These parameters are essential for achieving significant results from the perspective of user location privacy. To safeguard location privacy in VANETs, there is a demand to define the critical requirements of privacy. Some of the privacy requirements are mentioned in the following passage [35], [10].

i. **Anonymity:** It is the prime requirement of privacy to hide the sender of the message among multiple senders. The adversary could not distinguish the targeted sender in the crowd of vehicles. It is difficult for an adversary to link the message with the sender in the vehicular communication network. For example, an adversary may capture a message m in the network, but difficult to relate m with some particular user or vehicle.

ii. **Unlinkability:** It means that the association between two or more similar items can't be connected. It produced difficulty for an adversary to relate a message with a specific person. For example, an adversary may link a message to the vehicle, and based on this information, the vehicle is linked with a particular person, which provides sensitive information about that person. Therefore, unlinkability tries to break down the link between the vehicle and a person's identity.

iii. **Minimum disclosure:** A user would reveal the least amount of information for the smooth functioning of VANETs applications. This information should not demonstrate the private behavior of the person. It should follow the need-to-know principle in the privacy schemes. The exchange of information among vehicles is the fundamental concept of vehicular communication. Therefore, the user should provide some information in a controlled manner to protect personal information.

iv. **Uncertainty:** Privacy protection requires some uncertainty in sharing information in the network. It increased the confusion of an adversary while tracking the vehicle during communication. The uncertainty requirement should maintain a tradeoff between privacy and service utility.

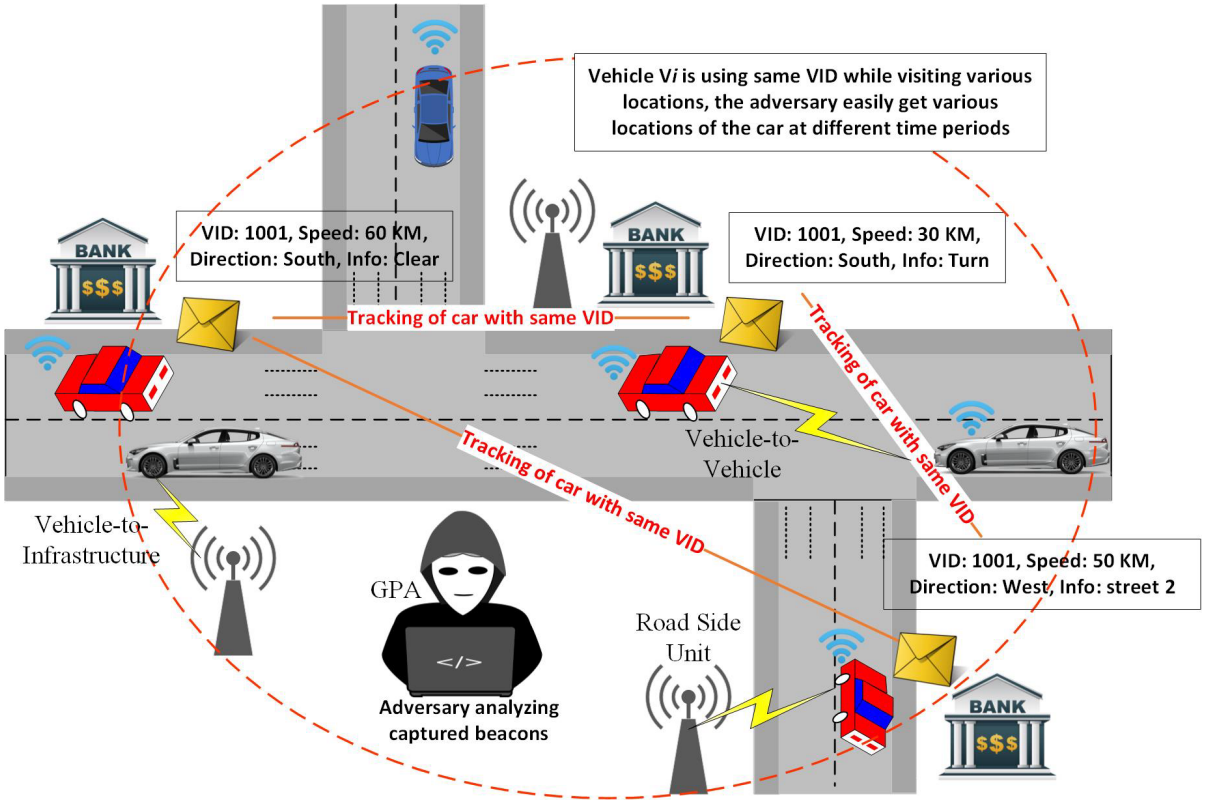

Figure 2 Location tracking of a vehicle with the same identity.

2. Location privacy attacks and threats

In this section, we discussed several types of location privacy threats and attacks in the context of the vehicular communication network. A summary of location privacy attacks is shown in Table 4. Following is the detail of some of the privacy attacks and threats.

a. Syntactic linking attack

In this type of attack, the attacker has the capability of linking the vehicle's old pseudonym with a new pseudonym. For example, there are three vehicles A, B, and C moving on the road with certain pseudonyms. After some Δt time, if only one vehicle B changes its pseudonym from B1 to B2.The attacker comes to know that only vehicle B changed the pseudonym. Thus the attacker easily links the old pseudonym B1 with the new pseudonym B2 of vehicle B and can reveal the identity which further helps in tracking the location movements [36], [37], [14].

b. Semantic linking attack

In this attack, the adversary may get some useful information from a safety message to link pseudonyms of a specific vehicle. The attacker takes the help of location data and other contextual information to find out the user's movement patterns or identities.

The contextual information may be the time of day, regularly visited locations or public events. For example, a person visiting specific locations like an exercise park every morning, and a specific shopping mall every weekend. By analyzing the location data, the adversary can infer that these visits are made by the same person. The adversary may link the pseudonyms of the concerned person at different locations and thus compromise the location privacy [36], [37].

Table 4 Summary of various privacy attacks/adversary/threats

Ref:	Syntactic linking attack	Semantic linking attack	Cheating attack	GPA	Transition attack	Local active adversary
[38]	✓	--	--	✓	--	--
[39]	--	--	--	✓	--	--
[36]	✓	✓	--	✓	--	✓
[40]	--	--	--	✓	✓	--
[41]	✓	--	--	✓	✓	--
[42]	--	--	--	✓	--	--
[43]	✓	--	✓	✓	--	--
[44]	✓	--	--	✓	--	--
[45]	--	--	--	✓	--	--
[46]	--	--	--	✓	--	✓
[47]	✓	--	--	✓	--	--
[48]	--	--	--	--	✓	--
[49]	✓	--	--	--	--	--
[50]	✓	--	--	✓	--	--
[51]	✓	--	--	✓	--	✓
[52]	--	--	--	✓	--	✓
[53]	✓	✓	--	✓	--	--
[54]	✓	--	✓	✓	--	--
[55]	✓	--	--	--	✓	--
[56]	--	--	--	✓	--	--
[7]	✓	✓		✓		
[57]	✓	--	✓	--	--	--
[58]	--	--	--	✓	--	--
[59]	✓	--	--	--	✓	--

c. Scrambler attack

Scrambler is a link-layer attack, in which the adversary tries to use scrambler values to link various messages irrespective of pseudonyms [60]. It beat the privacy measure of vehicle users. This attack is applicable when the vehicle is using static beacon frequencies. In the communication system, the scrambler value is used to randomize the data pattern before transmission. The scrambler value is a key or initial state used in the scrambler algorithm to change the original data sequence in pseudo-random mode. The receiver then takes the scrambler value for the descrambler algorithm to rebuild the original data pattern. The attacker exploits the scrambler values to correlate and link various messages of a vehicle during communication on the road network, which endangers the location privacy of vehicles.

d. Cheating attack

In a cheating attack, a malicious node broadcasts a falsified location message in the network to mislead other vehicles or infrastructure. It causes disruption in traffic navigation, safety applications, and traffic management. For the location tracking the compromised/malicious vehicle intentionally generates false beacon messages and sets a flag to 1 to obligate all neighbors in the

vicinity to change pseudonyms. The adversary is among the k neighbors of the network. In this way, the adversary cheats on other vehicles by making an image of a valid vehicle. Thus, the adversary analyzes location data and tries to track the target vehicle in that region [43].

e. Global passive adversary (GPA)

This adversary could overhear all vehicle communication in the network and may be able to find a vehicle location. Here global means the adversary, with the help of the radio transceiver, may collect and eavesdrop on the communication of a large part of the network. Passive means that the adversary may passively collect all the exchange messages during transmission. The main concern of GPA is to eavesdrop on location and driving paths to discover vehicle sensitive and personal information [61], [62]. The majority of the researchers consider GPA to analyze the location's privacy strength. Figure 3 contains an overview of the GPA for location tracking of a vehicle by analyzing location data and beacon messages broadcast in the network.

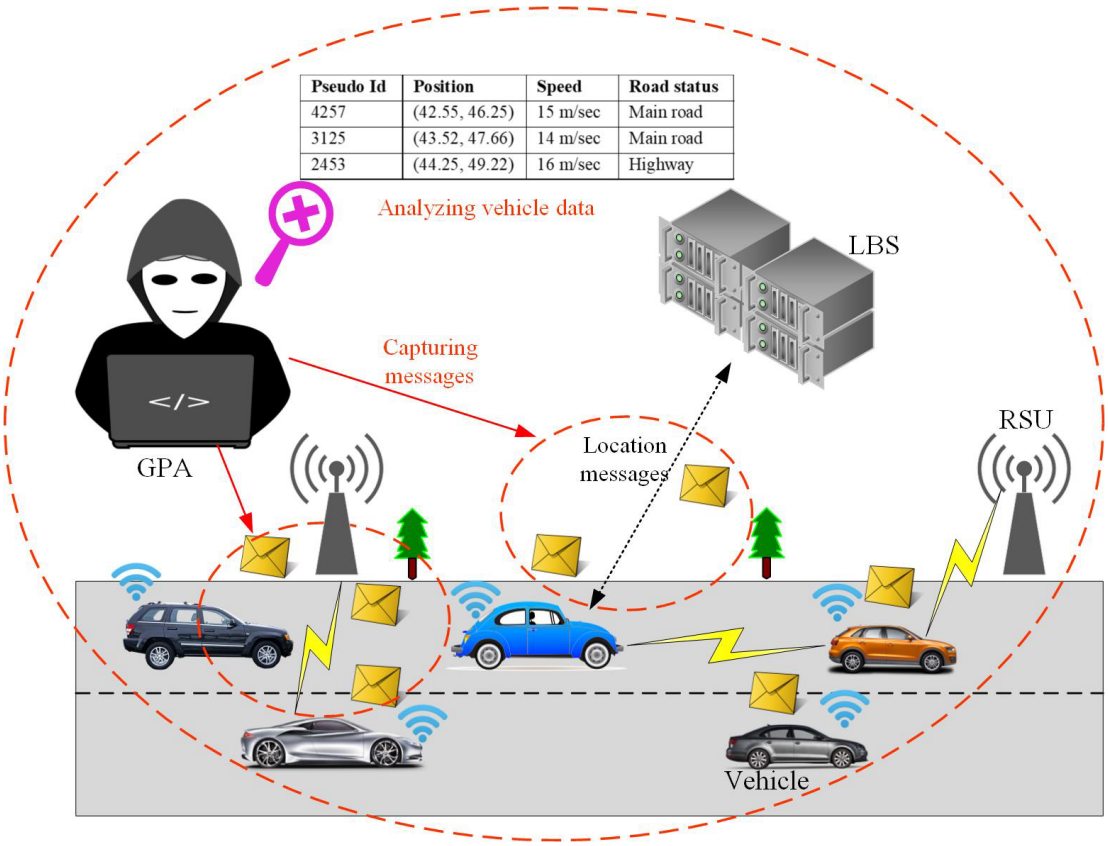

Figure 3 GPA vehicle tracking by analyzing vehicle data

f. Timing attack

The timing attack exploits the timing pattern of the message broadcast to infer the location movement of vehicles. The adversary did not alter the contents of the message during communication between nodes. The attacker adds an extra delay to the message delivery being transferred to the destination node. The timing information of mobile vehicles increased the knowledge of adversaries. The time mapping of the vehicle makes the possibility of linking the pseudonym with the real identity of the vehicle [63], [64]. For example, a vehicle broadcasts the change in its position and pseudonyms every second, the attacker monitors the regular timings of the broadcast messages. With the help of timing patterns and knowledge about the vehicle location habits provide a way for an attacker to deduce the location movements of a target vehicle.

g. Transition attack

In this attack, the adversary estimates the probability of a vehicle on each turn in a juncture based on prior observation. The attacker also kept a record of the transitions and pseudonym changes of a vehicle at the entry and exit points at the intersection. The attacker takes the help of historical data to guess the probability of vehicles taking certain turns or routes at each road intersection. Afterward, transition records are combined, and using estimated probability the attacker can link old and new pseudonyms of a vehicle [65], [48]. For example, a vehicle moving on the road changes pseudonyms at an intersection. The attacker has a record of previous patterns, transition records, and probability estimates about the concerned vehicle and tries to link the various pseudonyms used at different intersections. Thus the attacker could track the route of a target vehicle.

h. FIFO attack

If the vehicles have a fixed period in the mix zone and the mix zone does not assure an arbitrary period of time for vehicles that may be susceptible to FIFO (First in First Out) attack. The constant period inside the mix zone makes way for the adversary to link the new pseudonym of a vehicle with the old pseudonym. The vehicles come in and leave the mix zone in a FIFO manner, which makes the easy mapping of the pseudonym for adversary [66], [67]. For example, a vehicle enters a road intersection (mix zone), changes the pseudonym in the zone, and after a fixed time comes out of the intersection. The attacker notes the entry and exit timing of the concerned vehicle. Even, if a vehicle changes pseudonym in the zone, however using the noted records about vehicles, the attacker still can link and correlate the location tracks of a target vehicle at various segments of the road network.

i. Local active adversary

The local active adversary is restricted in its scope and covers a specific region of interest to capture messages communicated between vehicles [52], [54], [68]. This adversary takes the help of different parameters to track a vehicle such as transmission range and distance ranges between deploying units or vehicles. The adversary actively participates in the network to collect sensitive information for extracting the location of vehicles. It can transmit and receive messages, can inject and modify messages broadcast in the network for collecting information about vehicles. The local adversary actively interacts with other vehicles, monitors timing, transmission ranges, signal strength, and pseudonym change during broadcast messages in the network. Using this information, the adversary can link the pseudonyms of vehicles at various locations and able to compromise the location tracks of a vehicle.

IV. LOCATION PRIVACY TECHNIQUES

The location privacy concept in vehicular networks has evolved considerably over time. Initially, the main concern was the protection of the identity and location of vehicles on the road network which led to the development of basic location privacy techniques. At that time concept of the silent period integrated with vehicle grouping, and path confusion methods was introduced. Afterward, more sophisticated location privacy techniques emerged such as random silent period methods, mix zone concepts, cryptographic mechanisms, obfuscation mechanisms, pseudonym exchange processes, etc were introduced. Still, more advanced research continuous in protecting location privacy in VANETs. We devise a timeline of location privacy schemes in vehicular networks shown in **Error! Reference source not found.**.

