A Survey on Location Privacy Techniques Deployed in Vehicular Networks

Hassan Talat*, Tuaha Nomani*, Mujahid Mohsin*, Saira Sattar†
*Department of Avionics Engineering-College of Aeronautical Engineering
†Department of Electrical Engineering-School of Electrical Engineering and Computer Science (SEECS)
National University of Sciences and Technology, Islamabad, 44000, Pakistan
{hassan.talat, nomani, mujahid.mohsin}@cae.nust.edu.pk, 14mseessattar@seecs.nust.edu.pk

***Abstract*—Recent advancements in embedded technologies, pervasive computing, and ubiquitous connectivity have revolutionized our daily lives, making them safe, efficient and convenient as never before. These evolving technologies have not only transformed our workplaces but are also reshaping our living habits, including the way we communicate, travel, learn, and relax. In the field of transportation alone, a huge influx of highly-connected, situation-aware and even self-driving vehicles has been observed recently, thus revamping existing automobiles into smarter, automated and safer vehicular networks. This exponential rise in vehicular connectivity has introduced new terminologies such as Vehicular Ad-hoc NETworks (VANETs) and the Internet of Vehicles (IoV), aiming towards road-safety, smart traffic management, and real-time information/incident sharing. However, these highly-connected vehicles have also introduced several novel security and safety threats both to the hosts and associated assets, inducing serious even life-threatening consequences. Compromise of location privacy and vehicular identity is one of such serious threats, which may be exploited by an adversary to launch sophisticated attacks including stalking, identity theft/manipulation or even tracking and sabotaging of VIP moves. Such threat vectors primarily exploit subtle vulnerabilities in resource-constrained communication protocols being deployed for vehicular connectivity as well as improper security configurations of associated systems. The threats can be countered by placement of robust network security techniques suiting the VANET environment. This survey paper aims to probe into these vulnerabilities of vehicular networks, classify associated security and safety threats, and ultimately asses various countermeasures to safeguard against privacy-breach situations. Besides presenting a holistic overview of emerging threats in vehicular networks, the paper critically analyzes some of the recent approaches (2008-2018) to safeguard against location privacy threats with reference to a range of operational and security considerations.**

***Index Terms*—Location Privacy, VANETs, Internet of Vehicles (IoV), Threats, Countermeasures, Survey**

I. Introduction

In recent past, an exponential rise in the number of road vehicles has been observed, owing to economic growth and increase in population. This, in turn, has significantly increased traffic congestion, road accidents, driver fatigue, and premature deterioration of roads and support infrastructure. As per the statistics presented by the World Health Organization (WHO), road accidents are the number one cause of deaths for the age group of 15-29 years and these accidents take around 1.3 million lives per annum globally [1]. This alarming rise in road accidents can be controlled by leveraging modern technologies for real-time reporting of information about vehicle health parameters, road conditions / congestions and weather updates to the driver. The on-going advancements towards Intelligent Transportation Systems (ITS) [2] and connected vehicles (commonly known as the Internet of Vehicles or IoV) have extended the much needed communication infrastructure for information sharing regarding emergencies and evolving traffic dynamics. A recent research by Counterpoint's Internet of Things tracker service predicts that the connected cars market is expected to further grow 270% by 2022 with more than 125 million passenger cars having embedded connectivity [3]. This will further expand the size and complexity of existing Vehicular Adhoc Networks, commonly known as VANETs.

Besides operational challenges, the rapid-pace adoption of vehicular connectivity has also raised serious security and data privacy concerns for evolving and expanding VANET configurations. In addition to the connected vehicles, nodes in a VANET environment may comprise of road-side sensing and transmission modules, infotainment systems, and government-operated traffic monitoring and control systems etc. These devices share sensitive information over a diverse range of protocols each containing a varying set of vulnerabilities [4]. An adversary may exploit this communication to steal personally identifiable private information, including passenger details, followed routes and destination, travel time, road mileage, and important addresses. This data can be utilized to create personality profiles of targeted passengers for subsequent launch of complex multi-staged attacks. These attacks may be conducted with the intent to target a specific user or to sabotage the complete transportation system, thus crippling the traffic flow over a large area. For instance, a VIP move can be tracked or sabotaged by eavesdropping victim's location data [5]. Therefore, among the privacy-related threats, breach of location privacy is even more dangerous as it can lead to more sophisticated physical attacks such as stalking, mugging or burglary (knowing the victim is away).

