future internet

MDPI

Review

Security Challenges of Location Privacy in VANETs and State-of-the-Art Solutions: A Survey

Shawal Khan [1,*], Ishita Sharma [2], Mazzamal Aslam [1], Muhammad Zahid Khan [3] and Shahzad Khan [4]

[1] COMSATS Institute of Information Technology, Islamabad 44000, Pakistan; malikmuzamal72@gmail.com
[2] Department of Business Development and Technology, Aarhus University, 8000 Aarhus, Denmark; ishi@btech.au.dk
[3] Department of Computer Science and IT, University of Malakand, Chakdara 18800, Pakistan; mzahidkhan@uom.edu.pk
[4] Military College of Signal, NUST, Islamabad 44000, Pakistan; shahzadbehram@gmail.com
* Correspondence: shawalsbbu@gmail.com

Abstract: A Vehicular Ad-hoc Network (VANET) comprises a group of moving or stationary vehicles connected by a wireless network. VANETs play a vital role in providing safety and comfort to drivers in vehicular environments. They provide smart traffic control and real-time information, event allocation. VANETs have received attention in support of safe driving, intelligent navigation, emergency and entertainment applications in vehicles. Nevertheless, these increasingly linked vehicles pose a range of new safety and security risks to both the host and its associated properties and may even have fatal consequences. Violations of national privacy and vehicle identities are a major obstacle to introducing forced contact protocols in vehicles. Location privacy refers to the privacy of the vehicle (driver) and the location of the vehicle. Whenever a vehicle sends a message, no one but authorized entities should know their real identity and location of the vehicle. All the messages sent by the vehicle must be authenticated before processing, hence location privacy is an important design aspect to be considered in VANETs operations. The novelty of this paper is that it specifically reviews location privacy in VANETs in terms of operational and safety concerns. Furthermore, it presents a critical analysis of various attacks, identity thefts, manipulation and other techniques in vogue for location privacy protection available in state-of-the-art solutions for VANETs. The efforts in this paper will help researchers to develop a great breadth of understanding pertaining to location privacy issues and various security threats encountered by VANETs and present the critical analysis of the available state-of-the- art solutions to maintain location privacy in VANETs.

Keywords: intelligent transportation system; VANET; location privacy; VANET security

Citation: Khan, S.; Sharma, I.; Aslam, M.; Khan, M.Z.; Khan, S. Security Challenges of Location Privacy in VANETs and State-of-the-Art Solutions: A Survey. *Future Internet* **2021**, *13*, 96. https://doi.org/10.3390/fi13040096

Academic Editor: Luis Javier Garcia Villalba

Received: 17 March 2021
Accepted: 5 April 2021
Published: 10 April 2021

1. Introduction

In recent years, due to economic and population growth, a rapid increase has been observed in the numerous vehicles. This has automatically increased road accidents, driver exhaustion and worsening of roads and support framework. According to a healthcare report by the World Health Organization (WHO), the main cause of deaths of people between 15–29 years is road accidents, also 1.3 million people are killed in accidents annually worldwide [1]. This rapid increase in traffic accidents can be managed by practicing the latest technology to report real-time information to the driver about vehicle health parameters, circumstances of roads, traffic jams and forewarning of weather. Progressive advancement of Intelligent Transport Systems (ITS), associated vehicles internet of vehicles known as the (IoV) [2] is the fundamental of communication required to share data about crisis and developing traffic dynamics has been expanded.

A current study by the IoT tracker service declared that the linked car market would expand by an additional 270% by 2022 including more than 125 million cars [3]. This also expands the size and complication of current working vehicle ad hoc networks, usually

known as VANETs. In addition to running challenges, the rapid proliferation of vehicle connections has also created critical security and information confidentiality concerning the evolution and expansion of VANETs design. From the literature review, it can be asserted that some threats related to privacy and infringing location privacy are more dangerous as they can lead to more advanced physical attacks such as trail and robbery.

In the next three sub-sections, we first explain the generic VANET architecture and then its unique characteristics. We also present the motivation behind the survey and the contributions of this work.

1.1. Generic VANET Architecture

The two main communication models in VANETs are classified as Vehicle-to-Vehicle (V2V) communication and Vehicle to Infrastructure (V2I). V2V communication is the ability of exchanged transmission between different vehicles while V2I is the communication between the vehicles and the road-side framework. The main communication module consists of Road-Side Unit (RSU), on-board unit (OBU), and trusted authority (TA) as shown in Figure 1. The RSU unit is fixed and made up of a transceiver that sends and receives information from the OBU and TA.

Therefore, it acts as a communication frontier between OBU and TA. RSUs can be placed at key indicators after particular interlude to provide reliable network coverage and systematic operation. Therefore, the distance between nearby road-side units is kept within the range of each sequential RSU. OBU is fixed in the automobile and works as a central point for receiving, processing and managing all data developed in the vehicle. It also serves as a source for exchanging data with the OBU of close by vehicles as well as the RSU. TA is basically the foundation of the whole ITS and is usually connected to the RSU via fiber optic cable or wireless media. It manages the trust and safety of VANETs. TA verifies the entire network components via RSU and identifies the OBU that sends malicious packets and cancels the target node. TAs is in the center of the town and is managed by governments. The VANET system model is briefly described in Figure 1 below. A more detailed survey on this can be found at [4].

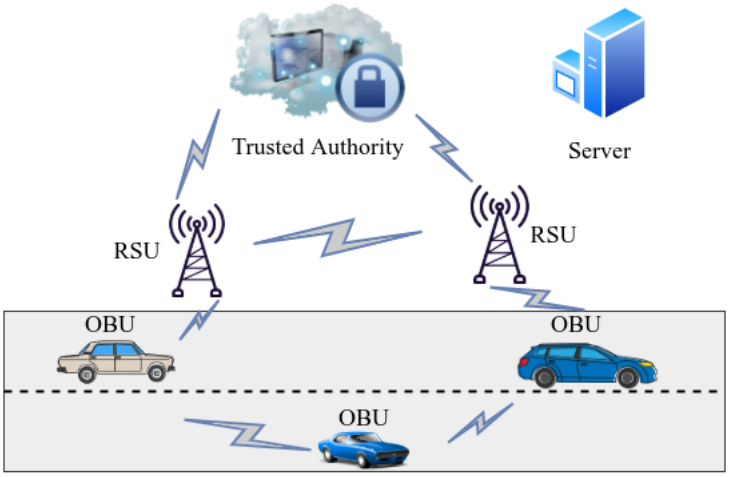

Figure 1. VANET Generic Architecture.

1.2. VANETs Characteristics

This subsection briefly explains the unique characteristics of VANET mainly mobility, storage and computing capabilities, dynamic topology, communication medium used etc.

1.2.1. Mobility

Because VANETs nodes are highly mobile, or move fast, it is often necessary to leave the localized network and participate in new configurations. These fast-moving

nodes can cause intrinsic communication interruptions or retard throughout V2V and V2I communications [5].

1.2.2. Storage and Computing Capabilities

The information interchange within VANETs depends on users linked at a particular time. Therefore, network bandwidth and adequate processing power are required to store, process and communicate important messages.

1.2.3. Real-Time Limitations

Regardless of the intrinsic delays between flexible platforms, some VANETs applications want the information to reach in real time. For example in fault discovery and collision prevention systems where the driver has minimum reaction time (several milliseconds) available to decode and react to the received message.

1.2.4. Dynamic Network Topology

VANET's network configuration continuously develops due to the mobility of vehicles as some nodes join and leave the network. Malicious nodes could benefit from these dynamic configurations, hiding their routes after compromising a particular network [6].

1.2.5. Frequent Network Disconnections

VANET's most disconnections are due to other issues such as high-speed movement between vehicles and weather conditions. Many vehicles on the road can also cause frequent amputations.

1.2.6. Communication Medium

VANETs use wireless communication same as Mobile Ad-hoc Network (MANET) but the nodes involved in VANETs have more mobility as compared to MANETs. Like other wireless networks, VANETs encounter security issues because of wireless communication [7].

1.2.7. Radio Transmission Depletion

The performance of Dedicated Short-range Communication (DSRC) radio communications has limitations associated with digital transmission in these frequency bands due to dispersion, diffraction, refraction, reflection and dispersing in city areas.

1.3. Motivation and Contribution

In VANETs, the connected vehicles and nodes of the VANETs environment contain road-side sensing and transmitting modules, traffic monitoring by the government, infotainment systems, and control systems etc. These devices share sensitive data with different protocols. VANETs are highly vulnerable to internal and external security attacks. For example, attackers can use the communication to steal personal information such as passenger details, travel times, tracked routes and destinations, range, and main locations. Furthermore, this data can be used to create selected personal profiles to launch multiple attacks. These attacks can be directed towards specific users or interfere with the whole transportation system, hence blocking the flow of traffic over a vast area. For example, movements can track or disrupt through spying on the victim's location data [8]. Therefore, location privacy in VANETs is an important design challenge to be considered.