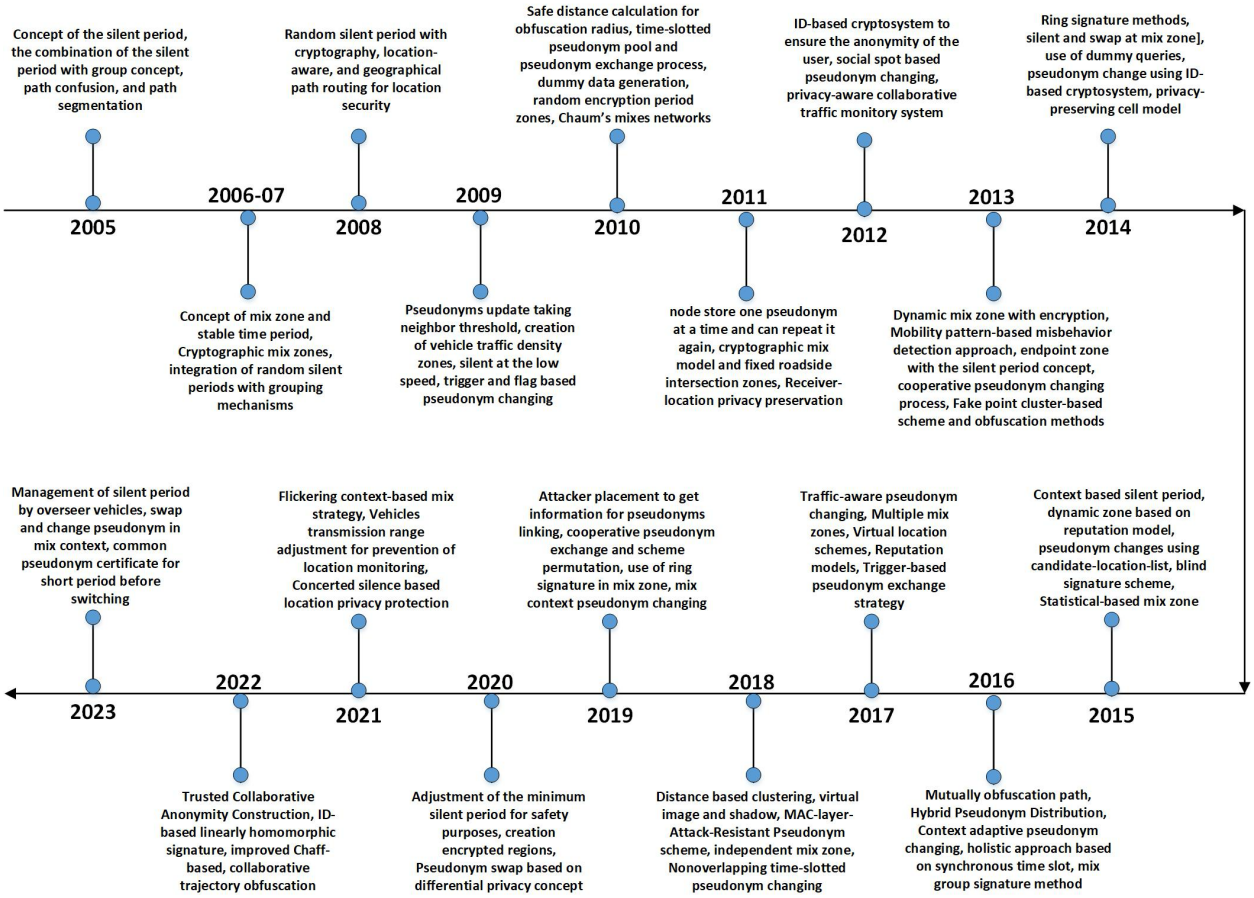

Figure 4 Evolution of location privacy in vehicular network in different periods

To solve the problem of location privacy in the case of VANETs, various techniques have been offered in the literature. The core concern of these techniques is to use the pseudonym in the beacon instead of the actual identity of the vehicle. The pseudonym must change properly at the proper time to conceal the actual identity of vehicles in the network. The existing research work considers one or two road network scenarios to apply the pseudonyms-changing process for location protection. However, it is challenging to provide location privacy in such a diverse network condition and environment. For this purpose, we divided location privacy schemes into various categories. The various categories of location privacy techniques are shown in Figure 5. Useful details about the various location privacy techniques are given in the following subsections.

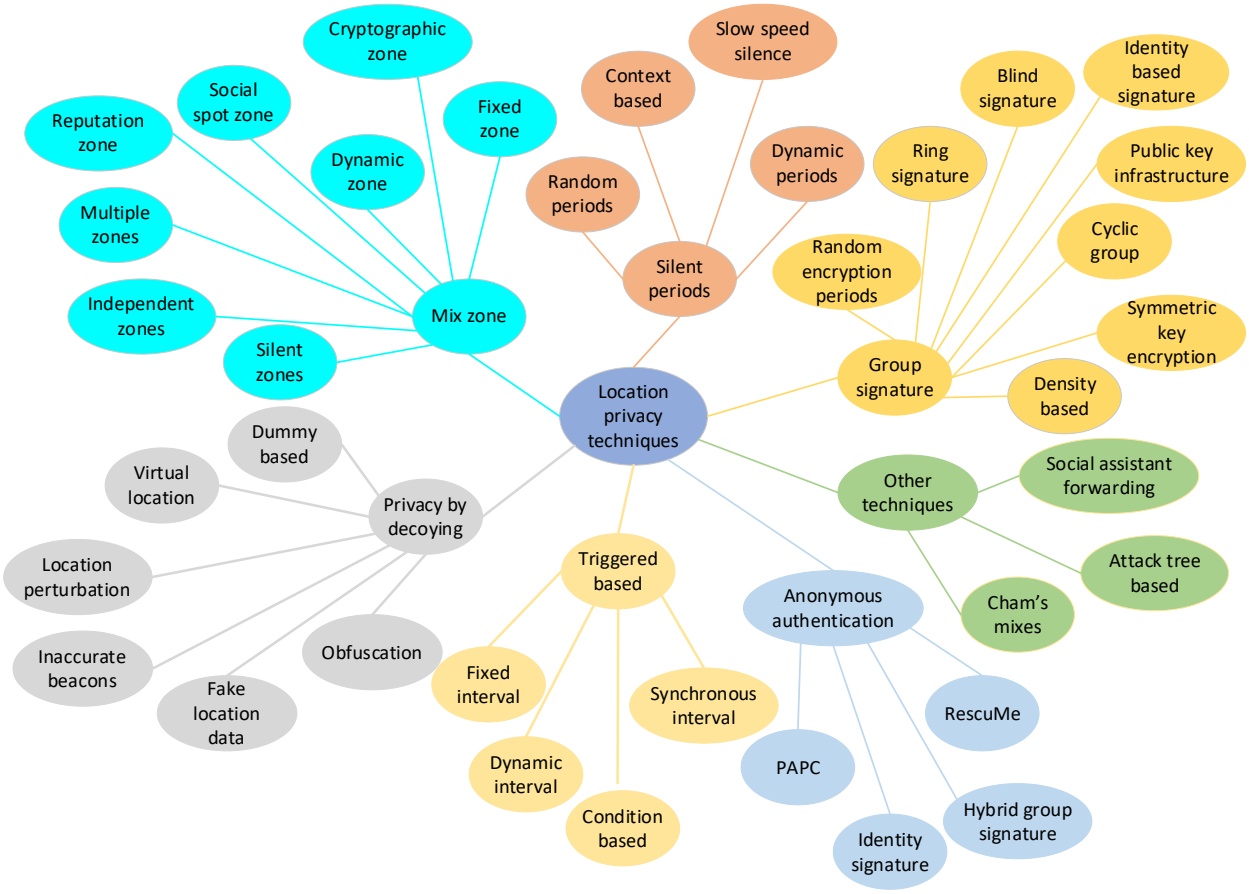

Figure 5 Categorization of location privacy technique in VANETs.

A. Mix zone-based location privacy techniques

The mix zone idea is firstly proposed in [69] for the field of pervasive computing for anonymous communication. The concept is taken from Chaum's mixes network [70], in which the correspondence between input and output is kept hidden. A Mix zone is a region usually constructed at the roadside or at a social spot, where many vehicles get together. Vehicles change or exchange their pseudonyms in that region, which obscures the identities of each vehicle. This generates a major difficulty for an adversary to recognize the movements of vehicles in the region, which preserves the privacy of vehicles. In [38], context information of vehicles is collected, such as the number of neighbor vehicles, speed, and direction for changing pseudonyms. Later on, other context information is taken in [71] such as the distance among vehicles, speed, and road section information. A vehicle uses a flag value and waits for the least k neighbor vehicles for pseudonyms changing. Similarly, the paper [72] uses three factors such as pseudonym age, vehicle speed, and direction of vehicle movement to change pseudonyms.

The notion of a cryptographic mix zone (CMIX) protocol is presented in [73], where vehicles collectively change their pseudonyms using cryptographic techniques. The CMIX enhanced the basic mix zone idea by integrating the cryptographic mechanisms (encryption, key exchange) in the zone. Cryptographic zones provide robust privacy protection through cryptographic methods, however, these techniques are more complex and require higher computation delay compared with the basic mix zone concept. RSU provides symmetric keys to legitimate vehicles, and vehicles encrypt all messages in the zone with the symmetric key. The combination of a mixed network with a mix zone provides pseudonym unlinkability. Another mix zone protocol based on the cryptographic concept is proposed in [74]. The RSU manages the mix zone by periodic beacon messages in the network to inform the vehicles about the mix zone area. These messages contain the position and radius of the mix zone. The cryptographic-based privacy schemes add an extra delay in message dissemination that is overhead. Another variation of CMIX in [75] implemented

vehicle public infrastructure protocol to solve the issue of linkability. Messages of a vehicle are signed with a different pseudo-identity. In case of low traffic conditions fake messages are disseminated to provide unlinkability outside of the zone.

The term social spot is used as a mix zone to change the pseudonym of the vehicles [76]. A social spot might be a parking portion, roadside intersection, etc. The vehicle change pseudonym is accomplished while entering or leaving a social spot. Another strategy based on the social spot for changing pseudonyms randomly is introduced in [44] which provides location protection both at large and small social spots. These social spots become mix zones where a huge quantity of vehicles meet together. The concept of a location privacy zone is constructed at roadside infrastructures such as toll booths and gas stations [77]. In these zones, the pseudonym of each vehicle is changed randomly. In [78], the mix zone area is divided into square sections called Endpoint Protection Zone (EPZ). The users in EPZ share login credentials and keep silent during that period. EPZ's anonymize the users in the protection zone and provide privacy. Users have protection only in these zones; however, they remain vulnerable to location privacy attacks outside of it.

A vehicle is said to be selfish if it does not cooperate with other vehicles in the pseudonym-changing process. This selfish behavior is due to limited resources such as the limited number of pseudonyms and bandwidth. The selfish behavior of vehicles might cause danger to the location privacy of other vehicles in the network. For example, there are ten vehicles in a mix zone, and two out of ten change pseudonyms while the eight vehicles do not change pseudonyms due to selfish behavior, the attacker comes to know only two vehicles change pseudonyms, thus can link the new pseudonym of a target vehicle to the old pseudonym by some random selection among two vehicles with a probability of 0.5. For controlling the selfish behavior of vehicles, a dynamic mix zone-based strategy (MPSVLP) is offered in [79]. A reputation model is developed, which inspires vehicles to collaborate in the creation of a mix zone for the protection of location data of vehicles. The control server is used to control and synchronize the pseudonym-changing process. The concept of a dynamic mix zone is also developed in [45] to hide the location information of a vehicle. Here, a mix zone is constructed at the request of the vehicle. In the zone area, the messages are encrypted during transmission to hide the association between the pseudonyms of vehicles at different periods. The dynamic mix zone is improved with the collection of candidates' location lists [39]. The vehicles are divided into various slots, and vehicle traffic information is collected. Based on the collected information, the decision is taken that slot vehicles should change pseudonyms. The effectiveness of the mix zone is measured with the use of a statistical metric in [80] for the improvement of the location privacy of vehicles. The vehicle should pass over a mix zone, and the additional overhead is kept minimum for adjusting the zones. Dynamic grouping and virtual pseudonym change technique is introduced in [81]. A group of vehicles is formed based on similar-status vehicles on the road and pseudonyms are changed cooperatively. A virtual pseudonym change process is applied in case of low vehicle density, where some randomized versions of pseudonyms are generated to create uncertainty for an adversary about the true location of vehicles.

A reputation-based model is introduced in [47], [82], for the change of pseudonyms in the mix zone. It offers an incentive to the vehicle and encourages them to cooperate in the pseudonym-changing process. Another model of vehicle location privacy zone based on the reputation to encourage the vehicles to join the privacy zone is introduced in [83]. The invitation request is broadcast in the network to motivate the vehicle to join the privacy zone. If the response is positive, the reputation of a vehicle is increased; otherwise, on a negative response, the reputation is decreased. The departure order of the vehicles from the privacy zone is random which increases the difficulty for an adversary to recognize the target vehicle. One of the privacy threats is an adversary's knowledge of the temporal metric. The spatiotemporal factor of the mix zone is addressed in [63] to guard against velocity and timing-based attacks. The temporal factor considers the traffic flow and time-dependent and time-independent aspects of the mix zone.

The idea of pseudonym change in the mix zone is extended to multiple mix zones in the vehicular network for location protection [66], [40]. The vehicles request two endpoints on the map hiding the actual location from the location server. The endpoints should be placed on the map so that it protects the location information and provides a location service convenience. Later on, the notion of a Reported Server (RS) is presented in [82] for dynamic pseudonyms changing at multiple mix zones. RS allocates virtual identity and pseudonyms to vehicles which hide the real identity of vehicles. A new pseudonym-changing approach is introduced in [57] for vehicle trajectory protection in multiple mix zones. It helps vehicles against cheating attacks. Vehicles change pseudonyms collaboratively in the zone area which safeguards the vehicle from pseudonym linking attack. In [49], a fixed mix zone concept is introduced to change the pseudonyms of the vehicle in that fixed area. These zones are established and spread over the road network. This method works against a pseudonym linking the attack to conceal the real identity of the vehicles. A new location protection scheme based on the construction of a dynamic virtual mix zone is introduced in [84]. This zone is created dynamically when the pseudonym of the vehicle is about to change. The reputation model is developed to convince the joining of

selfish nodes. This idea is extended in [50] to construct an independent mix zone scheme for the location secrecy of vehicles in VANETs. This scheme works well even in low traffic density. For low traffic density, vehicles generate fake pseudonyms.

Another variation of the mix zone is the introduction of a silent mix zone, silence, and swap at an intersection [85]. Two protocols are used in this approach: one protocol is designed for the creation of silent mix zones, and the other is for the exchange or swap of pseudonyms in these zones. The vehicles remain silent in the zone area, and out of the mix zone area, the vehicles begin to interchange pseudonyms randomly with each other. The idea of a silent mix zone is further extended in the Traffic-Aware Pseudonym Changing Strategy (TAPCS) for location protection [36]. The radio silence technique detects appropriate traffic conditions for pseudonym change. The traffic congestion situation is the most suitable environment for TAPCS. In [37], a silent mix zone is improved with a safe mode and introduced an urban pseudonym-changing strategy. The vehicle may use either the pseudonym-changing protocol or pseudonym exchange protocol based on the condition of the network. An independent and cooperative pseudonym exchange protocol in a mixed context is offered [86] without the infrastructure support to enhance the location privacy of vehicles. Then the pseudonym exchange is reported to the authority to ensure accountability and non-repudiation. A Mac layer attack resilient pseudonym policy is introduced in the context of VANETs to guard against a new MAC layer context linking attack [87]. It changes the pseudonym adaptively and accesses the wireless channel in distributed mode. One limitation of this strategy is that When the traffic density is sparse vehicle enters to longer silent period.

Remarks: Based on the detailed discussion on the mix zone-based privacy techniques, we explored some of the necessary limitations of mix zone-based techniques. Although the mix zone provides location privacy protection to some degree, however, there are some problems associated with the mix zone conception. First, the mix zone reduces the location privacy level under lower traffic conditions, if there is a lower number of vehicles in the region, fewer vehicles would change their pseudonyms which does not provide a higher level of vehicle anonymization. Second, vehicle privacy is provided only in the zone and there is no privacy guarantee outside the mix zone. Third, real-time location security is not provided in the mix zone [88]. The identity hiding is only connected to the zone as a vehicle may pass on different roads and regions. Consequently, each vehicle must wait for a mix zone creation to change pseudonyms which affects the privacy protection level.

B. Concept of Silent period based location privacy methods

The silent period concept is introduced in [89] to enhance wireless location privacy. It is a transition period in which the mobile node remains silent for a certain period. Afterward, the expiration of the silent period, the mobile node begins its communication with the surrounding nodes. Later on, the silent period concept is used in VANETs for location privacy protection. In a silent mode, each vehicle stays silent by not broadcasting messages in the vicinity and changing pseudonyms during this period. This breaks the link between the vehicle identity and the location tracks which preserve the privacy of vehicles. For the protection of location privacy in VANET, Sampigethaya et al. [69] presented the idea of a silent period, combined with the grouping mechanism[90]. Each vehicle changes pseudonyms in a group and remains silent for a certain period. Privacy threats are avoided with the help of an anonymous access control protocol. The random silent period concept is presented in [51]. A Group Leader (GL) is selected and after that, GL combines vehicles in a group. The GL is the front-line representative who interacts with other entities in the network, while the group members remain silent. A SafeAnon privacy preservation method is introduced in [91] based on safe distance calculation with the help of a kinematic analysis algorithm. In this scheme, the real value of the vehicle location position is disturbed to confuse the adversary. The random silent period concept is used in which the vehicle remains silent for random periods. Another random silent period based location privacy approach is presented in [92]. In this technique, pseudonyms are used for authentication and anonymous access. The complete trajectory is hidden with the help of changing pseudonyms. Autonomous Location Update Mechanism (ALUM) is used to trigger a location update without relying on a trusted authority.