This paper presents a survey of some of the recently introduced location-privacy protection schemes for VANETs. We critically weigh these techniques with respect to a diverse range of operational and security parameters, such as the ease of implementation, security efficiency, performance trade-offs

978-1-5386-7729-2/19/$31.00©2019 IEEE

and service delivery.

The rest of the paper is organized as follows. Section II presents an overview and characteristics of VANET's environment. The emerging VANET threats including the privacy threats are briefly introduced in section III. Section IV presents and critically analyzes some of the key and recently-proposed location privacy protection schemes for VANETs. Lastly, section VI concludes the paper.

II. Overview Of VANETs

In this section, we provide an overview of the main components forming VANETs and the major communicating entities in the network. A typical VANET communication can be classified into two main categories, namely Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication [6]. Here V2V is the communication among different vehicles on the road and V2I is the communication between a vehicle and the road side infrastructure. The key communication modules comprise of an On Board Unit (OBU), Road Side Unit (RSU), and a Trusted Authority (TA). The system model of VANET can be understood with the help of Fig. 1, and is briefly discussed below. For further details, readers are directed to a survey by Lu et al [7].

A. On Board Unit (OBU)

The OBU is installed inside the vehicle and serves as a nerve centre to receive, process and manage all data generated within the vehicle. It also acts as a gateway to exchange data with OBUs of nearby vehicles as well as RSUs. The OBU is integrated with different on-board sensors such as those (a) measuring critical vehicle parameters such as engine health, conditions of brakes and lights etc, (b) monitoring collision detection and avoidance parameters, (c) tracking vehicle's location and orientation through GPS and gyros, and (d) managing infotainment/weather systems. Besides the sole controller of intra-vehicular communication, the OBU also receives real-time information from nearby OBUs and RSUs, including traffic updates, road accidents and route diversion, which it further relays to other OBUs over a mesh-topology.

B. Road Side Unit (RSU)

The RSU unit is kept stationary and it comprises of transceivers to receive and send information from OBUs and TAs. It, therefore, acts as an intermediate communication interface between OBU and TAs. RSUs can be deployed at important landmarks after specified intervals with an aim to offer reliable network coverage and efficient operations. Hence, the distance between adjacent RSUs is kept such that they stay in the communication range of each successive RSU. They typically have the function of extending the range of mobile VANET, run important reporting applications like accident reporting, weather forecast and provide internet connectivity to the nearby OBUs.

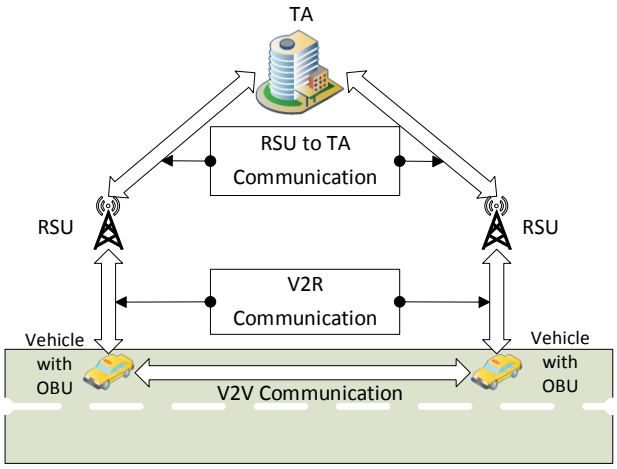

Fig. 1. System model of a typical VANET

C. Trusted Authority (TA)

This component is the backbone of the complete Intelligent Transportation System and is normally connected to RSUs via optical fiber cables or wireless media. The TA is responsible for management of security and trust in VANETs. It authenticates all the network components through RSUs. It is also responsible for identification of any OBU transmitting malicious packets and then revoking the subject node. TA is generally located at a central location within a city and is managed by state representatives. Since a TA handles large volumes of data and computationally-intensive cryptographic operations, therefore it requires high processing power and handsome storage space for data aggregation and analysis. More than one TAs can also be configured within a city to enhance coverage, distribute authority and to avoid a single point of failure. In such a case, high speed data links to share real time information between distributed TA architectures should also be made available.

D. Characteristics of VANETs

In order to understand the importance of trust management, security and privacy in vehicular networks the following unique characteristics of VANETs must be taken into account.