Many survey papers are available to focus on security and the location privacy aspects of VANETs. However, to the best of our knowledge there is no comprehensive survey that explores and critically analyzes the existing state-of-the-art solutions based on its operational and security concerns for location privacy in VANETs. Our survey is different in terms of classification and categorization of existing threats to location privacy. Moreover, we emphasize mostly on the location privacy of VANETs so that can help researchers and developers to differentiate and choose best schemes during deployment of security mea-

sures against violation of location privacy in VANETs. Motivated by this, the contribution of this survey paper can be outlined as follows:

- First, we overview and explore state-of-the-art solutions available for location privacy in VANETs, and also discuss its safety and operational concerns.
- Secondly, we critically analyze the most obvious security attacks, identity thefts, manipulation and other techniques poised to location privacy in VANETs.
- Thirdly, we compare these state-of-the-art solutions based on various operational and security boundaries such as alleviation of execution, security performance efficiency, trade-offs, and service conveyance and present them in tabular form.
- Finally, this survey will help researchers to develop a deeper understanding of the location privacy in VANETs and the state-of-the-art solutions and the challenges present in its design and development.

The rest of the paper is structured as follows, Section 2 provides background overview, security and privacy requirements, present privacy threats to VANETs environment and specifically brief explanation of location privacy. In Section 3 of this paper, we discussed the related work some adversary models, privacy preserving schemes. Analysis and discussion in Section 4. Finally, Section 5 concludes the paper.

2. Background

This section consists of an overview of VANETs, it is important to understand privacy, security in a network of vehicles for that purpose following are VANETs security and privacy requirements. We also discussed location privacy and the existing state-of-the-art techniques.

2.1. Security and Privacy Requirements

In this subsection, we discuss the privacy and security requirements of VANETs. These requirements need to be considered while implementing or deploying the security, privacy techniques [9].

2.1.1. Short-Term Link-Ability

Short-term link-ability is a necessary attribute in Intelligent Transportation System applications. Let us say if a car receives two or three messages within a short time span, the driver on the receiving end will be able to check the origins of the messages. By adding short-term link-ability, we guarantee that a compromised OBU cannot impersonate several vehicles and unleash a Sybil-attack [10]. Vehicles in the vehicle network often relay messages with their speed, position and acceleration. To create a trajectory of surrounding OBUs, these are the signals that are used. Meanwhile the privacy of a user regarding his/her location is not affected because location privacy of a vehicle is not impacted by the minor increment [9].

2.1.2. Long-Term Unlink-Ability

Long-term link-ability is a fundamental location privacy requirement for vehicular networks. The intruder would not be able to recognize the vehicle by connecting messages received by a single vehicle to attributes such as vehicle position, vehicle model and applications [9]. In order to shield users from the link-ability of two or more consecutive locations, it is important to enforce tracking security. In mobile networks, the internet service provider (ISP) should not be able to link multiple successive user positions.

2.1.3. Anonymity

The process of hiding a user's identity is called anonymity. The term is usually used to necessitate the user's ability to use services or access some resource without disclosing his/her identity. This helps the individual to take steps without revealing his/her identity to third parties. Anonymity strategies include ways of identifying the collection of consumers that cannot see the face of those doing those acts.

2.1.4. Pseudo-Anonymity

Pseudo-anonymity ensures that users may access resources or services without having to disclose their identity, but they can still be held accountable for that use. Since the users can be accountable for the use and they are not completely anonymous, it can be viewed as conditional pseud-anonymity or reversible pseudo-anonymity. The accountability can be achieved by directly linking the user's actual identity towards some reference held by an entity such as the certificate authority, or an alias that will be used for processing purposes, such as an account number. Conditional pseudo-anonymity is essential if the identity of the violator is to be disclosed by the law enforcement authorities for the purposes of liability. There are parallels between pseudo-privacy and anonymity. Although all methods shield the identity of the user, pseudo-anonymity maintains a connection to the identity of the user for transparency because, in anonymity, the user becomes absolutely anonymous.

2.1.5. Accountability (Non-Repudiation)

The conditions of good reputation must be fulfilled for anonymity. Although secrecy helps preserve the identity of the individual, it is important to identify a mischievous or faulty car that created an incident for future punishment. Be mindful that pseudonyms are connected to knowledge that allows the Certificate Authority to supply documentation for the responsibility of a person who acts maliciously.

2.2. Threats in VANETs

By construction, road safety has been a significant concern since the advent of the automobile in 1885. With the introduction of VANET, vehicles and drivers are now vulnerable to cyber security threats, compromising network access, anonymity, stability and data confidentiality, as well as physical safety for passengers and facilities. We studied the existing literature and categorized the attacks on VANETs based on their characteristics, and compiled them into the following table. The table explains the threats that VANETs can face. We used the table parameter as follows: whether the attack type is centralized or not, attack effect the privacy of individual node, Certificate Authority (CA) is used or not, whether the solution has support for routing protocol, the cryptographic algorithm is used and how efficient the detection. Table 1 below shows security attacks against VANETs and their countermeasure.

Table 1. Comparison between VANETs location privacy schemes.

Solution	Attack	Centralized	Privacy of Node	CA Used	Routing Protocol	Crypto-Algo	Remote-Activation	Detection
[11]	Tracking	Yes	Yes	Yes	No	Yes	Yes	Good
[12]	DoS	No	Yes	Yes	Yes	No	No	Limitations
[13]	Sybil	No	Yes	Yes	No	Yes	No	Good
[14]	MitM	No	No	Yes	No	Yes	Yes	Good
[15]	Replay	No	Yes	Yes	No	Yes	Yes	Good
[16]	Spam	Yes	Yes	Yes	No	Yes	Yes	Effective

Many surveys are available in the literature they explain the types of attacks pertaining to VANETs. However, we categorized these attacks in tabular form based on various attributes such as whether the scheme has support for CA, attacks types are centralized or decentralized, and how VANETs nodes react during attacks. In most of the attacks the privacy of nodes is preserved while most of the attacks target those areas where no routing support is available. Most of the attacks can be traced because they are reporting back to the concerned authority such as RSU or any other Trusted Third Party (TTP). Therefore, there is a need to further investigate and analyze the state-of-the-art in location privacy in VANET and discuss their pros and cons accordingly.

2.3. Location Privacy

In vehicular ad-hoc networks (VANETs) it is possible and a great problem for vehicles to be tracked while in transmission with other vehicles or during communication with road-side infrastructure which can become a dangerous situation, this type of threat can lead to location privacy of vehicles users. Figure 2 shows location privacy assessment methods.

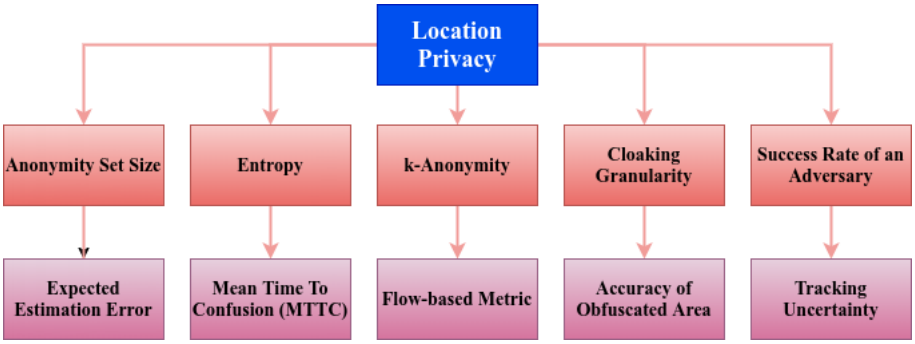

Figure 2. Location privacy assessment methods.

Several protection controls have been suggested in the literature [17]. However, this study focuses on the privacy measures used in the assessment of the following specific approaches to the position of privacy addressed in this paper.

2.3.1. Anonymity Set Size

The authors of [18], presented the concept of anonymity that they provided was a selection of all users willing to submit a single message that is clear to the global observer. It is believed that the global intruder is someone who has corrupted a group of nodes within a network. The definition has been used to model the Dining Cryptographers (DC) Network protection. According to [17] the ASS calculates the number of users that could be the target individual p. It is defined as the size of the region where the target user p will blend. where $\mid ASt \mid$ is the anonymity set of the targeted node. One of the drawbacks of this is that it does not bother taking up previous experience. This depends solely on the number of users in the program. The mixture of ASS and standardized entropy [19] does however provide a better privacy.

$$Priv_{ASS} = |ASt| \tag{1}$$

2.3.2. Entropy

Entropy is a method used in position safety, to quantitatively calculate the variance of the target. Measure of the quality of the cloaked location [20]. As a measure of secrecy, the confidentiality collection may be called an individual scale. In [21] the authors defined Entropy as the additional knowledge required for adversary user identification. As seen in the equation below, the adversary's approximate probabilities for each individual in the anonymity collection are shown by the random variable X. Entropy is extremely useful where we need more than once to measure privacy. Entropy of position anonymity is continuously measured as a result of adversaries' continuous surveillance. In [22], the author used entropy to calculate an adversary's precision in reporting the user 's role. Entropy may be expressed in mathematical terms as following equation, where N reflects the number of nodes in the secrecy collection and pi shows the likelihood of i being the node depending on the adversary's calculation. For mixed zones, standard entropy (degree of anonymity) is used. Normalized entropy is the ratio of entropy obtained from the road network to entropy obtained with the same collection of anonymity from the ideal mixed-zone Pairwise entropy has also been seen in a related way. Pairwise entropy is an entropy of two participants that are the only representatives of an anonymity party. Pairwise has

two mapping collections, two mapping parameters and two occurrences (entry and exit) [23].

$$Priv_{ENT}H(X)\sum_{i=1}^{n} pilog2(p(i)) \quad (2)$$

2.3.3. K-Anonymity

K-anonymity is achieved after the precise location of the users is extended to the enclosed regions so that there are at least k-users in each region. In location k-anonymity, protection of the privacy of the user is achieved by using the current location instead of using the historic locations. References [24–26] provide position k-anonymity strategies.