The different adversary capabilities are addressed to protect privacy vehicles in [93]. The pseudonym update mechanism depends on the neighbor's crowd and adversary capability rate. If the neighborhood ratio is below a certain threshold, the vehicle cannot update pseudonyms and remain silent in the network. SLOW (Silent at low speed) [94] a location privacy scheme without infrastructure support is introduced. The vehicles make their mix zone without RSU support. The vehicles are silent at low speed and do not transmit heartbeat (beacon) messages during this time. It would hide the identity of vehicles and reduce pseudonym-changing overhead during the silent period. A new approach to location privacy is introduced in [53] that consists of two schemes. In the first one, the network is divided into various cells which contain a few city blocks, and have a list of a pseudonym for that specific area. Secondly, pseudonyms are issued to each vehicle on request. The use of a silent zone breaks the linkage between

various pseudonyms of vehicles. In [95], a concerted silent-based privacy scheme is proposed in which vehicles cooperatively enter a silent period and change pseudonyms simultaneously. A safety-aware location privacy scheme is proposed in [96] where the concept of an overseer vehicle is introduced. The overseer vehicle takes care of vehicle safety and allows vehicles to enter a silent period to enhance location privacy. Another safety-related location privacy mechanism is given in [97] which the silent period is reduced without affecting the privacy level. The vehicle continuously monitors neighboring vehicles, if there is a chance of an accident, the silent period is exited and starts sharing location information.

A pseudonym-changing strategy is based on a mixed context, in which the vehicles change pseudonym, enter to silent period, and leave the silent period based on context information [98]. The vehicles enter the silent period taking the help of the silent mode of surrounding vehicles. It increases vehicle power against tracking attacks. The efficiency of [98] is improved by adjusting the minimum silent period with the increase in the number of exchange messages which also improves vehicle safety level [99]. A Context Adaptive Privacy Scheme (CADS) is offered in [52], in which the vehicle of VANETs decides autonomously when to change pseudonyms and when to remain silent for some period to ensure the un-likability of a pseudonym. Based on traffic density and user privacy preferences, the scheme adapts dynamically. In [43],[54], a location privacy scheme is presented that comprises two parts: The first one is the pseudonym-changing process which permits vehicles to change pseudonyms. The second portion protects vehicles from cheating attack. Similarly, a cooperative context-based hybrid scheme is introduced in [100] that combines two existing techniques, i.e., CAPS and Cooperative changing pseudonyms that take the number of neighbors in the vicinity. Another context-aware and traffic-adaptive scheme is proposed in [101] which finds a suitable situation to change pseudonyms using context and traffic pattern information that increases the anonymity of vehicles.

The switching periods of pseudonym certificates are managed between vehicles [102]. Each vehicle uses a common pseudonym shared with them for a short period to sign messages. After the expiry of a short period vehicles switch to new pseudonyms which improves privacy protection level. A flickering context-based mix method is given in [103] for the protection of privacy in VANETs. In this scheme, a random number is generated, if the random number is less than some threshold, vehicles will broadcast with new pseudonym otherwise will remain silent and wait for next broadcast. The context-based existing schemes only consider the silent neighbor vehicles to change pseudonyms in silent mode. However, it has certain limitations: the first one is, these schemes have effects on VANETs application. Secondly, the straight road structure and short silent assist a way for an adversary to detect the target vehicle. Thirdly, the subject vehicle knows the old pseudonym of a neighbor vehicle, which provides a way for pseudonym linkability. Similarly, on the expiry of the waiting time, if the subject vehicle does not find a silent neighbor, it will change the pseudonym individually, and the individual behavior vehicle can be easily identified.

Remarks: After a careful study of silent period-based location privacy schemes we found certain limitations. These techniques provide location privacy but have an impact on VANETs application services such as safety applications. Suppose a vehicle remains silent during an emergency, i.e., in case of an accident, the vehicle is unable to disseminate the message in such types of events, which is an essential requirement of VANETs.

C. Group Signature-based location privacy techniques

The group signature idea is introduced for the first time in [104] that hides the signature of an entity in the group. A group of vehicles is formed using road context information, in which the broadcast message is signed with a group key and the sender key, which anonymizes the sender of the message in the group. The receiver could only verify the signature but difficult to recognize the signer of the message in the group. In group signature techniques cryptographic methods are used to improve the location privacy of vehicles. A trusted authority produces group keys that consist of public keys and secret keys. The public key is used for verification and secret keys are for group members. The secret key is given to each member upon joining the group and members of the group use this secret key to create a group signature on the message. The signature shows the validity of each member and hides the individual identity of the member. The group signature provides anonymity and unlinkability to individual vehicles in the group. The signature hides the actual identity of the signer of the message in a group and multiple signatures of a group member can't be linked to the same member which offers both anonymity and unlinkability.

Before discussing the various existing group signature mechanisms for location privacy in VANETs, there is a need to talk about different cryptographic methods used in group signature schemes. These cryptographic methods are public key cryptography, identity-based signature, blind signature, and proxy re-encryption schemes. In public key cryptography, a vehicle contains two keys public and private, the message is encrypted with the receiver's public key and decrypted with their private key [105]. Each vehicle

encrypts the location message with the public key and this message can be only decrypted by the intended recipient, which prevents an adversary from determining the location and identity information of a vehicle. In identity-based signature schemes, user identity attributes (unique identifiers) such as email, phone no, or IP address for signature creation and verification instead of digital certificates [106]. The TA takes the unique identifier of a vehicle to generate a private key for it. Using the private key a vehicle signs a location message and the receiver of the message can verify the sender but can't reveal the actual identity of a vehicle in that region.

In the blind signature scheme, the message is disguised (blinded) before it is signed. The signer can't learn about the contents of a message [107]. In the case of the vehicular network, each vehicle blinded the content of the location message before sending it to the signature authority. This ensures that data can't be linked to a specific vehicle by authority. Later the blinded message is unblinded to acquire the valid signature. The proxy re-encryption scheme is a peculiar kind of public key encryption in which a proxy (intermediate authority) converts an encrypted message from one public key to another, even the proxy can't get information about the original message [108]. In a vehicular network, a vehicle encrypts location messages or data with its public key, the proxy re-encrypted it with another vehicle public key. This process ensures that only the intended receiver can decrypt and access the location data, which hides the identity and location of a target vehicle in the region of interest. In the following passage, various group signature schemes based on cryptographic methods are discussed.

One of the group-based techniques Random Encryption Periods (REP) [56], is offered in which messages are encrypted at random intervals of time to protect the location of vehicles in the network. REP creates encryption zones to guard vehicles against tracking by an attacker. Another privacy scheme based on a random encryption period is proposed in [109]. When a vehicle changes pseudonym, other neighboring vehicles encrypt all the communication using a group key, which prevents an adversary from accessing the sensitive information. A privacy-preserving approach is presented in [110] using cryptographic mechanisms, which provide a balance between privacy and accountability. Two strategies are introduced for privacy preservation, i.e., V2I and V2V privacy-preserving protocols. V2V communication is done in groups using the concept of group signature and hides the identity of the vehicle in a group. Vehicles are fitted with a short live pseudonym for encryption and digital signing.

A pseudonym-changing scheme based on ring signature verification is introduced for location privacy [111]. The vehicles randomly form a ring with neighbors' vehicles and anonymously sign the messages. This procedure hides the identity of vehicles in the ring and provides revocability by the authority. The blind signature-based scheme [41] is proposed in which vehicles generate short keys for different lifetimes. Blind signature is used to build trust between vehicles and RSU. Vehicles change their key based on the behavior of neighbors. Two spots are considered, one is a traffic signal, and the other is a social spot. The frequent change in pseudonyms is done at the collective spots. A revocable group signature privacy scheme based on the Chinese remainder theorem and a digital signature algorithm is offered in [112]. This scheme not only provides anonymity to vehicles but also provides traceability service to TA.

The group signature is combined with the identity signature in [113] for privacy in VANETs. In this scheme, the sender signs the message with a group signature, and then for authenticity, RSU signs the message with an identity signature. It also provides traceability in case of a dispute. Another identity signature scheme of social evaluation techniques is based on the group signature for location privacy protection [114]. This technique evaluates vehicle sociality by not disclosing the history of location information. It supports socially aware data diffusion to preserve privacy. The social witness collection is used to evaluate the social history of vehicles. An optimized conditional privacy preservation model is proposed in [115] for the vehicular network. It includes an ID-based cryptosystem, which ensures the anonymity of the user by considering the pseudonym concept. In this model, the authority could trace the vehicle in case of dispute and misbehaving users. Another ID-based cryptosystem location privacy scheme [116] is developed in which the pseudonym of the vehicle is changed synchronously to increase vehicle anonymity in the network. The ID-based linearly homomorphic signature scheme is offered by [117] which supports pseudonym changing process under various conditions to protect the location information of vehicles.

In [42], a one-time identity-based authenticated asymmetric group key agreement (OTIBAAGKA) is proposed for the creation of the Cryptographic Mix-zone (CMIX). The beacon messages of the vehicle are encrypted with the help of a secret group key. Any vehicle could be used as a distributor of a secret group key. One time pseudonym is used to preserve vehicle privacy. Another location-sharing technique based on an identity signature is introduced in [118]. A central manager is used as a broker between RSU and the vehicle, which keeps vehicle location trajectory data. The ID-based proxy re-encryption scheme protects vehicle

location data not only from unauthorized users but also from the central manager. Only legitimate RSUs have access to location trajectory data.

A group communication-based privacy scheme called Anonymous Online Service Access (AOSA) [119]. The main purpose of this scheme is to get online services through RSU anonymously. Public key infrastructure is used for message authentication and verification in a group manner. A synchronized group-based pseudonym-changing scheme is introduced [120] to improve unlinkability for location privacy. Asymmetric keys are used for the authentication of the message. The group is formed among the neighbor vehicles to anonymize in the network. Another technique of public-key cryptography scheme mobility pattern-based misbehavior detection for the security and privacy of a vehicle is suggested in [121]. A pseudonym issuance approach is introduced in [122] based on advanced cryptography (public key) to protect user anonymity against colluding backend providers. The two core stages are the obtain-pseudonym phase and the revoke phase. While obtaining a pseudonym, the vehicle remains anonymous. The vehicle identity is exposed if the vehicle violates the rules of protocol or requests for more pseudonyms.

A group signature scheme is deployed for authentication, integrity, and prevention from outsider attacks. To further increase, the complexity of an adversary novel location privacy technique is designed in [123], which is based on the mix group idea in the vehicular social network. Different social spots are combined to make an extended social region. The vehicle could change the pseudonym in these social regions that mix the identities of the vehicles. A hybrid group signature authentication mechanism to protect location privacy is proposed in [124]. The authentication is used as a dynamic hiding cover for pseudonym changing. One of the vehicles in the network, group the vehicles and changes the pseudonym cooperatively. The strategy of pseudonym changing at a proper location changes the pseudonym of the vehicle at the proper location, and the proper time to guard against location privacy attack is proposed in [125]. A data forwarding protocol IsPride is presented in [126] to protect the privacy of vehicles in VANETs. This mechanism is based on the social behavior of the vehicle. The vehicles forward messages to RSU efficiently with a high delivery ratio. Privacy is preserved with a group signature scheme using anonymous authentication.

A new concept of defending and attacking zones is presented in [127]. Encryption is used instead of radio silence and creates difficulty for an adversary to identify pseudonyms of vehicles. The intrusion detection system is deployed to protect the network from the attacker. A specific area called the defending zone is designated for vehicles, where all communication is encrypted to guard against linking attacks. Song et al. proposed a vehicle density-based location privacy approach [128], which utilizes vehicle-neighboring density as a threshold for changing pseudonyms in a group manner. Each vehicle changes its pseudonym when there are at least k-1 neighbors in the network. The Delay model is developed at a density zone to identify the tracking ratio of the adversary. A general cooperative framework of pseudonym change is introduced in [31] for the anonymity of the vehicles. Distance between vehicles is calculated, and vehicles in distance R are considered neighbors of a vehicle. The vehicle changes the pseudonym in a group in a cooperative manner. In [129] paper, a distributed algorithm is proposed for the election of a cluster head based on distance and clustering approach. The proposed method provides stable and balanced clustering to increase network lifetime. The cluster head implements the pseudonyms-changing process using the distance and energy of cluster members.

Remarks: The weakness of the group signature technique is the management of group size, i.e., the number of members in a group. A large number of members in a group are difficult to manage, while with small members in a group, the adversary can easily reveal the location information of the vehicle driver [40]. The group size must be in between large or small numbers, to provide efficient location privacy for VANETs users. In addition, there are some situations where it is challenging to implement a group signature scheme, i.e., under low traffic conditions (lower number of vehicles in a vicinity). The group-based strategies required collaboration from its neighbors, and if a sufficient number of neighbors or vehicles were not available at that time, difficult to manage a grouping scheme in this situation. The use of encryption schemes in the group signature methods increases communication delay and computation costs in the network. The signature generation and verification consume computation time which increases the time overhead in the network.

D. Time-slotted and triggered location privacy techniques

The basic concept of time-slotted and triggered-based privacy techniques is the change of pseudonyms of vehicles under meeting some conditions such as a specific period is expired, vehicle density threshold, lane change condition, etc. The vehicles started to change pseudonyms on the expiry of a time slot. For this purpose, a method for location privacy that takes a time-slotted pseudonym pool is introduced in [130]. Vehicles also exchange pseudonyms with a suitable node or vehicle in the network. This exchange process depends on the similar speed, position, and headings of the vehicles. In [131], the node only stores one pseudonym at a

time t. When this time slot is expired, every vehicle must change its pseudonym. Vehicles may also use the old pseudonym repeatedly for the same time slot on that day. It reduces the pseudonym storage cost of a vehicle. A dynamic privacy-preserving key management approach is presented, called DIKE in [132] for vehicle location services. For the double registration of vehicles, the authentication mechanism is applied. The session of LBS is divided into numerous time slots in which each time slots hold diverse session keys. A one-way hash function is used for session key updates.

A structured approach based on the holistic solution is proposed to protect location privacy [46]. A synchronous time-slotted pseudonym pool is used to reduce storage overhead and maximize adversary confusion. The pseudonym change is visible to direct neighbors to reduce the negative impact on the user's safety without sacrificing privacy. In addition, time-slotted work is efficiently defined to preserve backward privacy. Another synchronized time-slotted based pseudonym change scheme is proposed in [133] to solve the privacy-safety problem. Multiple pseudonyms are used during communication that are valid at any given time. The change in pseudonyms is visible to neighbors to reduce the negative impact on user safety applications. Similarly, a time-slotted pseudonym change scheme efficiently works with revocation schemes. In the [134] paper, a trigger-based pseudonym exchange mechanism is introduced for location secrecy in VANETs. When two vehicles trigger each other based on similar velocity and header, they exchange pseudonym vide RSU to CA. The pseudonym exchange and revocation are done with the support of the Certificate Authority (CA).

Remarks: The drawback of these techniques is that if an adversary gets the slotted periods of vehicle pseudonyms change. It will provide an opportunity for the adversary to link the pseudonyms of a target vehicle at various visited locations. This offers a means for an adversary to know about vehicle driver behavior at different locations. Another difficulty of these techniques is the synchronization of the time slot for pseudonyms changing of various vehicles in a vicinity. The other drawback is the visibility of a vehicle pseudonym to direct neighbors may provide a way for a malicious insider to associate various pseudonyms of visited locations of a target vehicle.

E. Location perturbation privacy techniques

Location perturbation privacy techniques add uncertainty to the information broadcast in the network. The uncertainty may be dummy data, path confusion, and broadcasting inaccurate location data in the communication network. The use of dummy data or inaccurate information creates difficulty for an adversary to recognize a target vehicle location information. In [58], a routing protocol that uses dummy location data is introduced. The routing choice is taken based on dummy distance to destination data in place of the actual vehicle location. Dummy location data is broadcast, and the real location data of a vehicle is hidden in it. A fake point cluster scheme [135] [136] for physical layer location protection prevents the attacker from extracting user location in NEMO based hot spot. The error in the received signal increases the confusion of an attacker and hides the actual position of the user. The selection of fake points is made randomly in the hotspot. In [137], a decoy is added to the message during communication with LBS. The real location of the vehicle is altered with a decoying location to increase uncertainty for a location update request that protects the location of vehicles.

A perturbation algorithm for location protection is introduced in [138]. For cross-path confusion, at least two users meet to exchange location data with each other. Therefore, it increases the confusion of an adversary and reduces the tracking of the actual location of the user. For location perturbation, a Nonnegative Matrix Factorization (NMF) is designed in [139]. NMF is a dimensional reduction method used in many applications such as privacy preservation, clustering, and text mining. NMF breaks down a matrix into two lower-rank matrices and all elements of the matrix are nonnegative. For location privacy, NMF decomposed location data into potential factors, and the actual location data is not directly represented in the matrix. This anonymizes the location information and creates difficulty for an adversary to extract actual location data. In VANETs, NMF clusters the driver's events according to directions, locations, and distances, which preserves the private information of drivers. Inaccurate beacon messages are added in between the accurate beacons while broadcasting in the network periodically [140]. Then the group communication method is applied to secure broadcasting messages from the attacker listening. The inaccuracy in beacon messages raises the confusion of the adversary to track and link the pseudonyms of vehicles in the network.

A new idea of dynamic virtual location is presented in [141] to hide the actual position of the vehicle. The location trajectory is blurred with route confusion by adding the virtual location of the neighbor vehicle. This technique is extended in [88] to produce a virtual location dynamically of the neighboring vehicles. The communicating vehicle sent two queries to LBS for location updates with two locations one is the real location, and the other is the virtual location of the surrounding vehicle. This increases uncertainty

for an adversary in information extraction. A Mutually Obfuscating Paths (MOP) technique is proposed in [142], in which the vehicle position tracking is protected from LBS. In MOP, vehicles generate plausible location updates for one other to branch off the continuous paths for LBS. Vehicles take the help of inter-vehicle communication to obscure location tracking via in-car Internet access while using LBS. These techniques are improved with the introduction of a multi-level obfuscation method that generates duplicate messages taking the help of transmission range vehicles to anonymize the identity and location of vehicles [143].
The paper [144] combines vehicle crowd and obfuscation mechanisms to prevent linkability and continuous trajectory of vehicles. A collaborative trajectory obfuscation mechanism is offered in [145] which the attacker model is analyzed and an efficient privacy design metric is introduced to balance privacy and its cost. A query-based dual privacy protection scheme is introduced [146] for communication models of VANETs. The vehicle applies a circle-based algorithm to generate dummy location data to communicate with LBS. The location perturbation technique taking differential privacy concept is designed in [147] to provide location privacy. The main concern is to add noise to the position of vehicles for location perturbation. A similar scheme based on the differential privacy concept is proposed in [148]. The Laplace approach is taken to add noise to the user location while sending a query to LBS. Another technique based on differential privacy uses the idea of reinforcement learning to randomize the locations released by the vehicle [149] to protect the semantic trajectory of the vehicle. A pseudonym swap process using differential privacy is given in [150] where RSU calculates the driving similarities between vehicles. Using the similarities and probability sampling vehicles obtain new pseudonyms through the swap process which provides unlinkability to vehicles.
Remarks: The leading shortcoming of these techniques is the generation of extra overhead in the network by using dummy data. For example, if a large amount of dummy data or information is used for the safety of vehicle position information that will create a higher overhead in the network. Similarly, the use of dummy data affects road safety applications of VANETs and does not efficiently utilize the location service utility. If wrong information in the network is discriminated in the network, how will the members of the network utilize the safety services?

F. Anonymous authentication techniques

Anonymous authentication is the process in which a user or node is authenticated without revealing its identity in a network. Anonymous authentication techniques can be used to hide the location information of vehicles. A conditional privacy preservation protocol for anonymous authentication is proposed in [151]. The protocol generates short anonymous keys between OBUs and RSUs to offer anonymous authentication and privacy protection. The pseudonym Authentication based Conditional Privacy (PACP) method is presented in [152] for privacy protection in VANETs. This technique uses a pseudonym as a substitute for the actual identity of the vehicle. For anonymous communication, the vehicle interacts with RSU to generate a pseudonym. A revocation mechanism is used to revoke a vehicle from the network in case of misbehavior. Sun et al. proposed a new security method RescueMe for the location-based vehicular network to aid security and rescue arrangements for the provision of rescue resources [153]. In this technique, the location information of the user is stored for post-disaster planning during normal network conditions. The technique guarantees that no sensitive information about user location will leak. Park and Rhee introduced a secure and location assurance protocol for authentication and location privacy in location-aware services of the vehicular network [154]. The authors used the pseudonym change and identity signature to conceal the location information of users. The pseudonym change provides an efficient anonymous authentication privacy-preserving location-aware service. A hybrid group signature authentication mechanism is proposed in [124] location secrecy. The authentication is used as a dynamic hiding cover for pseudonym changing. One of the vehicles in the network group the vehicles, and pseudonyms are changed cooperatively. The authentication mechanisms used for vehicle privacy have certain issues and problems, i.e., they create extra delay for the generation of short anonymous keys and the use of asymmetric cryptography generates high computation cost in a network.

G. Other location privacy techniques

There are some other location privacy schemes in the context of VANETs that do not fall into any one of the above categories. That is why we made a separate section for these schemes. The purpose of these approaches is to hide the location information of vehicle drivers. We discuss these location privacy techniques in the following passages.
A geographically secure routing protocol is proposed in [155], that prevents distraction produced by malicious nodes. The anonymous node locations are authenticated to provide location privacy and authentication. A social tier-assisted packet forwarding protocol is introduced to hide the receiver location information in VANETs [156]. The protocol exploits the people's lifestyle and

features of the social tier in a vehicular network. The protocol has four phases to work on, i.e., the initialization phase, the packet-sending phase, the social-tier dissemination phase, and the packet-receiving phase. One symmetric encryption AES and two cryptographic hash functions are used. A new architecture is proposed in [157] by integrating Chaum's mixes with distributed infrastructure based on location-based services for privacy preservation. The user has the choice of when to reveal the location to anyone and when to hide the location. No entity in the network has full knowledge of the location of the user at any time. A suite of new location security mechanisms was introduced in [158]. The user will connect to a single RSU at a time, and the RSU will assign a new pseudonym each time when a data packet is sent to him. In this secure system, the drivers and passengers easily access the required data without compromising system security and privacy.

In [159], a risk assessment based on the attack tree is presented to calculate the privacy risks of the vehicular network. The attack tree is constructed to identify possible attacks on user privacy. This technique also calculated the degree of impact of specific threats to vehicular system privacy. In the [160] paper, an analytical model is presented for a simple random pseudonym change scheme to improve location privacy level. Two distributions, i.e., uniform discrete and age-based distribution, are analyzed and compared. Results show that uniform discrete distribution is better than age-based distribution to improve the privacy of the user. A general analytical model is proposed for Random Pseudonym Change (RPC) for location protection [161]. Various parameters are considered to quantify the RPC strategy based on the expected size of anonymity set under uniform and reciprocal distribution of pseudonym lifetime. The impact of the age of the pseudonym used by a neighbor to conditionally pseudonym change with its neighbors is also discussed. Simulation results verify that the uniform distribution of pseudonym lifetime improves location privacy. In [33], the notion of the phantom node is used to provide location secrecy of the source node in the vehicular network. First, phantom selection is considered a multi-criteria problem, and the network analytical process solves this problem. Various parameters are considered for phantom node selection, i.e., distance, speed, trust, acceleration, and direction. The nodes in the network are ranked based on these parameters from best to worst. The most suitable node is nominated as a phantom node. A hybrid pseudonym distribution method is proposed in [162], in which both RSU and vehicles perform the distribution of pseudonyms. TA identifies vehicles for pseudonym distribution. These vehicles are called Pseudonym Provider Vehicles (PPV). Those vehicles are selected for PPV that frequently travel a long distance. Both RSU and PPV announced the availability of pseudonyms publicly in the network when a certain threshold is reached. A vehicle in the network can request the pseudonym through proper authentication. The pseudonym exchange scheme based on secret sharing is introduced in [163]. The actual identity is hidden using pseudonym exchange process. The message is split into several fragments to utilize secret sharing and then it is recovered. In [164] a novel method WHISPER is introduced in which vehicles reduce beacon transmission range according to its speed. The main purpose of this scheme is to hide a vehicle from a tracker (attacker), not from neighboring vehicles.

Remarks: The other location privacy schemes tried to protect the location tracks of a vehicle in a network. However, they faced certain problems. One of the limitations of these approaches is protecting the location information in a specific area or covering a limited region of interest, such as a social spot but not considering other road network scenarios, like main road networks and faraway roads. Second, for anonymization, a certain number of neighboring vehicles is required in a vicinity, which is not considered in these approaches.

V. COMPARATIVE ANALYSIS

In this section, various location privacy schemes are analyzed, as shown in Table 5. The table contains features, methods, adversary models, evaluation criteria, and limitations of existing location protection schemes in the vehicular network. Most of the schemes follow the construction of a mix zone where vehicles change pseudonyms to hide their identity. The zone may be fixed, multiple zones, virtual zones, dynamic or independent zones depending on the scheme used. Similarly, other techniques of location privacy use the concept of a silent period, group signature, path perturbation, obfuscation, and mix context. By studying various parameters, we come to know that most of the schemes trying to increase the level of privacy and limited attention are given to other factors such as the impact on privacy, overheads (time, computation, communication), and proper context for neighbor cooperation. Here, the level of privacy means the degree to which a privacy-preserving scheme or method or technique protects sensitive information or data of a vehicle or user from being inferred by an adversary. The level of privacy depends on the anonymization of a vehicle in a vicinity, the higher the level of anonymization higher the privacy level, since it becomes difficult for an adversary or attacker to

link an identity to a specific vehicle. The reader could take the help of Table 5 to analyze specific parameters of existing location privacy schemes.

Table 5 General comparison of location privacy techniques

Ref:	Features	Method	Attacker/ adversary model	Evaluation criteria	Weakness
[38]	Context information such as the number of neighbor vehicles, speed, and direction, stable time period	Mix context	General attacker	Vehicle traceability, average tracking time, un-linkable pseudonym change time	Finding a suitable neighbor is a difficult procedure
[39]	Candidate location list, slot change, max allow time for the beacon, zone dynamics	Dynamic mix zone	Global external attacker	Anonymity set size and success rate	Pseudonym change information is shared among vehicles, which makes a way for traceability
[63]	Spatial and temporal factors, anonymization, static and transient mix zones, analysis of time duration of mix zones	Mix zone	Timing and velocity-based attacks	Entropy, tracking success ratio	Based on a fixed zone, the attacker may enable to leak the vehicle location information
[40]	Path/Route query, Path similarity, Location prediction, Historical reputation, Trust value calculation, multiple zone registrations	Multiple mix zones	Global passive adversary	Utility, privacy loss, success rate, entropy, the computation cost	Adjusting routes creates extra overhead
[82]	Virtual identity and reputation mechanism, dynamic change of pseudonyms, public and private keys usage	Use of multiple zones	Mix attacks	Delay, ratio of packet delivery, pseudonym changing time	Increased communication overhead due to vehicle connection with RS
[66]	Location and map services for smartphones, pseudonyms changed synchronously, use of graphic construction algorithm	Multiple mix zones	First in First out attack	Endpoint deviation, computation cost, entropy	Adjusting routes increases overhead
[49]	Pseudonym change, mix zone with the virtual change, fixed zone, high-level privacy at zone	Fixed mix zone	General adversary	W_MAP, linking pseudonym	Does not provide real-time location security
[84]	Reputation model, pseudonym change, dynamic zone,	Virtual mix zone	General adversary	Privacy strength, k-anonymization	Lake of real-time protection due to fixed nature
[50]	Pseudonym change, vehicle collaboration, anonymization, generation of a fake pseudonym	Independent mix zone	External global attacker	Anonymity, Measuring broadcast messages time	The possibility of the malicious vehicle in the zone generating fake pseudonyms, difficult to apply under low traffic conditions
[36]	Traffic congestion detection, extension and creation of silent mix zones	Silent mix zone	Syntactic and semantic linking attacks	Entropy anonymity set, verification of the signature, traffic congestion time	Searching congested traffic zone creation is an extra overhead
[37]	Silent mix zone at a signalized intersection, pseudonym changing strategy, pseudonym exchanges,	Silent mix zone	Syntactic and semantic linking attacks	Anonymity set with entropy, the number of a used pseudonym	Applicable only dense number of vehicles in VANETs
[87]	Age fluid model, time slot reservation, mix zone construction, time slot shuffle, use of silent period	Mix zone and silent period	Global passive adversary	Age of pseudonym, time-to-confusion and anonymity set size	Impacts on vehicle safety application and extra overhead

[90]	Group navigation Identification, chain groups with a silent period, secret contact to LBS	Use of silent period	Global adversary	Measuring tracking time, mean anonymity set size	Silence period affects the safety application
[52]	Context-adaptive pseudonym changing, multi-tracking algorithm, user-centric privacy scheme	Silent period	Global passive adversary and local active adversary	Traceability cost, privacy preference combination, quality of service	De-anonymization is not considered during the traceability of vehicle
[43]	Check on silent period, group formation, cheating detection method, message information hiding	Silent period	Cheating attack	Mean anonymity set size, the number of total pseudonyms changed	Increases impact on safety services
[128]	Density zones, density-based pseudonym change, derivation of the delay distribution	Neighbor Grouping	General passive adversary	The probability of successful location tracking at arrival rate and vehicle speed	Privacy at the cost of safety application and liability
[41]	Short-lived keys, change of pseudonym based on neighboring vehicle behavior, parking lots, and traffic signals	Blind signature	General adversary	Key update time, pseudonym change	Insider attacker is not considered
[123]	Pseudonym mechanism, temporary in-group identity, encryption and authentication mechanism,	Group signature (mix group)	Internal and external adversaries	Mean entropy of the target vehicle and the entire network	There is a gap between combining social spots, i.e. if these spots are located at large distances.
[124]	Hybrid group signature authentication, pseudonym change periodically, dynamic hiding crowd,	Dynamic mix zone/ hybrid	Passive attack	Computation time, storage cost	Super anonymity verification is a slow and time-consuming process
[46]	A structured approach, local privacy, synchronized pseudonym pool	Road intersections	Sybil attack	Tracking fail rate, privacy safety trade-off	The visibility of pseudonyms could create a danger to tracking vehicles.
[138]	Perturbation of location position, generation of path confusion, and route segmentation	Path confusion	General adversary	Average location privacy, a measure of instant location privacy	No real-time security and creates extra overhead
[141]	Virtual image or shadow, route confusion, vehicle collects other vehicles location	Rout confusion	Passive attacker	Entropy, the anonymity set size, tracking success ratio	Not considered an internal attacker in the network
[33]	Use of Analytical network process, source node location privacy,	Group base phantom node selection	General attacker	Alternative weight, final weight	Heavily depends on the phantom node, which may be compromised

The existing techniques use pseudonym changing process for location privacy. Specific parameters are used for the pseudonym change process. For example, the age of pseudonyms, speed of the vehicle, moving direction, number of neighbor vehicles, and certain road context information are used for the change of pseudonyms. Table 6 contains an analysis of the existing scheme for different comparative parameters. The table has shown that the privacy metrics ASS, entropy, and traceability are common in the majority of the schemes. The mode of execution of the strategy is either infrastructure-based or infrastructure-less. The infrastructure-based methods required the support of infrastructure with a higher deploying cost as compared with infrastructure-less schemes. The exchange of pseudonyms hides the identity of a vehicle but may provide the possibility of an internal attacker. Conditional privacy means the accountability of the vehicle. Only authorities may disclose the right location vehicles in case of a dispute. The privacy protection level impacts road network applications, so there should be a balance between privacy and VANETs applications. The researchers should also need to compute the cost of computation and communication for privacy achievement.

VI. OPEN ISSUES AND CONSIDERATIONS

Various constraints and issues are to be considered to build an efficient location privacy scheme in VANETs. For example, pseudonyms of vehicles required to be changed at the proper time and location, pseudonym refill, and revocation problems. Another

issue is the selection of a proper metric for the evaluation of a higher level of location privacy. These issues are discussed in the following sections.

A. Pseudonym refill and change problems

Pseudonyms are fake or partial identifiers used by vehicles to make them anonymous and authenticate in the vehicular communication network. The location privacy schemes are required to anonymize the vehicle during communication. For this purpose, pseudonyms should be used efficiently to preserve the privacy of vehicles. The assignment and changing pseudonyms process should be effectively managed for the efficient use of the storage capacity of vehicle OBU.