2.3.4. Cloaking Granularity

It was suggested to resolve the limitations of the k-anonymity "Cloaking granularity". In the case of cloaking granularity, the cloaked region should be greater than the threshold defined by the user [27]. Place k-anonymity does not prohibit the release of user details, it preserves the privacy of the consumer. Cloaking granularity does not require the identification of the individual to be revealed, but cannot shield users from attacks linked to identity in the case of public awareness of the user's identity.

2.3.5. Success Rate of an Adversary

A location privacy indicator used to calculate the probability of an attacker 's effectiveness in detecting a person the attacker is attacking. The writers in [17] draw our attention to the problem that if an adversary succeeds, he/she may undermine the contact channel or reveal the source of the letter.

2.3.6. Expected Estimation Error

This calculation tests the performance of the adversary in the reconstruction of the desired trajectory. In position secrecy, the approximate error of the competitor is determined by the predicted difference between the true outcome xc and the projected difference x using the distance metric. In the case of [28], the posterior probability is used to calculate the expectations of the adversary's estimations x based on the observations o. Generally, error-based metrics quantify the error of the adversary in making his calculation.

$$Priv_{AEE} = \sum_{x}^{n}(Pr)(o)(x, xc) \quad (3)$$

2.3.7. Mean Time to Confusion (MTTC)

Use of the entropy to calculate the time of uncertainty of the opponent with respect to the defined threshold. Time taken by the intruder to detect a trace properly. Flow-based metric, flow-based measurements use data on the mixed-zone to measure the efficiency of mixing theoretically. Accuracy of obfuscated area, relevance metric models the relative precision failure of the indicator with respect to the average precision that should have been reached in an ideal environmental condition. Tracking uncertainty, this parameter calculates the likelihood that the position of the sample belongs to a specific vehicle.

2.4. Attacks in Location-Based Security (LBS)

This portion identifies various types of attacks that are important to the position of privacy in the literature of Mobile Services and Vehicular Networks. Furthermore, we classify the attacks related to VANETs security requirements namely: Availability, Confidentiality, Authentication and Integrity [29], which are shown in Figure 3.

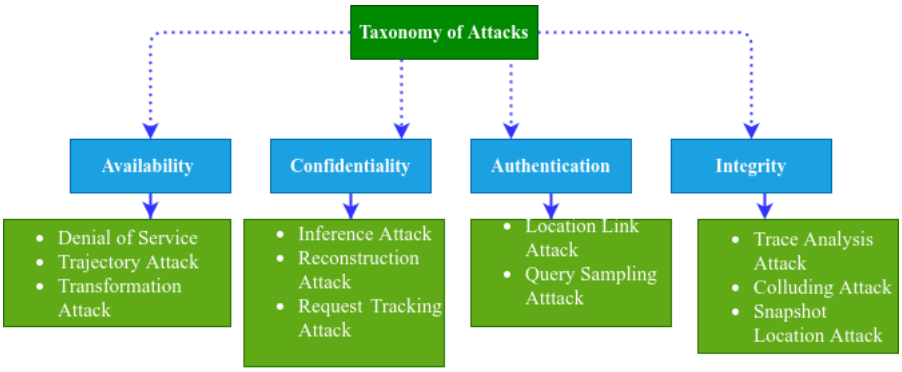

Figure 3. Classification of attacks.

1. *DoS*—Denial of service (DoS) is one of the most anticipated attacks in VANETs. This can be carried out by an internal or external malicious vehicle. The purpose of an adversary is to jam the communication between authorized communicating vehicles. The attack can also be launched in distributed manner called distributed denial of service (DDoS).
2. *Trace Analysis Attack*—In this attack, the adversary connects the traditional cloaking area to the user's mobility sequence. The chance can be calculated from the user's LBS registry at a separate position in the cloaked region [20].
3. *Colluding Attack*—Proof of the wrong location is created when two nodes collide with each other. For example, if one malicious node wants to show that it is in a wrong location, it may have an additional colluding node to jointly produce false location evidence to support it [30].
4. *Location Link*—An attack in which the location details used in the user query is used as a quasi-identifier to re-identify the identification of the consumer is defined as a role connecting the assault in [31].
5. *Query Sampling*—In the Query sampling the opponent uses the user's position details to relate the user's location to a specific application.
6. *Snapshot Location Attack*—The writers in [25] address inference attack close to trace research assaults. The user's potential path is tracked by inference, which depends on the user's past position.
7. *Request Tracking Attack*—In continuous LBS, the existence of the client enables queries to be tracked as the requests have a lifespan. A consumer who has been disguised with other users on several occasions during the query 's lifespan is susceptible to this attack [27].
8. *Trajectory Attack*—If a given trajectory is used by an LBS-server recipient to deduce the trajectory [32]. Trajectory assaults will also be carried out even though the user identity has been removes.
9. *Transformation Attack*—Previous results are used by the adversary to measure the transformation likelihood for each potential intersection turn [23].
10. *Reconstruction Attack*—The adversary tries to recreate the real trace by applying probability to incidents that could be linked to the user's path [33].
11. *Inference Attacks*—Similar to trace investigation assaults, Adversaries map past movements to assess potential locations [34,35].

3. Related Work

In this section, we broadly classify and review the literature into the privacy preserving schemes, trust management models adopted by researchers. The adversary's models and some other relevant schemes which do not fit this classification. Figure 4 shows privacy preserving schemes and trust management models.

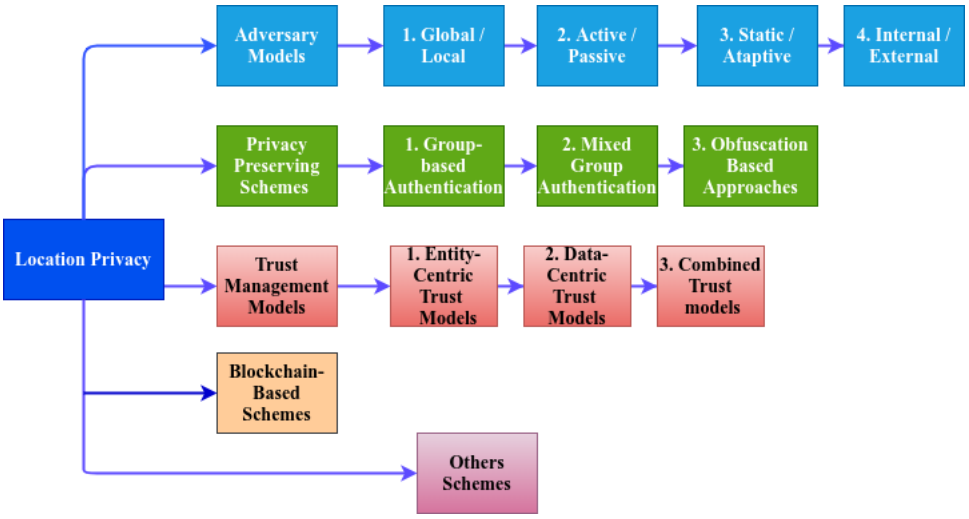

Figure 4. Privacy preserving schemes and trust management models.

3.1. Adversary Models

The methods suggested for the position of privacy in the literature have several specific characteristics. Some privacy indicators find the existence of an enemy of any kind. The writers in [36] found out that the more well informed the adversary becomes, the less anonymity he receives. The adversaries mentioned in the literature are listed as follows:

3.1.1. Global/Local

The opponent is defined by its context to be local or regional. External adversaries usually have access to the whole network, whereas local adversaries have access to a small portion of the network. For e.g., packet sniffers have access to a limited amount of RSUs installed at road intersections [17].

3.1.2. Active/Passive

Active adversaries are those that can interfere with the network by inserting/altering messages, whereas a passive adversary cannot change any message, they can only read the message and observe the information [37].

3.1.3. Static/Adaptive

An adversary that chooses the technique or strategy for an attack before launching it irrespective of how the attack progresses is a static adversary whereas an adaptive adversary observes the network by learning how the systems are configured and how the parameters are set [35].

3.1.4. Internal/External

A hostile node inside a network is known to be an internal adversary, whereas external opponents are often regional passive attackers. Examples of internal adversaries are untrusted LBS servers and TTP (anonymizers) in the context of LBS. Most scholars conclude the LBS servers are untrusted [38].