Table 6 Analysis of location privacy schemes based on different parameters

Ref:	Privacy metrics	Mode of execution	Pseudonym changing factors	Pseudonym exchange	Conditional privacy	Preserve VANETs Applications	Cost (time, computation, communication
[72]	Protection rate	Infrastructure less	Pseudonym age, speed, and direction	No	No	No	Not given
[44]	ASS, LPG	Infrastructure based		No	No	Yes	Reduced
[77]	ASS	Infrastructure based	Cooperative and randomly	No	No	No	Increased
[78]	ASS, entropy, tracking probability	Infrastructure less	No change	No	No	No	Reduced
[165]	ASS, traceability, confusion, entropy	Infrastructure less	Vehicle cooperation	Yes	Yes	Yes	Not given
[36]	ASS, entropy	Infrastructure less	Vehicle cooperation	No	Yes	Yes	Reduced
[50]	Anonymity	Infrastructure less	Cooperation	No	No	No	Reduced
[57]	ASS, entropy, attacker probability	Infrastructure base	Vehicle cooperation	Yes	No	No	Not mentioned
[83]	ASS, degree of anonymity	Infrastructure base	Cooperation	No	No	Yes	Reduced
[98]	Anonymity, Traceability	Infrastructure less	Context and silent period	No	No	Yes	Not mentioned
[54]	ASS, entropy, traceability	Infrastructure less	Speed, direction, positions	No	Yes	No	Not mentioned
[46]	Tracking failure rate	Infrastructure less	Cooperation	No	Yes	Yes	Reduced
[134]	Anonymity, entropy, Tracking percentage,	Infrastructure less	Condition-based	Yes	Yes	Yes	Not mentioned
[137]	ASS, entropy, tracking probability	Infrastructure less	No change	No	No	Yes	Not calculated
[88]	ASS, entropy, traceability		Simple change	No	No	No	Not mentioned

a. Pseudonyms distribution

For anonymous communication, a vehicle required a set of pseudonyms to be stored on its OBU. The set of pseudonym pools is requested from the pseudonym provider authority which is called a Trusted Authority (TA) or Certificate Authority (CA). These

pseudonyms should be successfully distributed to vehicles. The majority of the schemes take the support of roadside infrastructure (RSU) for pseudonym distribution to the vehicles [166], [167]. Some of the techniques are hybrid in which infrastructure, as well as vehicles, took part in the pseudonym distribution. In [162], pseudonyms are distributed both by RSU and vehicles. The distribution of pseudonyms through RSU is costly. There should be a higher number of RSUs at the roadside ready for pseudonyms distribution, which increases deployment cost. In addition, it is a burden on the RSU to manage pseudonyms. On the other hand, the vehicle that uses a pseudonym distributor provides a way for adversary attack. The researcher should be concerned with design, such as a strategy that reduces deployment cost as well as convenience for the vehicle to get the pseudonym pool easily.

b. Pseudonym refill problem

For the protection of being tracked, the vehicles are changing pseudonyms periodically. The vehicle needs a pool of pseudonyms to be used for message communication in the vehicular network. After the expiration of the pseudonym pool, each vehicle may request to pseudonym issuing authority to refill for another fresh pseudonym set. The process of assigning pseudonyms pool to a vehicle is called pseudonym refilling. There is a need for a suitable pseudonym strategy in this case. Two approaches are investigated in [168] for assigning a pseudonym pool to vehicles. The first strategy considers assigning as many pseudonyms as possible to a vehicle, which is to be used for a long period (for years). It reduces the number of connections with the pseudonym provider and is convenient for a driver. However, the long-term pseudonyms storage strategy has a storage burden and security concern of pseudonyms for a vehicle OBU. The second strategy is to refill a few pseudonyms at a time and repeat the process when pseudonyms are about to expire. It reduces the storage burden of the vehicle OBU, and vehicles frequently obtain fresh pseudonyms. The major drawback of this strategy is the communication overhead as the vehicle frequently makes connections with pseudonym providers for pseudonym refilling. The above mention two pseudonym refilling strategies have their pros and cons. Based on the above observation, we conclude that there should be a balance between these two strategies of pseudonym refilling that overcomes the disadvantages of both of these. The researcher should take into consideration in-between long and short-term pseudonym pool refilling and storage strategies.

c. Pseudonym revocation

Nodes with valid certificate credentials could take part in the network operation. The possession of a valid certificate does not mean that a node in the network will provide correct information and behave correctly. The incorrect or false data may be injected into the network by a valid node for its benefit to mislead other nodes [169], [170]. The inaccurate data injected node should be evicted to safeguard the system with a certificate revocation process. Only the certificate authority has the power to revoke the certificate credentials. When a faulty node is identified in the system, its certificate is revoked along with all the pseudonyms stored in the vehicle OBU [171]. It prevents future damage caused by such a malicious vehicle or node. The revoked certificate credential information is sent to the Certificate Revocation List (CRL). The CRL stores a small piece of information about the revoked certificate of a node to avoid future threats [172]. The node/vehicle long-term identity is also revoked, and future request for a pseudonym refilled is further denied. Once certificate revocation is done, the messages from that node are ignored in the network. Timely access to CRL is essential, and it is a crucial research problem. The CRL should be updated with the latest certificate withdrawal information.

d. Pseudonyms changing

The pseudonym change process has a critical role in the preservation of location privacy in a vehicular network. Massive research work suggested a pseudonym change mechanism for the preservation of the privacy of vehicles [173]. The constant change in the pseudonyms of a vehicle confuses the location tracker. However, the change in the pseudonym of the vehicle should not be in an individual manner; however, vehicles should cooperate in the pseudonym change process [174]. The strength of privacy protection can be determined by the numeral of vehicles that change pseudonyms cooperatively. The pseudonyms changing the process of vehicles create several challenges for the researchers. The first concern is that the pseudonym change should be coordinated between different layers. Otherwise, the vehicle would be traced by linking the identifiers of other communication layers. The second concern is the influence on communication protocols, the change of pseudonyms at a high rate improves privacy but creates complications for the routing protocols. Thirdly, it is hard to detect a malicious node in the vehicular network due to anonymization.

Therefore, it is concluded that the researchers should be concerned about these problems while designing the pseudonym-changing protocol.

B. Evaluation metrics

To evaluate location privacy for a vehicle in VANETs, various metrics are used. These metrics consist of Anonymity Set Size (ASS), Entropy, location traceability, linking attacks, and distortion. The privacy level is measured by ASS and entropy while the privacy efficiency is analyzed with location traceability and linking attacks. Table 7 contains a comparative analysis of privacy metrics.

i. Anonymity set size (ASS)

It is one of the oldest metrics to assess the achieved degree of privacy in a communication network. The user of a network is anonymized in a set of users that creates trouble for an adversary to detect the target user in the crowd. The widely held investigation work [165], [36], [134], for preserving location privacy in VANETs uses ASS as a privacy metric. The higher the size of the anonymity set higher will be the location privacy level. But the anonymization in vehicular networks is a difficult job due to vehicle movement and dynamic network topology. For efficient management of ASS, specific parameters must be considered, i.e., speed of the vehicle, transmission range, road traffic conditions, etc.

ii. Entropy

Entropy measures the uncertainty of an adversary about the various pseudonyms used for communication in the network [68], [91], [175]. Entropy is the degree of randomness of bits in the information exchange among various users of a network. The entropy accomplishes its maximal value based on the probability of uniform distribution. The entropy of a vehicle is efficiently utilized by changing pseudonyms. For the measurement of location privacy in the case of mobile and ad-hoc networks, entropy is used as a metric. However, the evaluation of entropy depends on the adversary model and system model of the concerned scheme [68].

iii. Location traceability

Traceability is the adversary tracking time to find the different location tracks of a user [68], [54]. Location traceability is used as a privacy measure metric. It is inversely proportional to privacy level. The higher the traceability rate of an adversary for a user location lower will be the privacy level. The existing research work calculates traceability based on the continuous tracks of users with each pseudonym update, and some researchers take the tracking percentage of vehicles during trips [54].

Table 7 Privacy Metrics Comparison

Privacy metric	Characteristics	Method	Strength
Anonymity	Simple to calculate Generally used Based on k-anonymity	Grouping of users or vehicles in a certain area	Hide the identity of a vehicle
Entropy	The randomness of the Anonymity set	Randomization of bits	Increased uncertainty
Traceability	Collection of vehicle traces	Tracking routes of vehicles	Increase knowledge of an adversary
Pseudonym linking	Linking of pseudonyms to get the identity of a vehicle	Matching several pseudonyms of a vehicle throughout a trip	Identify the pseudonyms of a vehicle
Distortion	Estimated error	A measure of the error in the actual data	Uncertainty

iv. Pseudonym Linking

How much the attacker successfully links the various pseudonyms of vehicles over time [54]. The privacy scheme should prevent an adversary from applying pseudonym linking attacks. It is measured by checking the adversary failure rate of linking the old pseudonym with a new pseudonym of a vehicle [176], [127].

v. Distortion

Another metric to evaluate the location privacy in VANETs is distortion, which means the estimated error is calculated in the location of a user/vehicle [68]. Distortion is measured in [138] as the expected distance error in the adversary accuracy about the location tracks of a vehicle. The distortion is introduced in a wireless network that increases the uncertainty of an adversary tracking a vehicle in the network [60].

VII. DESIGN CHALLENGES AND FUTURE DIRECTIONS

The development of a privacy protection scheme in case the vehicular network required certain things to be handled efficiently. The researchers face various challenges in the design of location privacy techniques. They should know the challenges during the designing of privacy schemes for the vehicular communication network. In this section, some of the crucial challenges to the design of location privacy schemes are discussed.

i. Pseudonym changing process

The location privacy schemes required a pseudonym to be used during communication on the road network. The pseudonym in the beacon generates confusion for an adversary to track a concerned vehicle. The pseudonym should be altered in the appropriate way to hide the actual identity of a vehicle [177]. Privacy-preserving schemes based on pseudonym changing have certain design challenges. The first one is the frequent change of pseudonyms; if the pseudonyms are changed massively, the vehicle requires a large set of pseudonyms, which will increase the storage burden on vehicle OBUs [37]. The pseudonym should be altered in such a way that it reduces the storage burden and communication overhead. Secondly, the pseudonyms should be changed cooperatively; an individual change in the pseudonym of a vehicle can easily be tracked by an adversary [178]. Thirdly, there should be a proper change in pseudonyms that reduces the tracking probability of a tracker. Fourthly, the high frequency of changes in pseudonyms impacts the geographical routing protocols [179]. Based on this discussion, we concluded that to design a privacy scheme, the researchers should look for a proper change in the pseudonyms of a vehicle that provides privacy as well as reduce the impact of pseudonyms change on other fields of VANETs.

ii. Dynamic network topology

The movement vehicles on the road network change network topology frequently. The regular change in the topology has an impact on the security of a vehicular network [15]. The high mobility and dynamic topology are unpredictable in the case of VANETs. Nodes have a very short connection time due to moving in the opposite direction. It creates difficulty for a researcher to detect a malfunction in such a mobile network [180]. The designer of the privacy scheme should be concerned about this dynamic change in topology. The topology change and straight road structure provide a way for an adversary to predict the future positions of a target vehicle.

iii. Impact on VANET's applications

The basic concept of a vehicular network is to deliver safety to the driver, passenger, and pedestrian on the road. Privacy, safety, and infotainment applications not only for drivers but can be extended to passengers and pedestrians too. In case of privacy, the identity and location of the driver should be hidden from unauthorized entities, the sensitive information of passengers such as personal information, usage of Internet facility in the vehicle needs protection, and the movements of pedestrians require anonymization in the area of vehicular communication. While in the case of safety, the system should deliver correct and timely basis road environment information to prevent accidents and collisions, the system should ensure the safety of the passenger in case of hazardous situations, and the pedestrians safety is also important, the system should detect the presence of pedestrians to ensure safety crossing. The applications of VANETs may be divided into intelligent transportation applications and infotainment (comfort) applications [181]. Intelligent transportation consists of transport safety and transport efficiency applications. While comfort applications consist of general information and entertainment applications. The detail about the applications of the vehicular network is shown in Figure 6. The designing of the privacy technique has an impact on VANETs applications. The researchers want a robust privacy scheme that should prevent an adversary from compromising the location information of a vehicle. It can be achieved with the help of adding inaccurate data or dummy data in beacons, using the silent period, and a piece

of mixed-context information. The fake data and silent periods impact road network applications. The impact of pseudonym change for privacy is analyzed in [182] on road safety applications with the help of simulations. It is shown that the silent period schemes degrade the accuracy of risk and road emergency information. There should be a balance between privacy level and safety applications. This is an essential challenge for the researcher to design a privacy scheme that will prevent the tracking of a vehicle and also provide an incentive for the proper usage of VANETs applications.

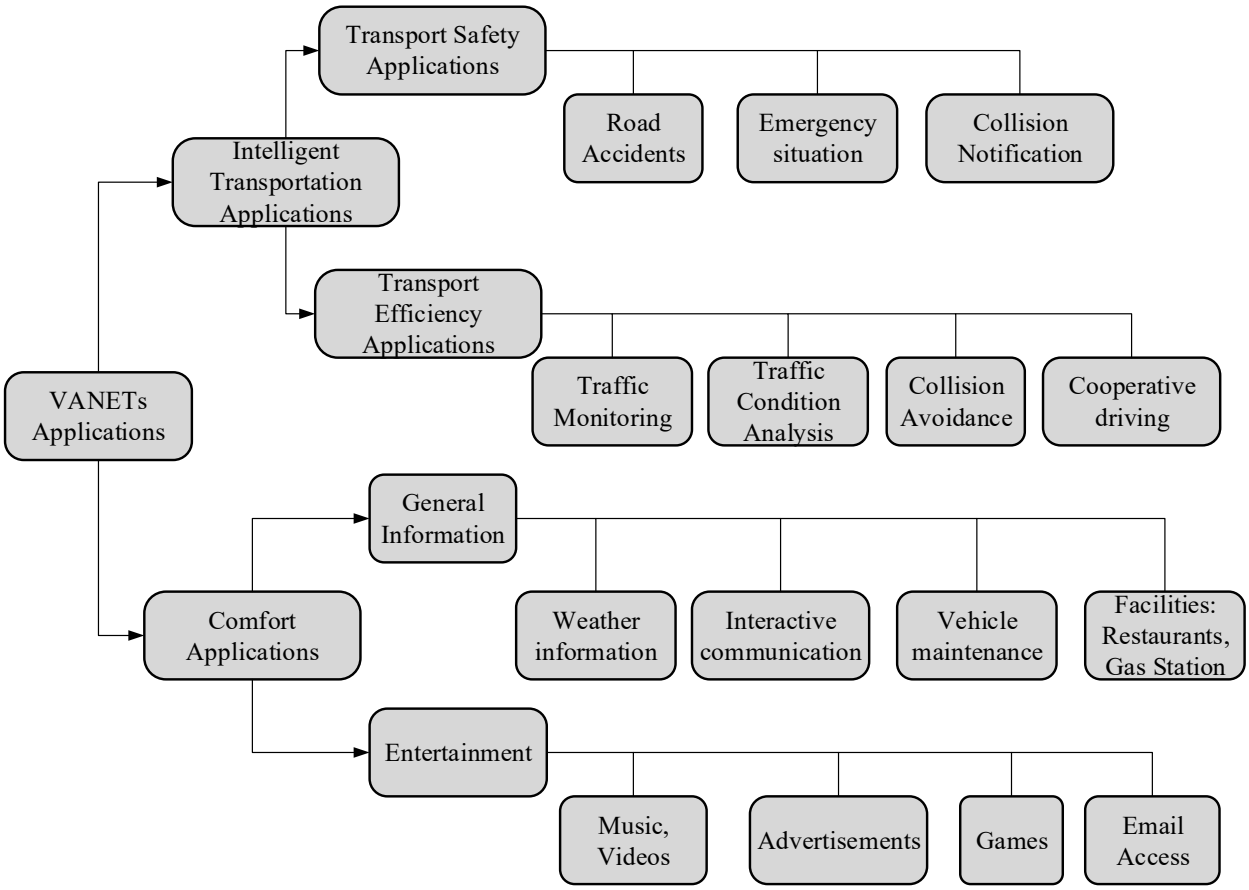

Figure 6 Applications of VANETs

iv. Communication and computation overhead

Another factor that the researcher should count on for the design of a privacy model is the communication and computation overhead that may occur due to the pseudonym change process. The small set of pseudonym pools creates communication overhead, in which a vehicle requests TA each time the pseudonym pool expires. While the large pseudonym set yields storage and computation overhead on vehicle OBUs [183]. This creates certificate management difficulty that how many numbers of pseudonyms are generated and stored in a vehicle [184], which creates a strain on the economic feasibility of pseudonym-changing schemes. So, to design the location privacy model, the researcher should consider the pseudonym management cost. The set of pseudonym pools should be in between small and large that could satisfy the privacy need and also reduce the communication and computation cost for a vehicle.

v. Limited connectivity

The interaction amongst the nodes of the vehicular network remains for a short amount of time, i.e., the network faces frequent disconnection. The instantaneous disconnection, arrival, and departure of vehicles pose a security threat to the network [185]. By using the wireless interface, the attacker can reveal the identity and geographical position of vehicles and try to track the traces of

vehicles. This is also one of the research challenges for the design of privacy-preserving techniques in the vehicular network. The researchers should consider this factor while designing a privacy model.

VIII. DISCUSSION

After the detailed discussion on existing location privacy techniques in VANETs, the core categories of pseudonym changing are mix zone-based, silent period-based, group signature, and dummy-based techniques. The existing methods have certain improvements regarding the location privacy of vehicles, but they're some of the challenges that need to be handled. The useful and negative features of the existing location privacy schemes are given below.

In mixed zone location privacy techniques, pseudo identities of vehicles are mixed when several vehicles are gathered at some locations. The zones are created at a road juncture or some congested areas. Here vehicles change their pseudonyms cooperatively to confuse the adversary. As for the concern of positive characteristics of these techniques. The vehicle identities are hidden in the zone, and it is very hard for an adversary to recognize a vehicle. The researcher takes advantage of a large number of vehicles in the zone and applies the pseudonym-changing strategy to hide vehicle identities from an adversary. The requirements of a mixed zone may have a higher number of vehicle traffic conditions, and all of the vehicles must change pseudonyms simultaneously. Researchers confront several difficulties and challenges in designing location privacy techniques in such scenarios. The first one is vehicle traffic density; if the density is high, location privacy is efficiently utilized in the zone; otherwise, the level of vehicle privacy may be reduced. Secondly, the zone may not be created in every area of the road network; the selection of suitable road vicinity may also be a concern of the researcher. The third challenge regarding privacy is the support of infrastructure in the mixed zone, which is costly and has computation overhead. Fourth, there is a lack of flexibility for a vehicle to change a pseudonym at other places where the pseudonym of a vehicle is about to expire.

In the silent period techniques, the vehicle stays silent by not broadcasting beacon messages and changing pseudonyms during this period. It hides the actual identity of vehicles from an adversary or attacker. These techniques protect vehicle identity from semantic pseudonym linking attacks. The researchers have some challenges regarding the development of silent period location privacy techniques. The first one is the effect of a silent period on road safety applications. Suppose a road accident occurs during the silent mode of the vehicle, how this information be disseminated in the network? The second key challenge in the design of the silent period technique is the synchronization of vehicles during this period. The third one is the management of neighbor cooperation for the silent mode in the network.

The protection of privacy in the group signature scheme is achieved efficiently and hides the actual identity of a vehicle in a group. However, there are certain challenges to the research for the development of group signature methods. The first one is the management number of members in a group. A higher quantity of vehicles in a cluster offers a high level of privacy but is hard to manage, and the lower number of vehicles in a group may reduce the level of privacy of vehicles [40]. Secondly, there are some situations on the road network to implement a group signature, i.e., under lower vehicle traffic conditions. The third challenge regarding group signature techniques is the delay due to signature verification. The researcher should be concerned with minimizing the delay (communication delay) as possible for the improvement of location privacy of vehicles.

The schemes based on path confusion or dummy data create confusion for an adversary to capture the real location and identity of vehicles on the road network. In the design of such strategies, there are certain challenges for the researchers. These techniques efficiently utilize the location privacy of vehicles but at the cost of overhead in the network. Also, the addition of dummy or wrong information in the beacon message affects road safety applications. The researchers should consider utilizing the dummy data in such a manner that does not compromise the location service utility of the vehicular network such as collision notification, road accident information, emergencies, etc.

Based on the above discussion, we come to know that the existing location privacy techniques in vehicular communication may work efficiently in one scenario but have deficiencies in another road scenario, i.e., in diverse vehicle traffic conditions. Some of the methods have an impact on road network applications; others have network and communication overhead. Based on this observation, we concluded that no single technique is suitable to preserve location privacy in VANETs [186]. There should be an integration of different approaches into a single method that works in all conditions of the road network, such as road traffic conditions, availability of infrastructure, and preserving safety applications. There is a need for an adaptive technique that utilizes

road context information (road traffic, safety application, transmission range neighbors, speed variations) to preserve the privacy of vehicles.

IX. CONCLUSION

We surveyed state-of-the-art location privacy techniques for vehicular communication networks. We included a comprehensive taxonomy of various privacy schemes and critically analyzed their features and deficiencies. A table of contributions of research papers on a yearly wise is developed. Privacy design challenges are also discussed which could help researchers know the design challenges for the development of a location privacy scheme in VANETs. Then, open research challenges are explained in the existing literature with limitations and concerns. We also analyze various location privacy attacks and their strength. The correct identification of vulnerabilities in the network and challenges may provide a way to develop a robust privacy-preserving scheme. The majority of the existing techniques of location privacy are trying to achieve a higher level of vehicle privacy. However, the level of privacy protection impacts other applications of VANETs, such as road safety and entertainment applications. Appropriate knowledge of an increase in the level of privacy protection is essential. In addition, existing schemes lack to utilize diverse road network scenarios and traffic conditions efficiently. Consequently, a single scheme does not cover the network requirements for location privacy. There is a need for an integrated strategy that covers the majority of the road network scenarios.

REFERENCES:

[1] D. Cao, B. Zheng, B. Ji, Z. Lei, and C. Feng, "A robust distance-based relay selection for message dissemination in vehicular network," Wirel. Networks, vol. 26, no. 3, pp. 1755–1771, 2020, doi: 10.1007/s11276-018-1863-4.

[2] S.-A.-H. Sedjelmaci, I. H. Brahmi, N. Ansari, and M. H. Rehmani, "Cyber Security Framework for Vehicular Network based on a Hierarchical Game," IEEE Trans. Emerg. Top. Comput., vol. 6750, no. c, pp. 1–1, 2019, doi: 10.1109/tetc.2018.2890476.

[3] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," J. Netw. Comput. Appl., vol. 37, no. 1, pp. 380–392, 2014, doi: 10.1016/j.jnca.2013.02.036.

[4] SAE-International, "SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary," DSRC Comm., 2009.

[5] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," Proc. IEEE, vol. 99, no. 7, pp. 1162–1182, 2011, doi: 10.1109/JPROC.2011.2132790.

[6] B. Hassanabadi and S. Valaee, "Reliable periodic safety message broadcasting in VANETs using network coding," IEEE Trans. Wirel. Commun., vol. 13, no. 3, pp. 1284–1297, 2014, doi: 10.1109/TWC.2014.010214.122008.

[7] A. Wahid, H. Yasmeen, M. A. Shah, and M. Alam, "Holistic approach for coupling privacy with safety in VANETs," Comput. Networks, vol. 148, pp. 214–230, 2019, doi: 10.1016/j.comnet.2018.08.017.

[8] I. Ullah, M. A. Shah, A. Wahid, A. Mehmood, and H. Song, "ESOT: a new privacy model for preserving location privacy in Internet of Things," Telecommun. Syst., vol. 67, no. 4, pp. 553–575, 2018, doi: 10.1007/s11235-017-0352-x.

[9] F. Qu, Z. Wu, F. Wang, and W. Cho, "A Security and Privacy Review of VANETs," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 6, pp. 2985–2996, 2015, doi: 10.1109/TITS.2015.2439292.

[10] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey," IEEE Commun. Surv. Tutorials, vol. 17, no. 1, pp. 228–255, 2015, doi: 10.1109/COMST.2014.2345420.

[11] F. Qu, Z. Wu, F. Wang, and W. Cho, "A Security and Privacy Review of VANETs," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 6, pp. 2985–2996, Dec. 2015, doi: 10.1109/TITS.2015.2439292.

[12] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-Preserving Schemes for Ad Hoc Social Networks: A Survey," IEEE Commun. Surv. Tutorials, vol. 19, no. 4, pp. 3015–3045, 2017, doi: 10.1109/COMST.2017.2718178.

[13] I. Wagner and D. Eckhoff, "Technical privacy metrics: A systematic survey," ACM Comput. Surv., vol. 51, no. 3, 2018, doi: 10.1145/3168389.

[14] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks," IEEE Commun. Surv. Tutorials, vol. 20, no. 1, pp. 770–790, 2018, doi: 10.1109/COMST.2017.2771522.

[15] Z. Lu, G. Qu, and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," IEEE Trans. Intell. Transp. Syst., vol. 20, no. 2, pp. 760–776, 2019, doi: 10.1109/TITS.2018.2818888.

[16] C. Kalaiarasy, N. Sreenath, and A. Amuthan, "Location Privacy Preservation in VANET using Mix Zones - A survey," 2019 Int. Conf. Comput. Commun. Informatics, ICCCI 2019, pp. 0–4, 2019, doi: 10.1109/ICCCI.2019.8822028.

[17] H. Talat, T. Nomani, M. Mohsin, and S. Sattar, "A Survey on Location Privacy Techniques Deployed in Vehicular Networks," Proc. 2019 16th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2019, pp. 604–613, 2019, doi: 10.1109/IBCAST.2019.8667248.

[18] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," Veh. Commun., vol. 16, pp. 45–61, 2019, doi: 10.1016/j.vehcom.2019.02.002.

[19] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in VANETs," Comput. Sci. Rev., vol. 41, p. 100411, 2021, doi: 10.1016/j.cosrev.2021.100411.

[20] X. Jia, L. Xing, J. Gao, and H. Wu, "A Survey of Location Privacy Preservation in Social Internet of Vehicles," IEEE Access, vol. 8, no. 4, pp. 201966–201984, 2020, doi: 10.1109/ACCESS.2020.3036044.

[21] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, "A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues," IEEE Access, vol. 9, pp. 153701–153726, 2021, doi: 10.1109/ACCESS.2021.3125521.

[22] J. Cui, Y. Cai, S. Yang, and Y. Zhang, "A Survey on Privacy-preserving Schemes for Vehicular Ad Hoc Networks," Proc. Int. Conf. Anti-Counterfeiting, Secur.

Identification, ASID, vol. 2021-October, pp. 129–134, 2021, doi: 10.1109/ASID52932.2021.9651711.

[23] 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," Futur. Internet, vol. 13, no. 4, pp. 1–22, 2021, doi: 10.3390/fi13040096.

[24] M. Babaghayou, N. Labraoui, A. A. Abba Ari, N. Lagraa, and M. A. Ferrag, "Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey," J. Inf. Secur. Appl., vol. 55, no. October, pp. 1–17, 2020, doi: 10.1016/j.jisa.2020.102618.

[25] F. D. Da Cunha, Z. Boukerche, L. Villas, A. Carneiro Viana, and A. A. F. Loureiro, "Data Communication in VANETs: A Survey, Challenges and Applications," [Research Report] RR-8498, INRIA Saclay, pp. 1–26, 2014, [Online]. Available: http://hal.inria.fr/hal-00981126/

[26] H. A. Omar, N. Lu, and W. Zhuang, "Wireless access technologies for vehicular network safety applications," IEEE Netw., vol. 30, no. 4, pp. 22–26, 2016, doi: 10.1109/MNET.2016.7513860.

[27] I. T. S. Committee, "IEEE trial-use standard for wireless access in vehicular environments-security services for applications and management messages," IEEE Veh. Technol., vol. 1609, no. July, p. 2006, 2006, [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:IEEE+trial-use+standard+for+wireless+access+in+vehicular+environments-security+services+for+applications+and+management+messages#0

[28] IEEE, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method an," IEEE Std 802.3-2005 (Revision IEEE Std 802.3-2002 Incl. all Approv. Amend., pp. 1–2695, 2005.

[29] R. Z. Xiang Cheng and L. Yang, 5G-Enabled Vehicular Communications and Networking. United Kingdom: Elsevier, 2018.

[30] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," Eur. Data Prot. Coming Age, no. January, pp. 3–32, 2013, doi: 10.1007/978-94-007-5170-5_1.

[31] Y. Pan and J. Li, "Journal of Network and Computer Applications Cooperative pseudonym change scheme based on the number of neighbors in VANETs," J. Netw. Comput. Appl., vol. 36, no. 6, pp. 1599–1609, 2013, doi: 10.1016/j.jnca.2013.02.003.

[32] Y. Toor, P. Mühlethaler, A. Laouiti, and A. De La Fortelle, "Vehicle ad hoc networks: Applications and related technical issues," IEEE Commun. Surv. Tutorials, vol. 10, no. 3, pp. 74–88, 2008, doi: 10.1109/COMST.2008.4625806.

[33] H. Farman et al., "Multicriteria-Based Location Privacy Preservation in Vehicular Ad Hoc Networks," Complexity, vol. 2018, pp. 1–12, Jun. 2018, doi: 10.1155/2018/7697324.

[34] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," Comput. Commun., vol. 44, pp. 1–13, 2014, doi: 10.1016/j.comcom.2014.02.020.

[35] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," Proc. - 12th IEEE Int. Conf. Comput. Sci. Eng. CSE 2009, vol. 3, no. March, pp. 139–145, 2009, doi: 10.1109/CSE.2009.135.

[36] A. Boualouache and S. Moussaoui, "TAPCS: Traffic-aware pseudonym changing strategy for VANETs," Peer-to-Peer Netw. Appl., vol. 10, no. 4, pp. 1008–1020, Jul. 2017, doi: 10.1007/s12083-016-0461-4.

[37] A. Boualouache and S. Moussaoui, "Urban pseudonym changing strategy for location privacy in VANETs," Int. J. Ad Hoc Ubiquitous Comput., vol. 24, no. 1/2, p. 49, 2017, doi: 10.1504/IJAHUC.2017.080914.

[38] M. Gerlach and F. Guttler, "Privacy in VANETs using Changing Pseudonyms - Ideal and Real," in 2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring, Apr. 2007, pp. 2521–2525. doi: 10.1109/VETECS.2007.519.

[39] B. Ying and D. Makrakis, "Pseudonym Changes scheme based on Candidate-location-list in vehicular networks," in 2015 IEEE International Conference on Communications (ICC), Jun. 2015, vol. 2015-Septe, pp. 7292–7297. doi: 10.1109/ICC.2015.7249491.

[40] Q. A. Arain, I. Memon, Z. Deng, M. H. Memon, F. A. Mangi, and A. Zubedi, "Location monitoring approach: multiple mix-zones with location privacy protection based on traffic flow over road networks," Multimed. Tools Appl., vol. 77, no. 5, pp. 5563–5607, Mar. 2018, doi: 10.1007/s11042-017-4469-4.

[41] T. Thenmozhi and R. M. Somasundaram, "Pseudonyms Based Blind Signature Approach for an Improved Secured Communication at Social Spots in VANETs," Wirel. Pers. Commun., vol. 82, no. 1, pp. 643–658, May 2015, doi: 10.1007/s11277-014-2245-6.

[42] L. Zhang, "OTIBAAGKA : A New Security Tool for Cryptographic Mix-Zone Establishment in," Ieee Trans. Inf. Forensics Secur., vol. 12, no. 12, pp. 2998–3010, 2017.

[43] I. Khacheba, M. B. Yagoubi, N. Lagraa, and A. Lakas, "Location privacy scheme for VANETs," in 2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), May 2017, pp. 1–6. doi: 10.1109/MoWNet.2017.8045942.

[44] L. Rongxing, L. Xiaodong, H. L. Tom, L. Xiaohui, and S. Xuemin, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, 2012.

[45] B. Ying, D. Makrakis, and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks," IEEE Commun. Lett., vol. 17, no. 8, pp. 1524–1527, 2013, doi: 10.1109/LCOMM.2013.070113.122816.

[46] D. Eckhoff and C. Sommer, "Marrying safety with privacy: A holistic solution for location privacy in VANETs," in 2016 IEEE Vehicular Networking Conference (VNC), Dec. 2016, pp. 1–8. doi: 10.1109/VNC.2016.7835971.

[47] B. Ying and D. Makrakis, "Reputation-based Pseudonym Change for Location Privacy in vehicular networks," in 2015 IEEE International Conference on Communications (ICC), Jun. 2015, vol. 2015-Septe, pp. 7041–7046. doi: 10.1109/ICC.2015.7249449.

[48] A. K. Tyagi and N. Sreenath, "Location privacy preserving techniques for location based services over road networks," in 2015 International Conference on Communications and Signal Processing (ICCSP), Apr. 2015, pp. 1319–1326. doi: 10.1109/ICCSP.2015.7322723.

[49] B. Amro, "Protecting Privacy in VANETs Using Mix Zones with Virtual Pseudonym Change," Int. J. Netw. Secur. Its Appl., vol. 10, no. 1, pp. 11–21, 2018, doi: 10.5121/ijnsa.2018.10102.

[50] N. Guo, L. Ma, and T. Gao, "Independent Mix Zone for Location Privacy in Vehicular Networks," IEEE Access, vol. 6, pp. 16842–16850, 2018, doi: 10.1109/ACCESS.2018.2800907.

[51] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1569–1589, Oct. 2007, doi: 10.1109/JSAC.2007.071007.

[52] K. Emara, W. Woerndl, and J. Schlichter, "Context-based Pseudonym Changing Scheme for Vehicular Adhoc Networks," arXiv:1607.07656, Jul. 2016, [Online]. Available: http://arxiv.org/abs/1607.07656

[53] Gongjun Yan, S. Olariu, Jin Wang, and S. Arif, "Towards Providing Scalable and Robust Privacy in Vehicular Networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1896–1906, Jul. 2014, doi: 10.1109/TPDS.2013.142.

[54] I. Khacheba, M. B. Yagoubi, N. Lagraa, and A. Lakas, "CLPS: Context-based location privacy scheme for VANETs," Int. J. Ad Hoc Ubiquitous Comput., vol.

29, no. 1–2, pp. 141–159, 2018, doi: 10.1504/ijahuc.2018.094404.

[55] B. Palanisamy and L. Liu, “Attack-resilient mix-zones over road networks: Architecture and algorithms,” IEEE Trans. Mob. Comput., vol. 14, no. 3, pp. 495–508, 2015, doi: 10.1109/TMC.2014.2321747.