3.2. Location Privacy Preserving Schemes

Location privacy is characterized as the context within which an entity's identity remains unrelated to its actions, location and unique characteristics [39]. VANETs allow each vehicle to deliver a beacon message containing the required details, including the speed and direction of the GPS. The Administrator, TA and the authorized third-party provider are required to provide this detail. The beacon message is continuously demanded from the network, according to which every vehicle sends its ID on a continuous basis. This is further most often closely related to the driver of the vehicle or the owner that a

breach of location could further help the enemy harm the driver, owner of the vehicle. The identity of the vehicle must be obscured or isolated from its location for the safety of the driver. Therefore, many algorithms, schemes have been proposed [40]. The section also addresses recent privacy legislation for locations and presents a detailed overview of their functionality. To solve the location privacy issues different mechanisms are used such as K-anonymity, Group signature, Pseudonyms, Silent period and Mixed-zone.

Anonymization strategies also modify pseudonym mappings, interrupting the creation of continuous time series that could be the subject of statistical analysis. Unfortunately, the fast replacement of pseudonyms directly sacrifices ease of use and functionality. Other services, such as personalized refueling and dietary guidelines, calculated based on historical personality specific data, can have a negative effect. In view of the application of interest, these trade-offs involve careful choice of technologies. Some popular privacy preservation strategies are discussed below.

3.2.1. Group-Based Authentication

In the group authentication scheme, vehicles are distributed into smaller groups and a group leader is allocated to each group as stated in [41] proposed the Trust-text End of Authentication Mechanism (TEAM), an authentication scheme that allows participants to be co-located. Every participant authenticates to the chief, who then authenticates to the TA via the RSU. At intersections, group leaders may change. A new group is formed after taking turns [42]. The group leader may be a bus, a regular taxi service or a licensed public transport vehicle such as a well-known police patrol vehicle. When a single vehicle goes down or out of the party, you can switch between groups just like your cell phone moves between base stations. Nonetheless, the driver keeps the ID of the vehicle on his own and does not show it to the RSU or the TA. A recent study [43] demonstrates a new method recognized as Trustworthy VANETs Routing with Group Authentication Key (TROPHY) that uses symmetric and asymmetric encryption for authentication inside group members and TAs. This method takes advantage of all regular group-based authentication features with slightly different leader assignments.

Reference [32] proposed a group-oriented privacy security approach oriented on a post-quantum safe forget transfer protocol, built based on an effective NTRU cryptosystem. Similarly, group-led trust and authentication schemes were also discussed in several other studies [44], each with different methods in addition to maintaining the required location services. Offers the place of anonymity contrasts and critically analyzes the privacy strategies mentioned in this white paper. Advantages of each approach in terms of different operational and safety parameters, For example, ease of implementation, low and heavy performance under highway traffic conditions, personal-specific customized quality, location-based services and a summary of disadvantages. This scheme considers group-based authentication critically and is appropriate for traffic patterns that are similar in. In other words, a group where vehicles are often reconfigured to move in and out of the group can place a computational load on the leader of the OBU. At the other hand, if a malicious individual is part of a specific group, the privacy of each group member may be violated for a certain period.

Group-based authentication systems have many advantages and disadvantages when growing location-based security services to protect user privacy. Best of all, it is fairly easy to execute this system [45]. The computational load used by the community leader is heavier than the regular OBU, but this aspect can be overcome by assigning leadership to daily vehicles with better computing capabilities. This scheme is supposed to work equally well when considered for low and high traffic. However, if the consumer remains in a specific community for a longer period of time (e.g., on a highway) and the members of the group stay the same, then you can track the vehicle easily. As a result, the performance of highway traffic is considered weak. In addition, TA cannot provide personalized service to the car because it does not have access to the true identity of the car.

3.2.2. Mixed Group Authentication

A simple mixed group scheme establishes mixed areas in various parts of the town where vehicles can join it and quit. Vehicles change their pseudonyms at the same time as they enter the mixed zone, and their Identities change as they leave the same mixed zone. As a result, trackers cannot track vehicles entering the mixing zone under a given pseudonym and leaving under another pseudonym, as suggested by [46]. Nevertheless, issues occur when the amount of traffic is small. In this case, building several mixed zones in different parts of the city can solve the issue of privacy. One similar strategy was proposed by [47], called the Urban Pseudonym Strategy (UPCS). This approach produces silent mixed zones (SM) at different signalized intersections in the area. This method needs a high bulk of traffic. The drawback of this scheme is that targets remain traceable between mixed areas, which expose them to privacy attacks. One more variant of the traditional mix-group approach is the Velocity-Based pseudonym Change (VBPG) approach [48]. This approach implies a change in the nickname depending on the velocity classes. Here, classes are formed based on the speed of each vehicle. Vehicles that have similar speed and are identical to the same RSU have been collected together and consequently validated by TA using the same username. This makes it impossible for an attacker to recognize and trace specific automobiles in a particular community.

The UPCS and VBPG approaches are identical as they both have the essential features of the mixing groups. UPCS can be called a subclass of VBPG. Because Basically VPGB approach is followed. In other terms, you change the user ID by joining and exiting the Mix-group. Nevertheless, in addition to its location, VBPG also integrates a variable for user speed, ensuring the sharing of pseudonyms between nodes with identical patterns of activity and increasing resistance to malicious pseudonym monitoring. In the latest study proposed by [49], the writers introduced privacy security via modifying pseudonyms based on the number of nearby vehicles and their location. Many other similar efforts have also been made via mixed group-based, Pseudonym-Driven Dynamic ID assignment to authenticate authentic VANET knobs while hiding position information have adopted an anonymous approach. Uncertainty (or entropy) is the power to maintain the position protection pseudonym scheme. The Mix-group scheme focuses on connecting hotpots near transport to the extended Kana evolution domain. Increasing the storage area of the vehicle increases confusion and improves the security of privacy. Mix-Group provides excellent confrontation to Brute Force crypto attacks through authentication and encryption techniques.

Timestamps avoid replay attacks as well as guard against spoofing such as legitimate RSUs or forging RSU messages. When local traffic is low (to remove pseudonyms), the attacker will listen to the safety message of the OBU and then record the probabilities and frequencies to chart the probability distribution and track the target vehicle. However, the Mix-Group operates with several pseudonyms, enabling vehicles to pass vehicles and swap pseudonyms with new areas. If this change occurs in a very huge group, it will be very tough for an invader to keep track of a particular vehicle. For unauthorized traffic in a mixed party, fake data transmission within the party is possible. However, the same can be avoided from the spoofed malicious code.

In addition, by introducing digital certificates in OBU, you can prevent forgery. It also addresses a related approach. Mixing-Group schemes that focus on a wider variety of benefits and are easy to implement. Nevertheless, frequent adjustments to Kana require strong OBU and RSU computational resources. Low-traffic areas, the probability of monitoring is high due to the limited number of participants involved in the pseudonym exchange. The scheme can work well in urban models. However, VBPC technology is less successful in road/highway settings, as vehicles do not cross over regularly. In addition, the VBPC approach allows you to track known-speed vehicles by leveraging the creation of mixed zones to calculate vehicle entry and exit times. As with personalized service, the true identification of the driver is never established, and it is not possible to provide

tailored identity-based customer support. Precise Location-based services that can extend to be used quickly.

3.2.3. Obfuscation-Based Approaches

Obfuscation strategies can make tracking hard by reducing the precision of position data and growing the time interval between messages received by OBU. This method works well in situations where LBS do not need precise location information to provide an appropriate level of quality of service (QOS). Reference [50] proposed an information theoretic method that uses Markov chains to induce certain pre-calculated location errors. The sum of error is estimated when checking that the LBS are usable, but the position specificity is decreased, and a new nickname is given. Selection of pseudonyms is often randomized by first sorting out all likely pseudonyms. The method mentioned represented the entire traffic population, assuming that the user had very little knowledge of the number and characteristics of the other users available. The location of each user shall be recorded along with a calculated error correlated with a certain probability.

The Probability Distribution Function (PDF) can present the location and velocity of each consumer. The purpose of the obfuscation feature is to modify the PDF for all users' changes to the victim's PDF source remain unclear to the offender. The aim of this obfuscation function is to make unaware of the user's historical data and so it does not overlap with it. User locations are known as independent and uniformly distributed variables, based on Markov chains to capture their dependency over time [50]. Possible locations are related to the number of Markov-row states, Whitman, and so on [51]. Three new blotting techniques, namely N-Rand, N-Mix and N-Dispersion algorithms, were introduced. By comparing the average distance, maximum distance and minimum distance between the original position and the obfuscated direction, we evaluated the efficiency of these algorithms. Another recent work carried out by [11] used privacy with the aid of the Circle Based Dummy Generation (CBDG) algorithm while using a trustworthy third party. The proposed solution benefits both from obfuscation and anonymization techniques by sharing location information between neighboring vehicles in a two-step verification process [12]. Many other parallel efforts [34] have used a variety of obfuscation mechanisms to hide accurate location data while providing an appropriate quality of service. Upon evaluating the pros and cons of the obfuscation method, the algorithm can be repeatedly applied at the OBU, so its implementation is considered easy. Under light traffic conditions, even if it is relatively noisy, the attacker can monitor the target vehicle within the range set by the noise level of the system.