[56] A. Wasef and X. (Sherman) Shen, “REP: Location Privacy for VANETs Using Random Encryption Periods,” Mob. Networks Appl., vol. 15, no. 1, pp. 172–185, Feb. 2010, doi: 10.1007/s11036-009-0175-4.

[57] I. Memon, L. Chen, Q. A. Arain, H. Memon, and G. Chen, “Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks,” Int. J. Commun. Syst., vol. 31, no. 1, pp. 1–44, 2018, doi: 10.1002/dac.3437.

[58] Q. Yang, A. Lim, X. Ruan, and X. Qin, “Location Privacy Protection in Contention Based Forwarding for VANETs,” in 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Dec. 2010, pp. 1–5. doi: 10.1109/GLOCOM.2010.5684166.

[59] B. Palanisamy, S. Ravichandran, L. Liu, B. Han, K. Lee, and C. Pu, “Road network mix-zones for anonymous location based services,” Proc. - Int. Conf. Data Eng., pp. 1300–1303, 2013, doi: 10.1109/ICDE.2013.6544929.

[60] B. Bloessl, C. Sommer, F. Dressler, and D. Eckhoff, “The scrambler attack: A robust physical layer attack on location privacy in vehicular networks,” in 2015 International Conference on Computing, Networking and Communications (ICNC), Feb. 2015, pp. 395–400. doi: 10.1109/ICCNC.2015.7069376.

[61] I. Saini, S. S. Ahmed, and A. Jakel, “Attacker Placement for Detecting Vulnerabilities of Pseudonym Change Strategies in VANET,” IEEE Veh. Technol. Conf., vol. 2018-Augus, 2018, doi: 10.1109/VTCFall.2018.8690701.

[62] S. Wang and N. Yao, “LIAP: A local identity-based anonymous message authentication protocol in VANETs,” Comput. Commun., vol. 112, pp. 154–164, 2017, doi: 10.1016/j.comcom.2017.09.005.

[63] R. S. Zuberi and S. N. Ahmad, “Secure Mix-Zones for Privacy Protection of Road Network Location Based Services Users,” J. Comput. Networks Commun., vol. 2016, no. c, pp. 1–8, 2016, doi: 10.1155/2016/3821593.

[64] M. A. Hezam Al Junaid, A. A. Syed, M. N. Mohd Warip, K. N. Fazira Ku Azir, and N. H. Romli, “Classification of Security Attacks in VANET: A Review of Requirements and Perspectives,” MATEC Web Conf., vol. 150, p. 06038, Feb. 2018, doi: 10.1051/matecconf/201815006038.

[65] K. Emara, “Safety-Aware Location Privacy in VANET: Evaluation and Comparison,” IEEE Trans. Veh. Technol., vol. 66, no. 12, pp. 10718–10731, Dec. 2017, doi: 10.1109/TVT.2017.2736885.

[66] Q. Ali, A. Zhongliang, and D. Imran, “Map Services Based on Multiple Mix-zones with Location Privacy Protection over Road Network,” Wirel. Pers. Commun., vol. 97, no. 2, pp. 2617–2632, 2017, doi: 10.1007/s11277-017-4626-0.

[67] Q. A. Arain, I. Memon, Z. Deng, M. H. Memon, F. A. Mangi, and A. Zubedi, “Location monitoring approach: multiple mix-zones with location privacy protection based on traffic flow over road networks,” Multimed. Tools Appl., vol. 77, no. 5, pp. 5563–5607, 2018, doi: 10.1007/s11042-017-4469-4.

[68] F. F. Ü. R. Informatik, K. Ahmed, and A. E. Emara, “Safety-aware Location Privacy in Vehicular Ad-hoc Networks,” 2016. [Online]. Available: https://mediatum.ub.tum.de/?id=1281018

[69] A. R. Beresford and F. Stajano, “Location privacy in pervasive computing,” IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, 2003, doi: 10.1109/MPRV.2003.1186725.

[70] D. L. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” Commun. ACM, vol. 24, no. 2, pp. 84–90, 1981, doi: 10.1145/358549.358563.

[71] J. Liao and J. Li, “Effectively Changing Pseudonyms for Privacy Protection in VANETs,” in 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009, pp. 648–652. doi: 10.1109/I-SPAN.2009.103.

[72] Y.-S. Chen, T.-T. Lo, C.-H. Lee, and A.-C. Pang, “Efficient pseudonym changing schemes for location privacy protection in VANETs,” in 2013 International Conference on Connected Vehicles and Expo (ICCVE), Dec. 2013, pp. 937–938. doi: 10.1109/ICCVE.2013.6799933.

[73] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, “Mix-Zones for Location Privacy in Vehicular Networks,” ACM Work. Wirel. Netw. Intell. Transp. Syst., vol. 51, pp. 1–7, 2007.

[74] A. M. Carianha, L. P. Barreto, and G. Lima, “Improving location privacy in mix-zones for VANETs,” Conf. Proc. IEEE Int. Performance, Comput. Commun. Conf., 2011, doi: 10.1109/PCCC.2011.6108111.

[75] M. S. Al-Marshoud, A. H. Al-Bayatti, and M. S. Kiraz, “Improved chaff-based cmix for solving location privacy issues in vanets,” Electron., vol. 10, no. 11, 2021, doi: 10.3390/electronics10111302.

[76] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, “Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs,” IEEE Int. Conf. Commun., pp. 1–5, 2011, doi: 10.1109/icc.2011.5962919.

[77] A. Boualouache, S. Senouci, and S. Moussaoui, “VLPZ : The Vehicular Location Privacy Zone,” Procedia - Procedia Comput. Sci., vol. 83, no. Ant, pp. 369–376, 2016, doi: 10.1016/j.procs.2016.04.198.

[78] G. Corser, H. Fu, T. Shu, P. D’Errico, and W. Ma, “Endpoint protection zone (EPZ): Protecting LBS user location privacy against deanonymization and collusion in vehicular networks,” in 2013 International Conference on Connected Vehicles and Expo (ICCVE), Dec. 2013, pp. 369–374. doi: 10.1109/ICCVE.2013.6799822.

[79] B. Ying, D. Makrakis, and Z. Hou, “Motivation for protecting selfish vehicles’ location privacy in vehicular networks,” IEEE Trans. Veh. Technol., vol. 64, no. 12, pp. 5631–5641, 2015, doi: 10.1109/TVT.2015.2487262.

[80] Y. Sun, B. Zhang, B. Zhao, X. Su, and J. Su, “Mix-zones optimal deployment for protecting location privacy in VANET,” Peer-to-Peer Netw. Appl., vol. 8, no. 6, pp. 1108–1121, Nov. 2015, doi: 10.1007/s12083-014-0269-z.

[81] I. Ullah, M. A. Shah, A. Khan, C. Maple, and A. Waheed, “Virtual pseudonym-changing and dynamic grouping policy for privacy preservation in vanets,” Sensors, vol. 21, no. 9, p. 3077, 2021, doi: 10.3390/s21093077.

[82] Q. Ali, A. Zhongliang, and D. Imran, “Location Privacy with Dynamic Pseudonym-Based Multiple Mix-Zones Generation over Road Networks,” Wirel. Pers. Commun., vol. 97, no. 3, pp. 3645–3671, 2017, doi: 10.1007/s11277-017-4690-5.

[83] A. Boualouache, S. Senouci, and S. Moussaoui, “Towards an Effi cient Pseudonym Management and Changing Scheme for Vehicular Ad-Hoc Networks,” Glob. Commun. Conf., no. IEEE, pp. 1–7, 2016, doi: 10.1109/GLOCOM.2016.7842339.

[84] N. Guo, L. Ma, and T. Gao, “A Location Privacy-Preserving Scheme for VANETs Based on Virtual Mix Zone,” Res. Briefs Inf. Commun. Technol. Evol., vol. 3, no. 10, pp. 1–8, 2017.

[85] A. Boualouache and S. Moussaoui, “S2SI: A practical pseudonym changing strategy for location privacy in VANETs,” in Proceedings - 2014 International Conference on Advanced Networking Distributed Systems and Applications, INDS 2014, 2014, pp. 70–75. doi: 10.1109/INDS.2014.20.

[86] A. P. Mdee, M. T. R. Khan, J. Seo, and D. Kim, “Security Compliant and Cooperative Pseudonyms Swapping for Location Privacy Preservation in VANETs,”

IEEE Trans. Veh. Technol., pp. 1–15, 2023, doi: 10.1109/TVT.2023.3254660.

[87] Z. Liu, Z. Liu, L. Zhang, and X. Lin, “MARP: A Distributed MAC Layer Attack Resistant Pseudonym Scheme for VANET,” IEEE Trans. Dependable Secur. Comput., vol. 17, no. 4, pp. 869–882, Jul. 2020, doi: 10.1109/TDSC.2018.2838136.

[88] J. Cui, J. Wen, S. Han, and H. Zhong, “Efficient Privacy-Preserving Scheme for Real-Time Location Data in Vehicular Ad-Hoc Network,” IEEE Internet Things J., vol. 5, no. 5, pp. 3491–3498, 2018, doi: 10.1109/JIOT.2018.2797206.

[89] L. Huang, K. Matsuura, H. Yamanet, and K. Sezaki, “Enhancing wireless location privacy using silent period,” IEEE Wirel. Commun. Netw. Conf. WCNC, vol. 2, no. 1, pp. 1187–1192, 2005, doi: 10.1109/WCNC.2005.1424677.

[90] K. Sampigethaya, L. Huang, M. Li, K. Poovendran, Radha Matsuura, and K. Sezaki, “CARAVAN: Providing location privacy for VANET,” Embed. Secur. Cars, pp. 1–15, 2005.

[91] Y.-C. Wei and Y.-M. Chen, “Safe Distance Based Location Privacy in Vehicular Networks,” 2010 IEEE 71st Veh. Technol. Conf., pp. 1–5, 2010, doi: 10.1109/VETECS.2010.5494209.

[92] B. Amro, Y. Saygin, and A. Levi, “Enhancing privacy in collaborative traffic-monitoring systems using autonomous location update,” IET Intell. Transp. Syst., vol. 7, no. 4, pp. 388–395, Dec. 2013, doi: 10.1049/iet-its.2011.0212.

[93] B. K. Chaurasia, S. Verma, G. S. Tomar, and S. M. Bhaskar, “Pseudonym based mechanism for sustaining privacy in VANETs,” 2009 1st Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSYN 2009, pp. 420–425, 2009, doi: 10.1109/CICSYN.2009.79.

[94] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte, “SLOW: A Practical pseudonym changing scheme for location privacy in VANETs,” in 2009 IEEE Vehicular Networking Conference (VNC), Oct. 2009, pp. 1–8. doi: 10.1109/VNC.2009.5416380.

[95] L. Benarous, S. Bitam, and A. Mellouk, “CSLPPS: Concerted Silence-Based Location Privacy Preserving Scheme for Internet of Vehicles,” IEEE Trans. Veh. Technol., vol. 70, no. 7, pp. 7153–7160, 2021, doi: 10.1109/TVT.2021.3088762.

[96] M. Babaghayou, N. Chaib, N. Lagraa, M. A. Ferrag, and L. Maglaras, “A Safety-Aware Location Privacy-Preserving IoV Scheme with Road Congestion-Estimation in Mobile Edge Computing,” Sensors, vol. 23, no. 1, pp. 1–38, 2023, doi: 10.3390/s23010531.

[97] R. Al-ani, T. Baker, B. Zhou, and Q. Shi, “Privacy and safety improvement of VANET data via a safety-related privacy scheme,” Int. J. Inf. Secur., pp. 1–21, Feb. 2023, doi: 10.1007/s10207-023-00662-6.

[98] K. Emara, W. Woerndl, and J. Schlichter, “CAPS: Context-aware Privacy Scheme for VANET Safety Applications,” Proc. 8th ACM Conf. Secur. Priv. Wirel. Mob. Networks, pp. 21:1--21:12, 2015, doi: 10.1145/2766498.2766500.

[99] R. Al-ani, B. Zhou, Q. Shi, T. Baker, and M. Abdlhamed, “Adjusted Location Privacy Scheme for VANET Safety Applications,” in NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, Apr. 2020, pp. 1–4. doi: 10.1109/NOMS47738.2020.9110362.

[100] P. K. Singh, D. Chourasiya, A. Singh, S. K. Nandi, and S. Nandi, “CCAPS: Cooperative context aware privacy scheme for VANETs,” IEEE Veh. Technol. Conf., vol. 2019-Septe, pp. 1–5, 2019, doi: 10.1109/VTCFall.2019.8891099.

[101] I. Saini, S. Saad, and A. Jaekel, “A context aware and traffic adaptive privacy scheme in VANETs,” 2020 IEEE 3rd Connect. Autom. Veh. Symp. CAVS 2020 - Proc., 2020, doi: 10.1109/CAVS51000.2020.9334559.

[102] B. Moussaoui, N. Chikouche, and H. Fouchal, “An efficient privacy scheme for C-ITS stations,” Comput. Electr. Eng., vol. 107, p. 108613, Apr. 2023, doi: 10.1016/j.compeleceng.2023.108613.

[103] Z. Zhang, T. Feng, B. Sikdar, and W. C. Wong, “A Flickering Context-based Mix Strategy for Privacy Protection in VANETs,” IEEE Int. Conf. Commun., pp. 1–6, 2021, doi: 10.1109/ICC42927.2021.9500880.

[104] D. Chaum and E. van Heyst, “Group Signatures,” Work. Theory Appl. Cryptogr. Tech. Bright. UK, Proc. 10, Springer Berlin Heidelberg, pp. 257–265, 1991.

[105] D. Manivannan, S. S. Moni, and S. Zeadally, “Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs),” Veh. Commun., vol. 25, 2020, doi: 10.1016/j.vehcom.2020.100247.

[106] C. March and C. Youngblood, “An Introduction to Identity-based Cryptography,” Cryptol. Inf. Secur. Ser., vol. 2, no. March, pp. 1–12, 2005.

[107] W. Kong, J. Shen, P. Vijayakumar, Y. Cho, and V. Chang, “A practical group blind signature scheme for privacy protection in smart grid,” J. Parallel Distrib. Comput., vol. 136, pp. 29–39, 2020, doi: 10.1016/j.jpdc.2019.09.016.

[108] D. Nuñez, I. Agudo, and J. Lopez, “Proxy Re-Encryption : Analysis of Constructions and its Application to Secure Access Delegation,” J. Netw. Comput. Appl., vol. 89, pp. 193–209, 2017.

[109] X. Deng, X. Xin, and T. Gao, “A location privacy protection scheme based on random encryption period for VSNs,” J. Ambient Intell. Humaniz. Comput., vol. 11, no. 3, pp. 1351–1359, 2020, doi: 10.1007/s12652-019-01227-z.

[110] M. Burmester, E. Magkos, and V. Chrissikopoulos, “Strengthening privacy protection in VANETs,” Proc. - 4th IEEE Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob 2008, pp. 508–513, 2008, doi: 10.1109/WiMob.2008.32.

[111] Y. Mei, G. Jiang, W. Zhang, and Y. Cui, “A Collaboratively Hidden Location Privacy Scheme for VANETs,” Int. J. Distrib. Sens. Networks, vol. 10, no. 3, p. 473151, Mar. 2014, doi: 10.1155/2014/473151.

[112] and L. W. Xinxin Liu, Zhijuan, Erfeg Xu, Bei Gong, “A Privacy Protection Scheme in VANETs Based on Group Signature,” China Commun., vol. 10, no. 11, pp. 286–300, 2019, doi: 10.1109/CC.2013.6674204.

[113] X. Lin, X. Sun, P. H. Ho, and X. Shen, “GSIS: A secure and privacy-preserving protocol for vehicular communications,” IEEE Trans. Veh. Technol., vol. 56, no. 6 I, pp. 3442–3456, 2007, doi: 10.1109/TVT.2007.906878.

[114] A. Alganas, X. Lin, and A. Grami, “EVSE: An efficient vehicle social evaluation scheme with location privacy preservation for vehicular communications,” IEEE Int. Conf. Commun., 2011, doi: 10.1109/icc.2011.5962526.

[115] M. Dikmak, Z. Sabra, A. Kayssi, and A. Chehab, “Optimized conditional privacy preservation in VANETs,” 2012 19th Int. Conf. Telecommun. ICT 2012, no. Ict, 2012, doi: 10.1109/ICTEL.2012.6221234.

[116] W. Ying and Y. Shiyong, “Protecting Location Privacy via Synchronously Pseudonym Changing in VANETs,” in 2014 Fourth International Conference on Communication Systems and Network Technologies, Apr. 2014, no. 61362038, pp. 644–648. doi: 10.1109/CSNT.2014.135.

[117] X. Deng, T. Gao, N. Guo, C. Zhao, and J. Qi, “PCP: A Pseudonym Change Scheme for Location Privacy Preserving in VANETs,” Entropy, vol. 24, no. 5, pp. 1–28, 2022, doi: 10.3390/e24050648.