Nevertheless, crowded urban areas and road, highway settings contribute to the confusion and obscure certain users' position. This scheme provides a personalized service extension for the customer, since the TA will identify the user uniquely. The compensation provided, though, cannot provide position related facilities. The positioning accuracy does not indicate the user's exact position.

3.3. Trust Management Models in VANETs

The Methods for managing confidence depending on a trusted Third-Party Partnership (TTP) are proposed. Reference [13] are developing a chief evaluation scheme for carriage and RSUs to define and remove hackers from the network. It provides the trust and credibility details of unethical records to ensure the prolonged reliability of VANETs [52]. introduced a scheme to test the reliability of messages. The main purpose of this scheme is to focus on robustness and error tolerance of the fleeting unavailability of the main server. In [15] the scheme proposes a Reputation-based Global Trust Establishment (RGTE) scheme for exchanging trust information in VANETs based on law. Above all, confidence management approaches based on TTP need a reputation server to create a framework for managing world reputations. Nonetheless, these infrastructures can be a goal for hackers, the total cost of maintaining regular TTP functionality is high and may be higher or recovery from accessing. The centralized networks are also not good for VANETs. One

more approach to developing secure protection in VANETs is the use of hubs. Reference [16] develop a trust-conscious research learning automated intrusion detection system (T-CLAIDS) for secure management in VANETs. It confides on the high size of vehicles in a given area to build a classifier that can be shared to the so-called Collaborative Trust Index (CTI) to detect any illegal behavior. Table 2 shows VANETs location privacy schemes used in different papers. Table 3 shows comparison between VANETs location privacy schemes.

Table 2. VANETs location privacy schemes used in different papers.

Ref	Category	Salient Feature	Goals	Limitations	Parameter
[53]	Silent period	Enhances anonymity, transmission control capability	Address location privacy, tracking attacks	No comparison	Anonymity set size
[54]	Mix-group	system initialization, key generation, pseudonym exchanging, group leaving revocation protocol	exploit the meeting opportunity for pseudonym changing, improve the location privacy	Many assumption for implementation	Location privacy
[55]		OBU safety message generation, verification OBU fast tracing	support a multi-level confidentiality, privacy	Limited analysis with threat model	Multi-level authority
[56]	Silent period	Pseudonym changing at small social spot, Pseudonym changing at large social spot	Achieving the location privacy based on pseudonyms changing technique	No comparison with other methods	Location privacy, Anonymity
[46]	Mix-group	System initialization and key generation, Group join, Pseudonyms exchanging, RSU signing protocol, Group leaving, Revocation protocol, Conditional tracking	Exploit the meeting opportunities for pseudonym changing, Improve the location privacy preservation	Many assumptions needed to understand implementation	Location privacy
[57]	Obfuscation Scheme	The true path of the vehicles is hidden over long trajectories	Location tracking	Location entropy	tracking success

Table 3. Comparison between VANETs location privacy schemes.

Performance Feature	Group-based	Mix-Group	Obfuscation
Computation at RSU	Average	Average	Low
Simplicity of implementation at OBU/RSU	Yes	Yes	Yes
Acculturation-based services	Yes	Yes	No
Performance in low-traffic conditions	High	Low	Low
High performance in freeway model	Low	Average	High
Computation at OBU	Low	Average	Average
Low Performance in urban (multi-velocity multidirectional) model	High	High	High
Adapted recommendation services	No	No	Yes

Reference [58] use the credibility of network services and develop a two-phase model to enable and to cooperate during combine formation and to identify illegal behavior after combine formation. Reference [59] is developing an effective and insignificant intrusion finding system named AECFV to secure VANETs from the most dangerous attacks. AECFV uses a stable clustering algorithm to pick the Cluster Head (CH) based on automobile and belief level. Reference [60] use Petri Networks to model dynamic automobiles capable of making decisions preceding the reliability of warning mails based on a successful collabora-

tion perfect for VANETs. Such approaches boost support between automobiles in VANETs by creating a bunch and choosing a CH according to a particular procedure. Security info collected from all automobiles in the bunch is used to measure the trustworthiness of automobiles and communications. Agreement is reached by collaboration between all vehicles. The main downside of bunch-based confidence organization approaches stems from the short nature of VANETs. Typically, the accuracy of the CH conclusion is contingent on the size of the bunch, which reduces those bunch-based methods in regions of bad automobile mass. In addition, the communication among each automobile in VANETs is short-term so that it is hard to establish a secure bunch for the purposes of dependence administration. It is realistic to organize regionalized faith prototypes that are not entirely dependent on static setups. These prototypes can be categorized into: (1) Entity-Centric Trust Models (2) Data-Centric Trust Models and (3) Combined Trust Models.

3.3.1. Entity-Centric Trust Models

The goal of entity-centric confidence models is to estimate reliability of automobiles. The key approaches to do this professionally and precisely are to create a standing system or to mark decisions based on the opinions of neighbors. There is a variety of traditional plays. Reference [61] propose a confidence and credibility model-based proposal (TRIP) that relies on RSUs to differentiate between cruel and selfish automobiles in VANETs by great competence and exactness. Three dissimilar sources of knowledge are measured when calculating the Ea credibility ranking: Direct prior experience with the mark automobile, references from the neighboring automobiles and recommendations from the vital specialist. Reference [62] suggest a dispersed dependence model (DTM2) for the allocation of acknowledgments to automobiles with stable organization. Own-selection systems are set up in a system that would drain the credit of misbehavior automobiles. Commonly, the correctness of data from other automobiles can be sure. As automobiles traffic moves fast on the road, it is hard to gather enough information to calculate the standing score of an exact bulge.

3.3.2. Data-Centric Trust Models

Data-centric confidence models concentrate on approximating the reliability of the data received. To reliably check the consistency of the information obtained, the prototypes need mutual data from several bases, such as national automobiles or RSUs. Reference [63] constructs a trust typical to estimate the reliability of a communication directly constructed on several variables, including gratified resemblance, content clash and path resemblance. Reference [64] suggest a deterministic method to calculate the self-reliance near the transmitted communication by using the transmitted signal strength (RSS) for the measurement of spaces and the geolocation of the automobile (location coordinate). Reference [65] Propose email-based joint dependence and social network trust to create and maintain data trust. Latency and data sparsity are the main disadvantages of data-centric models. Great records of data from numerous bases, respectively, hold dismissed data that increases potential or overwhelms important data. In comparison, information sparsity is established in VANETs.

3.3.3. Combined Trust Models

The focus in this category is on to gather the object and the information. Combined trust models not only assess vehicle confidence, then also compute the reliability of information. Thus, these prototypes have the advantages and disadvantages of data-centric and entity-centric trust models. Li and Song's proposed Attack-Resistant Faith Managing Scheme (ART) [66] approximates the reliability of mutual automobiles and communications for coping with hateful attacks in VANETs. The reliability of the information is calculated based on the data collected from various automobiles. The dependability of the node shall be calculated based on practical trust and recommendation expectation, which shall mean correspondingly, whether the nodule will achieve its functionality and the close of trust of

the approvals. The suggested arrangement will not yield into explanation the information sparsity that remains prevalent in VANETs.

3.4. Blockchain-Based Scheme

Presently blockchain technology have gained popularity among researchers because of its widespread use in many fields, including academic, finance, banking and medicine. More specifically, blockchain composed of an unlimited number of blocks which are connected in a sequential manner to form a blockchain. The blockchain is effective due to the features such as decentralization, immutability, transparency, shared security, anonymity, and more efficient for untrusted environments [67].

Various types of blockchain-enabled security models have been introduced recently. The paper [68] proposed an efficient privacy preserving data communication architecture which is based on a blockchain model to ensure privacy in cluster-based VANETs. They leverage a rainfall optimization algorithm (ROA), the vehicles are grouped into various clusters and a cluster head (CH) is selected for each cluster. The ROA-based clustering along with blockchain-based communication is known as ROAC-B technique. First, the vehicles are grouped and then the transmission is initiated using blockchain. The data is generated at random depending on parameters such as node count, grid size, and communication range. Clusters are made according to the features of nodes such as navigation, speed, position etc. To make an effective clustering a node must reside in a single cluster. Consequently, every cluster has a CH which is responsible for the entire cluster and identifies entering or leaving nodes. As a result it provides load balancing and creates a minimum overhead on the network.

In VANETs infrastructure, blockchain technology play a vital role in authentication of vehicles because of the fact that any vehicle can access the past event if the information is placed in the public blockchain [69]. Application of existing blockchain is not sufficient to the VANETs environment, as transaction form of event messages is adopted instead of bitcoin transaction for the cryptocurrency feature. To address medium access control (MAC) layer threats, the work proposed in [70] is based on trust-based that make use of blockchain technology to improve security and privacy to thwarts MAC layer attacks. They integrate blockchain with MAC packet structure to achieve secure communication between VANETs components. Every block is composed of vehicle i (V_i) , identity of the vehicle i (ID_i), message (M_i), timestamp (t_i), hash value and transaction root value. Safety messages are involved here and blockchain act as a medium of trustworthiness for event messages. A public blockchain is considered to store information of all the nodes based on geographical region. According to the blockchain whether public or private, various set of consensus protocol are offered. Hence, security level of blockchain is also depends on the consensus protocols.

3.5. Other Schemes

Reference [71], presented a new baseline metric for the analysis of mixing effects at possible mixing zone locations. The optimum mixing zone structure can be studied using mixture optimization techniques. They describe a mixing zone as a region of a specified form and scale that can be defined anywhere. The mixing influence of the mixing zone is calculated prior to the extension of the mixing zone using flow-based metrics. These schemes mostly do not ensure full privacy in situations where changing pseudonyms inside a low-traffic environment. However, the scheme depends on fixed mixed zones that are planted on road-side changing pseudonyms in mixed zones make it more difficult for an adversary to learn anything about their identity. Reference [72] proposed modifying the nickname to social sites, which are simply public areas, such as where the traffic light turns red or at the corner of a parking lot or a shopping center. Two basic pseudonym shift approaches are suggested in these articles. Both cars stuck at the signalized intersection in front of the red light, change the username when the traffic light turns orange. The parking area outside the shopping center will change its name shortly before entering the parking

lot. By this technique, better location privacy can be achieved when vehicles changed their pseudonym near highly social spots. can also assist vehicles to change their pseudonym at the right place and right movement.

Reference [73] suggested a pseudonym reform policy focused on a road-side network, named the Vehicle Position Privacy Zone (VLPZ). The VLPZ concept is close to the current road-side facilities, such as petrol stations, charging points for electric cars and toll booths. The simple VLPZ is made up of two pieces. (i) A single entry point called a router, and (ii) an egress level called an aggregator. Vehicles reach at VLPZ one after the other on one lane. Once the car enters the router, it ceases transmitting protection signals and moves to a VLPZ lane that is arbitrarily and secretly allocated to the router. Vehicles can remain in the VLPZ for a random period. For e.g., if the VLPZ is placed at a gas station, it is time for the driver to fill the fuel tank of the car. Vehicles must change their pseudonym before they leave the VLPZ via the aggregator. However, the order of exit varies from the order of entry, as the time of residency of the car is arbitrary. The key usage of multiple lanes for this tactic is to confuse the opponent. In reality, if the vehicle starts transmitting safety signals before reaching the VLPZ, the enemy does not know the lane of the vehicle or anticipate when the vehicle does exit the VLPZ. Therefore, the First-In-First-out (FIFO) attack cannot be carried out, as the final order and the start order are distinct.

In this paper [74], found the path and number of vehicles inside the range to be mixed background parameters. The car senses k neighboring vehicles at a distance less than the minimum distance and updates the username even if it has a specific path within the range of contact. In the simulation, the total distance is assumed to be 4.25 meters. References [75,76] suggested a Density-based Privacy Location (DPL) approach. It is based on a zone known as a nickname that affects the K intensity level. When a (k-1) neighborhood is located inside the set, the vehicle must adjust its nickname inside the K density field. The method of changing the pseudonym of vehicles continuously or at some stage it is accepted, is a solution in VANETs. Reference [76] introduced changes to [77]. In a mixed context, the author suggested adding rpm, gap between vehicles and road segments. They also recommended that bits (flags) be included in the protected post. A vehicle shall change its nickname if k neighboring vehicles have the same rank as themselves and its flag is equivalent to one. The goal of these changes is to maximize the probability that several automobiles can update their nickname at the same time. Reference [78] suggested a basic nickname shift technique named SLOW (low-speed silence). This approach is focused on the principle of wireless silence. In reality, the author indicated that if the speed was less than 30 km/h, the car should turn off the radio communication and adjust the username during radio silence.

Reference [79] present a strategy called SPCP (Synchronized Pseudonym Change Protocol). Vehicles are self-organized as a community in SPCP. Each community is controlled by the leader of the party. The leader of the party arbitrarily chooses whether to modify the identity of a member of the group. Both participants must be informed as the username shift process happens. In this method, each participant recognizes the community identity as a temporary nickname, each car terminates the party, and its username must therefore be modified. Reference [79] the program is introducing a new measure that is robust to inference attacks. Attackers can detect users with side details or estimate attacks. Multiple blend zones will be configured to preserve the anonymity of the location of the customer. Although the location of the mixing zone is a complicated question for Np, two optimization algorithms are used depending on the uniformity of the mixing zone. If the user has no traffic knowledge, a single traffic mixed-zone placement algorithm is used. The non-uniform traffic combination region placement method is used.

Interactive vehicles in the network have often developed a reputation for their behavior to improve the degree of cooperation [47]. Reference [80], they suggest a method of secrecy and trade for changing pseudonyms at road intersections. This method is based on two protocols. The first is to require vehicles to alter pseudonyms based on road-side traffic, and the second is to secure the mixing zones [4]. Motivational methods have been

suggested to reduce selfish vehicles inside the network. This strategy offers opportunities for automobiles during the username transition cycle to encourage engaging automobiles to eliminate self-interested vehicles. In consideration of the impact of vehicle density, they suggested an approach to the prevention of connection attacks without considering the effect of pseudonym warning during mixed-zone creation simulated mixed-zone solution has been proposed [73] to manage unbalanced vehicle capacity.

Reference [9] proposes a user-centric game-theoretic mixed-zone methodology that tests the progression of position privacy over time and examines its activity on smartphone, car and delay-tolerant networks. They claim that even though the risk of position anonymity is minimized by cell nodes, the utility gained by several pseudonyms may be jeopardized in uncooperative scenarios. Carry out a static review of the game with full details to reach a pure and mixed Nash equilibrium. Using the Bayesian approach, we are studying incomplete information scenarios where nodes are not fully aware of the payoff of adjacent nodes. They aim for a symmetrical equilibrium where all the nodes agree with the same likelihood and evaluate a complex variant of the game that reveals how to cope with ambiguity.

4. Analysis and Discussion

The precise position details of the customer must be secured from unwanted individuals. The history of the consumer including the geographic details of the existing and historical positions of the consumer, including points of interest, shall not be released to unauthorized persons. In Vehicular Ad-hoc Networks (VANETs) it is possible and a great problem for vehicles to be tracked while in transmission with other vehicles or during communication with road-side infrastructure which can become a dangerous situation, this type of threats can lead to location privacy of vehicles users. Table 4 shows VANETs location privacy schemes used in different papers.

Table 4. VANETs location privacy schemes used in different papers.

Ref	Computation Overhead	Communication Overhead
[81]	Medium	×
[82]	High	High
[83]	Medium	Medium
[84]	×	×
[85]	Low	×
[86]	Low	Medium
[87]	Low	High
[88]	Medium	High
[89]	Low	Low

The following conclusions can be drawn from the analysis of these state-of-the-art, discussed above.

- The choice of the best location privacy technology depends largely on the standard and type of service and the computing resources available on the VANETs node.
- Obfuscation is a good choice if the sponsored LBS is for a personalized, user-specific history-driven recommendation service.
- If you need an accurate LBS service, then choosing a group-based or group-mixed approach may produce the desired results.
- As far as mixed party strategies are concerned, group-based authentication is preferred for VANETs' low-traffic or comparable speed and traffic trends as seen on highways.

- Due to frequent changes in pseudonyms, mixed group authentication schemes introduce more overhead computation relative to community-dependent schemes.

Location privacy schemes can be classified into two types, the disturbance of ID (anonymization) and the disturbance of position (obfuscation). Both approaches are similar from a security and operational perspective, as location privacy can be increased at the expense of service quality. However, their implementation is very different. Anonymization focuses primarily on protecting the identity of the user by protecting the Mapping between users and locations monitored. User mappings are switched on and off to inhibit and disable statistical analysis. The statistical analysis in networks uses a continuous time series that may match the user's previous history. On the other side, obfuscation-based techniques ensure the secrecy of locations by intentionally sharing incorrect knowledge of the location over the network.

5. Conclusions

The threats to data privacy are stealthy, asymmetric and global, being passive in nature. Modern cyber-physical devices, such as VANETs provide very lucrative targets for stealing private-identifiable material, extending these vectors of danger and techniques of attacks. Location-infringement of a mobile VANETs node may result in physical attacks that are essential to protection, such as mugging and stalking. This paper provided an outline of the different strategies for preserving the privacy of roles in VANETs used in different papers. We first discussed the fundamentals of VANETs design and types of risks. After this, we discussed location privacy and thoroughly examined some of the new privacy management strategies. Security services in the literature have been discussed with advantages of the proposed solution. Researchers have proposed different solutions to enhance the location privacy regarding security of VANETs, they also have improved their solutions to reduce the consumption of resources. Most security functions need more resources because of large operations. Preserving the privacy of drivers and passengers in the location is an important field of study and there is an urgent need to further improve the privacy frameworks to render them reliable and effective under various circumstances. In the near future, we are committed to extend this paper to include key management protocols as they play a vital role in the location privacy and security of VANETs.