[118] Y. Park, C. Sur, S.-W. Noh, and K.-H. Rhee, “Secure vehicle location-sharing for trajectory-based message delivery on VANETs,” in 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), Jun. 2017, pp. 1451–1456. doi: 10.1109/ISIE.2017.8001459.

[119] H. Weerasinghe, H. Fu, and S. Leng, “Anonymous service access for Vehicular Ad hoc Networks,” Inf. Assur. Secur. (IAS), 2010 Sixth Int. Conf., pp. 173–178, 2010, doi: 10.1109/ISIAS.2010.5604052.

[120] H. Weerasinghe, H. Fu, S. Leng, and Y. Zhu, “Enhancing unlinkability in Vehicular Ad Hoc Networks,” in Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, Jul. 2011, pp. 161–166. doi: 10.1109/ISI.2011.5983992.

[121] F. A. Ghaleb, M. A. Razzaque, and I. F. Isnin, “Security and privacy enhancement in VANETs using mobility pattern,” Int. Conf. Ubiquitous Futur. Networks, ICUFN, pp. 184–189, 2013, doi: 10.1109/ICUFN.2013.6614808.

[122] D. Forster, F. Kargl, and H. Lohr, “PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET),” in IEEE Vehicular Networking Conference, VNC, Dec. 2015, vol. 2015-Janua, no. January, pp. 25–32. doi: 10.1109/VNC.2014.7013305.

[123] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, “MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks,” IEEE Trans. Dependable Secur. Comput., vol. 13, no. 1, pp. 93–105, 2016, doi: 10.1109/TDSC.2015.2399291.

[124] S. Al-Shareeda and F. Ozguner, “Preserving location privacy using an anonymous authentication dynamic mixing crowd,” in 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Nov. 2016, pp. 545–550. doi: 10.1109/ITSC.2016.7795607.

[125] S. Mathews M and Y. Bevish Jinila, “An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet,” in 2014 International Conference on Electronics and Communication Systems (ICECS), Feb. 2014, pp. 1–6. doi: 10.1109/ECS.2014.6892619.

[126] J. Ni, X. Lin, and X. Shen, “Privacy-Preserving Data Forwarding in VANETs: A Personal-Social Behavior Based Approach,” in GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Dec. 2017, vol. 2018-Janua, pp. 1–6. doi: 10.1109/GLOCOM.2017.8254013.

[127] A. Tomandl, H. Federrath, and F. Scheuer, “VANET privacy by ‘defending and attacking,’” in 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), Apr. 2013, pp. 1–7. doi: 10.1109/WMNC.2013.6549052.

[128] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, “Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks,” Mob. Networks Appl., vol. 15, no. 1, pp. 160–171, Feb. 2010, doi: 10.1007/s11036-009-0167-4.

[129] I. Memon, “Distance and clustering-based energy-efficient pseudonyms changing strategy over road network,” Int. J. Commun. Syst., vol. 31, no. 11, p. e3704, 2018, doi: 10.1002/dac.3704.

[130] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, “Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping,” in 2010 IEEE Vehicular Networking Conference, VNC 2010, Dec. 2010, pp. 174–181. doi: 10.1109/VNC.2010.5698239.

[131] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, “SlotSwap: strong and affordable location privacy in intelligent transportation systems,” IEEE Commun. Mag., vol. 49, no. 11, pp. 126–133, Nov. 2011, doi: 10.1109/MCOM.2011.6069719.

[132] R. Lu, X. Lin, X. Liang, and X. Shen, “A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs,” IEEE Trans. Intell. Transp. Syst., vol. 13, no. 1, pp. 127–139, Mar. 2012, doi: 10.1109/TITS.2011.2164068.

[133] D. Eckhoff and C. Sommer, “Readjusting the privacy goals in Vehicular Ad-Hoc Networks: A safety-preserving solution using non-overlapping time-slotted pseudonym pools,” Comput. Commun., vol. 122, no. January, pp. 118–128, 2018, doi: 10.1016/j.comcom.2018.03.006.

[134] S. Wang, N. Yao, N. Gong, and Z. Gao, “A trigger-based pseudonym exchange scheme for location privacy preserving in VANETs,” Peer-to-Peer Netw. Appl., vol. 11, no. 3, pp. 548–560, 2018, doi: 10.1007/s12083-017-0557-5.

[135] S. Taha and X. S. Shen, “Fake point location privacy scheme for mobile public hotspots in NEMO based VANET,” in 2013 IEEE International Conference on Communications (ICC), Jun. 2013, pp. 2037–2041. doi: 10.1109/ICC.2013.6654825.

[136] S. Taha and X. Shen, “Physical-Layer Location Privacy for Mobile Public Hotspots in a NEMO-Based VANET,” SpringerBriefs Comput. Sci., vol. 14, no. 9783319013503, pp. 73–101, 2013, doi: 10.1007/978-3-319-01351-0_4.

[137] G. Corser et al., “Privacy-by-Decoy: Protecting location privacy against collusion and deanonymization in vehicular location based services,” in IEEE Intelligent Vehicles Symposium, Proceedings, 2014, no. Iv, pp. 1030–1036. doi: 10.1109/IVS.2014.6856595.

[138] B. Hoh and M. Gruteser, “Protecting location privacy through path confusion,” Proc. - First Int. Conf. Secur. Priv. Emerg. Areas Commun. Networks, Secur. 2005, vol. 2005, pp. 194–205, 2005, doi: 10.1109/SECURECOMM.2005.33.

[139] K. Lim and X. Wang, “Nonnegative Matrix Factorization based privacy preservation in vehicular communication,” in Conference Proceedings - IEEE SOUTHEASTCON, Apr. 2015, vol. 2015-June, no. June, pp. 1–2. doi: 10.1109/SECON.2015.7132917.

[140] K. Emara, “Location Privacy in Vehicular Networks,” IEEE 14th Int. Symp. on" A World Wireless, Mob. Multimed. Networks"(WoWMoM). IEEE, pp. 6–7, 2013.

[141] J. Cui, J. Wen, H. Zhong, and J. Zhang, “A Privacy Protection Scheme for Vehicle’s Location Based on Virtual Location and Route Confusion,” in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Jun. 2017, vol. 2018-Janua, pp. 190–194. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.33.

[142] J. Lim, H. Yu, K. Kim, M. Kim, and S. B. Lee, “Preserving Location Privacy of Connected Vehicles With Highly Accurate Location Updates,” IEEE Commun. Lett., vol. 21, no. 3, pp. 540–543, Mar. 2017, doi: 10.1109/LCOMM.2016.2637902.

[143] I. Ullah, M. A. Shah, A. Khan, and G. Jeon, “Privacy-preserving multilevel obfuscation scheme for vehicular network,” Trans. Emerg. Telecommun. Technol., vol. 32, no. 2, pp. 32(2), e4204, Feb. 2021, doi: 10.1002/ett.4204.

[144] L. Benarous, B. Kadri, and S. Boudjit, “Alloyed Pseudonym Change Strategy for Location Privacy in VANETs,” 2020 IEEE 17th Annu. Consum. Commun. Netw. Conf. CCNC 2020, pp. 1–6, 2020, doi: 10.1109/CCNC46108.2020.9045740.

[145] Z. Li, X. Xing, J. Qian, H. Li, and G. Sun, “Trajectory Privacy Preserving for Continuous LBSs in VANET,” Wirel. Commun. Mob. Comput., vol. 2022, 2022, doi: 10.1155/2022/1424078.

[146] M. Arif, G. Wang, and T. Peng, “Track me if you can? Query Based Dual Location Privacy in VANETs for V2V and V2I,” Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018, pp. 1091–1096, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00152.

[147] Z. Chen, X. Bao, Z. Ying, X. Liu, and H. Zhong, “Differentially private location protection with continuous time stamps for VANETs,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 11337 LNCS, Springer International Publishing, 2018, pp. 204–219. doi: 10.1007/978-3-030-05063-4_17.

[148] Q. Li, H. Wu, X. Wu, and L. Dong, “Multi-level location privacy protection based on differential privacy strategy in VANETs,” IEEE Veh. Technol. Conf., vol. 2019-April, no. 1, pp. 1–5, 2019, doi: 10.1109/VTCSpring.2019.8746396.

[149] W. Wang, M. Min, L. Xiao, Y. Chen, and H. Dai, “Protecting Semantic Trajectory Privacy for VANET with Reinforcement Learning,” IEEE Int. Conf. Commun., vol. 2019-May, pp. 1–5, 2019, doi: 10.1109/ICC.2019.8761415.

[150] X. Li et al., “PAPU: Pseudonym Swap with Provable Unlinkability Based on Differential Privacy in VANETs,” IEEE Internet Things J., vol. 7, no. 12, pp. 1–1, 2020, doi: 10.1109/jiot.2020.3001381.

[151] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, “ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,” Proc. - IEEE

INFOCOM, pp. 1903–1911, 2008, doi: 10.1109/INFOCOM.2007.179.

[152] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs," IEEE Trans. Intell. Transp. Syst., vol. 12, no. 3, pp. 736–746, Sep. 2011, doi: 10.1109/TITS.2011.2156790.

[153] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "RescueMe: Location-based secure and dependable VANETs for disaster rescue," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 659–669, 2011, doi: 10.1109/JSAC.2011.110314.

[154] Y. Park and C. S. Rhee, Kyung-hyune, "A Secure and Location Assurance Protocol for Location-Aware Services in VANETs," Proc. 2011 Fifth Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput., pp. 456–461, 2011, doi: 10.1109/IMIS.2011.40.

[155] V. Pathak, D. Yao, and L. Iftode, "Securing location aware services over VANET using geographical secure path routing," Proc. 2008 IEEE Int. Conf. Veh. Electron. Safety, ICVES 2008, pp. 346–353, 2008, doi: 10.1109/ICVES.2008.4640905.

[156] X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs," in Proceedings - IEEE INFOCOM, Apr. 2011, pp. 2147–2155. doi: 10.1109/INFCOM.2011.5935026.

[157] F. Scheuer, M. Brecht, and H. Federrath, "A privacy-aware location service for VANETs using Chaum's mixes," 2010 IEEE 6th Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob'2010, pp. 159–164, 2010, doi: 10.1109/WIMOB.2010.5644986.

[158] K. Mershad and H. Artail, "REACT: Secure and efficient data acquisition in VANETs," 2011 IEEE 7th Int. Conf. Wirel. Mob. Comput. Netw. Commun., pp. 149–156, 2011, doi: 10.1109/WiMOB.2011.6085411.

[159] D. Ren and S. Du, "A Novel Attack Tree Based Risk Assessment Approach for Location Privacy Preservation in the VANETs," Commun. Soc., no. 61003218, pp. 11–15, 2011, doi: 10.1109/icc.2011.5962947.

[160] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random changing pseudonyms scheme in VANETs," Proc. - 2011 Int. Conf. Netw. Comput. Inf. Secur. NCIS 2011, vol. 2, pp. 141–145, 2011, doi: 10.1109/NCIS.2011.127.

[161] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random pseudonym change scheme in VANETs," Cluster Comput., vol. 17, no. 2, pp. 413–421, 2014, doi: 10.1007/s10586-012-0242-7.

[162] A. Boualouache, S. M. Senouci, and S. Moussaoui, "HPDM: A Hybrid Pseudonym Distribution Method for Vehicular Ad-hoc Networks," Procedia Comput. Sci., vol. 83, no. Ant, pp. 377–384, 2016, doi: 10.1016/j.procs.2016.04.199.

[163] P. Yang and L. Deng, "An effective privacy protection mechanism in VANETs," Int. Conf. Mob. Multimed. Commun., vol. 2018-June, no. 3, 2018, doi: 10.4108/eai.21-6-2018.2276638.

[164] M. Babaghayou, N. Labraoui, A. A. A. Ari, M. A. Ferrag, L. Maglaras, and H. Janicke, "Whisper: A location privacy-preserving scheme using transmission range changing for internet of vehicles," Sensors, vol. 21, no. 7, pp. 1–21, 2021, doi: 10.3390/s21072443.

[165] P. K. Singh, S. N. Gowtham, T. S, and S. Nandi, "CPESP: Cooperative Pseudonym Exchange and Scheme Permutation to preserve location privacy in VANETs," Veh. Commun., vol. 20, p. 100183, 2019, doi: 10.1016/j.vehcom.2019.100183.

[166] J. Benin, M. Nowatkowski, and H. Owen, "Unified pseudonym distribution in VANETs," 2010 IEEE 6th Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob'2010, pp. 529–533, 2010, doi: 10.1109/WIMOB.2010.5645015.

[167] J. Benin, M. Nowatkowski, and H. Owen, "Vehicular network pseudonym distribution in congested urban environments," Conf. Proc. - IEEE SOUTHEASTCON, pp. 1–5, 2012, doi: 10.1109/SECon.2012.6196902.

[168] Z. Ma, F. Kargl, and M. Weber, "Pseudonym-on-demand: A new pseudonym refill strategy for vehicular communications," in IEEE Vehicular Technology Conference, 2008, pp. 1–5. doi: 10.1109/VETECF.2008.455.

[169] J.-P. H. Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1557–1568, 2007, doi: 10.1007/978-3-319-93332-0_2.

[170] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," IEEE Veh. Technol. Conf., 2011, doi: 10.1109/VETECF.2011.6093096.

[171] M. E. Nowatkowski, J. E. Wolfgang, C. McManus, and H. L. Owen, "The effects of limited lifetime pseudonyms on certificate revocation list size in VANETS," Conf. Proc. - IEEE SOUTHEASTCON, pp. 380–383, 2010, doi: 10.1109/SECON.2010.5453849.

[172] M. A. Simplicio Junior, E. Lopes Cominetti, H. Kupwade Patil, J. Ricardini, L. Ferraz, and M. V. Silva, "Privacy-Preserving Method for Temporarily Linking/Revoking Pseudonym Certificates in VANETs," Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018, pp. 1322–1329, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00182.

[173] S. Wang and N. Yao, "A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs," Wirel. Networks, vol. 25, no. 3, pp. 1099–1115, 2019, doi: 10.1007/s11276-018-1681-8.

[174] Q. A. Arain, Z. L. Deng, I. Memon, A. Zubedi, and F. A. Mangi, "Location Privacy with Dynamic Pseudonym-Based Multiple Mix-Zones Generation over Road Networks," Wirel. Pers. Commun., vol. 97, no. 3, pp. 3645–3671, 2017, doi: 10.1007/s11277-017-4690-5.

[175] C. Kalaiarasy, N. Sreenath, and A. Amuthan, "An effective variant ring signature-based pseudonym changing mechanism for privacy preservation in mixed zones of vehicular networks," J. Ambient Intell. Humaniz. Comput., vol. 11, no. 4, pp. 1669–1681, 2020, doi: 10.1007/s12652-019-01304-3.

[176] M. Zeng and H. Xu, "Mix-context-based pseudonym changing privacy preserving authentication in VANETs," Mob. Inf. Syst., vol. 2019, 2019, doi: 10.1155/2019/3109238.

[177] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," WONS 2010 - 7th Int. Conf. Wirel. On-demand Netw. Syst. Serv., pp. 176–183, 2010, doi: 10.1109/WONS.2010.5437115.

[178] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in VANETs," Journal of Network and Computer Applications, vol. 36, no. 6. pp. 1599–1609, 2013. doi: 10.1016/j.jnca.2013.02.003.

[179] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in VANETs," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2006, vol. 4357 LNCS, pp. 43–57. doi: 10.1007/11964254_6.

[180] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," Veh. Commun., vol. 1, no. 2, pp. 53–66, 2014, doi: 10.1016/j.vehcom.2014.05.001.

[181] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," Comput. Commun., vol. 44, pp. 1–13, 2014, doi: 10.1016/j.comcom.2014.02.020.

[182] I. Ben Jemaa, A. Kaiser, and B. Lonc, "Study of the impact of pseudonym change mechanisms on vehicular safety," IEEE Veh. Netw. Conf. VNC, vol. 2018-January, pp. 259–262, 2017, doi: 10.1109/VNC.2017.8275632.

[183] S. Bao et al., “Pseudonym Management Through Blockchain: Cost-Efficient Privacy Preservation on Intelligent Transportation Systems,” IEEE Access, vol. 7, pp. 80390–80403, 2019, doi: 10.1109/ACCESS.2019.2921605.

[184] S. Bao, “Dynamic pseudonym management for privacy preservation in vehicular communication systems,” Commun. Syst., no. November, pp. 1–416, 2020, doi: 10.1007/b138483.

[185] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” Veh. Commun., vol. 7, pp. 7–20, 2017, doi: 10.1016/j.vehcom.2017.01.002.

[186] I. Saini, S. Saad, and A. Jaekel, “Evaluating the effectiveness of pseudonym changing strategies for location privacy in vehicular ad-hoc network,” Secur. Priv., no. February, p. e68, May 2019, doi: 10.1002/spy2.68.