Funding: This research is supported by Aarhus University, Denmark.

Data Availability Statement: Not Applicable, the study does not report any data.

Acknowledgments: This research work is funded by Aarhus University, Denmark.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. WHO. *W. H. Organization, Global Status Report on Road Safety 2015*; World Health Organization: Geneva, Switzerland, 2015.
2. Alam, M.; Ferreira, J.; Fonseca, J. Introduction to intelligent transportation systems. In *Intelligent Transportation Systems*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 1–17.
3. Bhatia, H. 125 Million+ Connected Cars Shipments by 2022; 5G Cars by 2020; Available online: https://www.counterpointresearch.com/125-million-connected-cars-shipments-2022-5g-cars-2020/ (accessed on 15 February 2020).
4. Lu, Z.; Qu, G.; Liu, Z. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 760–776. [CrossRef]
5. Dhamgaye, A.; Chavhan, N. Survey on security challenges in VANET 1. 2013. Available online: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.300.3967 (accessed on 15 February 2020).
6. He, Z. Structure based or structure free? Topology management in VANETs. In Proceedings of the 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–23 September 2012; pp. 1–4.
7. Mejri, M.N.; Ben-Othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. *Veh. Commun.* **2014**, *1*, 53–66. [CrossRef]
8. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [CrossRef]

9. Studer, A.; Shi, E.; Bai, F.; Perrig, A. TACKing together efficient authentication, revocation, and privacy in VANETs. In Proceedings of the 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, Rome, Italy, 22–26 June 2009; pp. 1–9.
10. Douceur, J.R. The sybil attack. In *International Workshop on Peer-to-Peer Systems*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 251–260.
11. Arif, M.; Wang, G.; Peng, T. Track me if you can? Query based dual location privacy in VANETs for V2V and V2I. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security and Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1091–1096.
12. Khan, M.N.; Rahman, H.U.; Almaiah, M.A.; Khan, M.Z.; Khan, A.; Raza, M.; Al-Zahrani, M.; Almomani, O.; Khan, R. Improving Energy Efficiency With Content-Based Adaptive and Dynamic Scheduling in Wireless Sensor Networks. *IEEE Access* **2020**, *8*, 176495–176520. [CrossRef]
13. Bißmeyer, N.; Njeukam, J.; Petit, J.; Bayarou, K.M. Central misbehavior evaluation for vanets based on mobility data plausibility. In Proceedings of the Ninth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications, Low Wood Bay, Lake District, UK, 25 June 2012.
14. Omar, H.A.; Zhuang, W.; Li, L. VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs. *IEEE Trans. Mob. Comput.* **2012**, *12*, 1724–1736. [CrossRef]
15. Li, X.; Liu, J.; Li, X.; Sun, W. RGTE: A reputation-based global trust establishment in VANETs. In Proceedings of the 2013 5th International Conference on Intelligent Networking and Collaborative Systems, Xi'an, China, 9–11 September 2013; pp. 210–214.
16. Kumar, N.; Chilamkurti, N. Collaborative trust aware intelligent intrusion detection in VANETs. *Comput. Electr. Eng.* **2014**, *40*, 1981–1996. [CrossRef]
17. Wagner, I.; Eckhoff, D. Technical privacy metrics: A systematic survey. *ACM Comput. Surv.* **2018**, *51*, 1–38. [CrossRef]
18. Chaum, D. The dining cryptographers problem: Unconditional sender and recipient untraceability. *J. Cryptol.* **1988**, *1*, 65–75. [CrossRef]
19. Diaz, C.; Troncoso, C.; Danezis, G. Does additional information always reduce anonymity? In Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society, Alexandria, VA, USA, 29 October 2007; pp. 72–75.
20. Xu, J.; Tang, X.; Hu, H.; Du, J. Privacy-conscious location-based queries in mobile environments. *IEEE Trans. Parallel Distrib. Syst.* **2009**, *21*, 313–326. [CrossRef]
21. Serjantov, A.; Danezis, G. Towards an information theoretic metric for anonymity. In *International Workshop on Privacy Enhancing Technologies*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 41–53.
22. Palanisamy, B.; Liu, L. Mobimix: Protecting location privacy with mix-zones over road networks. In Proceedings of the 2011 IEEE 27th International Conference on Data Engineering, Hannover, Germany, 11–16 April 2011; pp. 494–505.
23. Palanisamy, B.; Liu, L. Attack-resilient mix-zones over road networks: Architecture and algorithms. *IEEE Trans. Mob. Comput.* **2014**, *14*, 495–508. [CrossRef]
24. Gedik, B.; Liu, L. Location privacy in mobile systems: A personalized anonymization model. In Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), Columbus, OH, USA, 6–10 June 2005; pp. 620–629.
25. Kalnis, P.; Ghinita, G.; Mouratidis, K.; Papadias, D. Preventing location-based identity inference in anonymous spatial queries. *IEEE Trans. Knowl. Data Eng.* **2007**, *19*, 1719–1733. [CrossRef]
26. Chow, C.Y.; Mokbel, M.F.; Aref, W.G. Casper* Query processing for location services without compromising privacy. *ACM Trans. Database Syst. (TODS)* **2009**, *34*, 1–48. [CrossRef]
27. Pan, X.; Xu, J.; Meng, X. Protecting location privacy against location-dependent attacks in mobile services. *IEEE Trans. Knowl. Data Eng.* **2011**, *24*, 1506–1519. [CrossRef]
28. Bordenabe, N.E.; Chatzikokolakis, K.; Palamidessi, C. Optimal geo-indistinguishable mechanisms for location privacy. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014.
29. Sheikh, M.S.; Liang, J.; Wang, W. A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets). *Sensors* **2019**, *19*, 3589. [CrossRef] [PubMed]
30. Sabahi, F. The security of vehicular adhoc networks. In Proceedings of the 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks, Bali, Indonesia, 26–28 July 2011; pp. 338–342.
31. Gruteser, M.; Grunwald, D. Anonymous usage of location-based services through spatial and temporal cloaking. In Proceedings of the 1st International Conference on Mobile Systems, Applications and Services, San Francisco, CA, USA, 5–8 May 2003; pp. 31–42.
32. Mi, B.; Huang, D.; Wan, S. NTRU implementation of efficient privacy-preserving location-based querying in VANET. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 7823979. [CrossRef]
33. Shokri, R.; Freudiger, J.; Jadliwala, M.; Hubaux, J.P. A distortion-based metric for location privacy. In Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society, Chicago, IL, USA, 9–13 November 2009.
34. Cui, J.; Wen, J.; Han, S.; Zhong, H. Efficient privacy-preserving scheme for real-time location data in vehicular ad-hoc network. *IEEE Internet Things J.* **2018**, *5*, 3491–3498. [CrossRef]

35. Hara, T.; Suzuki, A.; Iwata, M.; Arase, Y.; Xie, X. Dummy-based user location anonymization under real-world constraints. *IEEE Access* **2016**, *4*, 673–687. [CrossRef]
36. Humbert, M.; Manshaei, M.H.; Freudiger, J.; Hubaux, J.P. Tracking games in mobile networks. In *International Conference on Decision and Game Theory for Security*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 38–57.
37. Petit, J.; Schaub, F.; Feiri, M.; Kargl, F. Pseudonym schemes in vehicular networks: A survey. *IEEE Commun. Surv. Tutorials* **2014**, *17*, 228–255. [CrossRef]
38. Niu, B.; Gao, S.; Li, F.; Li, H.; Lu, Z. Protection of location privacy in continuous LBSs against adversaries with background information. In Proceedings of the 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, HI, USA, 15–18 February 2016; pp. 1–6.
39. Corser, G.P.; Fu, H.; Banihani, A. Evaluating location privacy in vehicular communications and applications. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 2658–2667. [CrossRef]
40. Faisal, M.; Abbas, S.; Rahman, H.U.; Khan, M.Z.; Rahman, A.U. An Analysis of DDoS Attacks on the Instant Messengers. *Secur. Commun. Netw.* **2019**, *2019*, 1751285. [CrossRef]
41. Chuang, M.C.; Lee, J.F. TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks. *IEEE Syst. J.* **2013**, *8*, 749–758. [CrossRef]
42. Salem, F.M.; Ibrahim, M.H.; Ibrahim, I. Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks. In Proceedings of the 2010 Sixth International Conference on Networking and Services, Cancun, Mexico, 7–13 March 2010; pp. 156–161.
43. Cirne, P.; Zúquete, A.; Sargento, S. TROPHY: Trustworthy VANET routing with group authentication keys. *Ad Hoc Netw.* **2018**, *71*, 45–67. [CrossRef]
44. Ying, B.; Makrakis, D.; Mouftah, H.T. Privacy preserving broadcast message authentication protocol for VANETs. *J. Netw. Comput. Appl.* **2013**, *36*, 1352–1364. [CrossRef]
45. Mehmood, G.; Khan, M.Z.; Rahman, H.U.; Abbas, S. An efficient and secure session key establishment scheme for health-care applications in wireless body area networks. *J. Eng. Appl. Sci.* **2018**, *37*, 9–18.
46. Yu, R.; Kang, J.; Huang, X.; Xie, S.; Zhang, Y.; Gjessing, S. MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks. *IEEE Trans. Dependable Secur. Comput.* **2015**, *13*, 93–105. [CrossRef]
47. Boualouache, A.; Moussaoui, S. Urban pseudonym changing strategy for location privacy in VANETs. *Int. J. Ad Hoc Ubiquitous Comput.* **2017**, *24*, 49–64. [CrossRef]
48. Ullah, I.; Wahid, A.; Shah, M.A.; Waheed, A. VBPC: Velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET. In Proceedings of the 2017 International Conference on Communication Technologies (Comtech), Rawalpindi, Pakistan, 19–21 April 2017; pp. 132–137.
49. Zidani, F.; Semchedine, F.; Ayaida, M. Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach for location privacy in VANETs. *Comput. Electr. Eng.* **2018**, *71*, 359–371. [CrossRef]
50. Takbiri, N.; Houmansadr, A.; Goeckel, D.L.; Pishro-Nik, H. Limits of location privacy under anonymization and obfuscation. In Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017; pp. 764–768.
51. Wightman, P.; Coronell, W.; Jabba, D.; Jimeno, M.; Labrador, M. Evaluation of location obfuscation techniques for privacy in location based information systems. In Proceedings of the 2011 IEEE Third Latin-American Conference on Communications, Belem, Brazil, 24–26 October 2011; pp. 1–6.
52. Li, Q.; Malip, A.; Martin, K.M.; Ng, S.L.; Zhang, J. A reputation-based announcement scheme for VANETs. *IEEE Trans. Veh. Technol.* **2012**, *61*, 4095–4108.
53. Sampigethaya, K.; Huang, L.; Li, M.; Poovendran, R.; Matsuura, K.; Sezaki, K. *CARAVAN: Providing Location Privacy for VANET*; Technical Report; University of Washington Department of Electrical & Computer Engineering: Seattle, WA, USA, 2005.
54. Kang, J.; Yu, R.; Huang, X.; Zhang, Y. Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2017**, *19*, 2627–2637. [CrossRef]
55. Xiong, H.; Chen, Z.; Li, F. Efficient and multi-level privacy-preserving communication protocol for VANET. *Comput. Electr. Eng.* **2012**, *38*, 573–581. [CrossRef]
56. Lu, R.; Lin, X.; Luan, T.H.; Liang, X.; Shen, X. Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs. In Proceedings of the 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011; pp. 1–5.
57. Lim, J.; Yu, H.; Kim, K.; Kim, M.; Lee, S.B. Preserving location privacy of connected vehicles with highly accurate location updates. *IEEE Commun. Lett.* **2016**, *21*, 540–543. [CrossRef]
58. Wahab, O.A.; Otrok, H.; Mourad, A. A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles. *Comput. Commun.* **2014**, *41*, 43–54. [CrossRef]
59. Sedjelmaci, H.; Senouci, S.M. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Comput. Electr. Eng.* **2015**, *43*, 33–47. [CrossRef]
60. Ltifi, A.; Zouinkhi, A.; Bouhlel, M.S. Smart trust management for vehicular networks. *Int. J. Electron. Commun. Eng.* **2016**, *10*, 1128–1135.

61. Mármol, F.G.; Pérez, G.M. TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *J. Netw. Comput. Appl.* **2012**, *35*, 934–941. [CrossRef]
62. Haddadou, N.; Rachedi, A.; Ghamri-Doudane, Y. A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2014**, *64*, 3657–3674. [CrossRef]
63. Gurung, S.; Lin, D.; Squicciarini, A.; Bertino, E. Information-oriented trustworthiness evaluation in vehicular ad-hoc networks. In *International Conference on Network and System Security*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 94–108.
64. Rawat, D.B.; Yan, G.; Bista, B.B.; Weigle, M.C. Trust On the Security of Wireless Vehicular Ad-hoc Networking. *Ad Hoc Sens. Wirel. Netw.* **2015**, *24*, 283–305.
65. Hussain, R.; Nawaz, W.; Lee, J.; Son, J.; Seo, J.T. A hybrid trust management framework for vehicular social networks. In *International Conference on Computational Social Networks*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 214–225.
66. Li, W.; Song, H. ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2015**, *17*, 960–969. [CrossRef]
67. Prashar, D.; Jha, N.; Jha, S.; Joshi, G.P.; Seo, C. Integrating IOT and blockchain for ensuring road safety: An unconventional approach. *Sensors* **2020**, *20*, 3296. [CrossRef]
68. Joshi, G.P.; Perumal, E.; Shankar, K.; Tariq, U.; Ahmad, T.; Ibrahim, A. Toward Blockchain-Enabled Privacy-Preserving Data Transmission in Cluster-Based Vehicular Networks. *Electronics* **2020**, *9*, 1358. [CrossRef]
69. Babaghayou, M.; Labraoui, N.; Ari, A.A.A.; Ferrag, M.A.; Maglaras, L.; Janicke, H. WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles. 2021. Available online: https://www.mdpi.com/1057656 (accessed on 4 April 2021).
70. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors* **2019**, *19*, 4954. [CrossRef] [PubMed]
71. Humbert, M.; Manshaei, M.H.; Freudiger, J.; Hubaux, J.P. On the optimal placement of mix zones: A game-theoretic approach. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009.
72. Lu, R.; Lin, X.; Luan, T.H.; Liang, X.; Shen, X. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE Trans. Veh. Technol.* **2011**, *61*, 86–96. [CrossRef]
73. Boualouache, A.; Senouci, S.M.; Moussaoui, S. Vlpz: The vehicular location privacy zone. *Procedia Comput. Sci.* **2016**, *83*, 369–376. [CrossRef]
74. Gerlach, M.; Guttler, F. Privacy in vanets using changing pseudonyms-ideal and real. In Proceedings of the 2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring, Dublin, Ireland, 22–25 April 2007; pp. 2521–2525.
75. Liao, J.; Li, J. Effectively changing pseudonyms for privacy protection in vanets. In Proceedings of the 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, Kaoshiung, Taiwan, 14–16 December 2009; pp. 648–652.
76. Song, J.H.; Wong, V.W.; Leung, V.C. Wireless location privacy protection in vehicular ad-hoc networks. *Mob. Netw. Appl.* **2010**, *15*, 160–171. [CrossRef]
77. Buttyán, L.; Holczer, T.; Weimerskirch, A.; Whyte, W. Slow: A practical pseudonym changing scheme for location privacy in vanets. In Proceedings of the 2009 IEEE Vehicular Networking Conference (VNC), Tokyo, Japan, 28–30 October 2009; pp. 1–8.
78. Weerasinghe, H.; Fu, H.; Leng, S.; Zhu, Y. Enhancing unlinkability in vehicular ad hoc networks. In Proceedings of the 2011 IEEE International Conference on Intelligence and Security Informatics, Beijing, China, 10–12 July 2011; pp. 161–166.
79. Liu, X.; Zhao, H.; Pan, M.; Yue, H.; Li, X.; Fang, Y. Traffic-aware multiple mix zone placement for protecting location privacy. In Proceedings of the 2012 Proceedings IEEE INFOCOM, Orlando, FL, USA, 25–30 March 2012; pp. 972–980.
80. Ying, B.; Makrakis, D.; Hou, Z. Motivation for protecting selfish vehicles' location privacy in vehicular networks. *IEEE Trans. Veh. Technol.* **2015**, *64*, 5631–5641. [CrossRef]
81. Vijayakumar, P.; Chang, V.; Deborah, L.J.; Balusamy, B.; Shynu, P. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. *Future Gener. Comput. Syst.* **2018**, *78*, 943–955. [CrossRef]
82. Fan, C.I.; Hsu, R.H.; Tseng, C.H. Pairing-based message authentication scheme with privacy protection in vehicular ad hoc networks. In Proceedings of the International Conference on Mobile Technology, Applications, and Systems, I-Lan, Taiwan, 10–12 September 2008.
83. Johnson, D.; Menezes, A.; Vanstone, S. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63. [CrossRef]
84. Agustina, E.R.; Hakim, A.R. Secure VANET protocol using hierarchical pseudonyms with blind signature. In Proceedings of the 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, Indonesia, 26–27 October 2017; pp. 1–4.
85. Li, G.; Ma, M.; Liu, C.; Shu, Y. A lightweight secure VANET-based navigation system. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6.
86. Mohanty, S.; Jena, D.; Panigrahy, S.K. A secure RSU-aided aggregation and batch-verification scheme for vehicular networks. Available online: http://psrcentre.org/images/extraimages/12%20812573.pdf (accessed on 17 February 2020).
87. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]

88. Kang, Q.; Liu, X.; Yao, Y.; Wang, Z.; Li, Y. Efficient authentication and access control of message dissemination over vehicular ad hoc network. *Neurocomputing* **2016**, *181*, 132–138. [CrossRef]
89. Liu, J.; Li, J.; Zhang, L.; Dai, F.; Zhang, Y.; Meng, X.; Shen, J. Secure intelligent traffic light control using fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 817–824. [CrossRef]