1) Mobility: As VANET nodes are highly mobile i.e. moving at high speeds, they are often required to leave localized networks and join new network configurations. These high speed nodes may induce inherent communication delays or disruptions during V2V and V2I communications [8].

2) Real-Time Constraints: Despite the inherent delays among mobile platforms, some VANET services require the information to reach in real-time. This requirement is more pronounced in, for example, obstacle detection and collision avoidance systems (as demonstrated in Figure 2), where only a small reaction time (few milli-seconds) is available to the driver for interpreting and reacting to the received message.

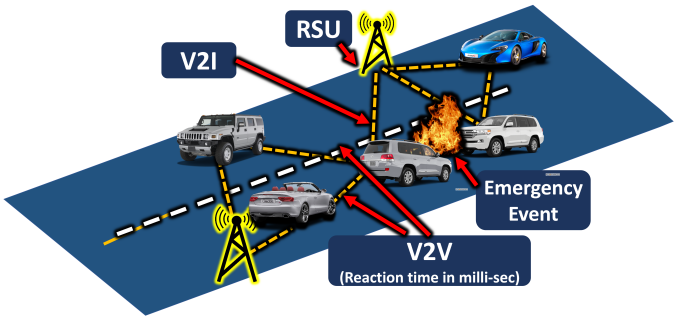

Fig. 2. Real-time communication constraints in case of any mishap

3) Computing and Storage Capability: The amount of information exchange within VANETs depends upon the number of connected users at a specific time. Therefore, a sufficient processing power, storage and network bandwidth is needed to process, store and communicate important messages. This requirement becomes even more prominent for the case of TA and RSUs.

4) Dynamic Network Topology: The network configurations of VANETs evolve continuously due to vehicular mobility, with several nodes joining and leaving a network. A malicious node can benefit from these dynamic configurations to conceal its tracks after compromising a given network [9].

III. Threat Perception in VANET Environment

By design, road safety has been a prime concern since the invention of automobiles in 1885. With the introduction of VANETs, vehicles and drivers are additionally exposed to cyber security threats as well, targeting to compromise network availability, information privacy, authenticity, data integrity, and even physical safety of passengers and infrastructure. This section deliberates upon some of the possible threat scenarios faced by VANETs.

A. Denial of Information/Services

Availability of requisite services at all times is of prime importance for smooth functionality of VANETs. Any vehicle in the network needs to maintain an active communication link with the RSU or nearby vehicles depending upon the network configuration. There are many attacks which are focused to sabotage the availability of services. Only a few of these are introduced below.

1) Denial of Service (DoS) Attack: The DoS attack can be performed either from within or outside the network. In DoS, communication towards a specific network node is jammed by overwhelming or saturating the victim or linked network resources. An advanced version of DoS is called distributed DoS (DDoS), where a coordinated attack is launched through either physically or virtually distributed positions, thereby overwhelming the network and thus, successfully creating enough traffic to deny legitimate services to an authenticated user. From VANET's perspectives, denial of services can be catastrophic if safety critical information fails to reach in time to the intended node [10]. Dynamic network topology, limited bandwidth and computing resources, as well as decentralized control in VANETs can allow malicious vehicles and fake RSU nodes to launch DoS attacks with serious consequences.

2) Jamming Attack: Jamming is a physical/MAC layer attack during which an area or targeted node is overwhelmed with a strong signal having the same signature characteristics as that of the genuine signal. Jamming in VANET is not far from reality (see for example [11]) and therefore, requires potent counter-measures at the receiving end to safeguard against these attacks.

3) Broadcast Tampering Attack (BTA) and Malware: A VANET attacker can plant a backdoor (both in fixed and mobile nodes) and then exploit it to disrupt the normal functionality of the network [12]. These malwares can also be used to broadcast fake safety instructions or warning messages to authenticated/ registered vehicles in the network, thus creating confusion.

4) Black Hole (BH) / Gray Hole (GH) Attacks: BH and GH attacks are very unique to mesh topologies since they exploit distributed and Adhoc nature of such networks while remaining stealthy. During these attacks, a malicious network node drops or filters selected data packets to cause denial of services, thus isolating the victim node(s) from communicating with the network [13].

5) Spamming Attack: During VANET spamming, the attacker generates a large quantity of false messages, carefully crafted to pose as genuine messages, and then transmits them towards the victim nodes/network. This undesired traffic can overwhelm the network with spam messages subsequently compromising/denying the quality of available services [14].

B. Breach of Information Privacy

Confidentiality is mostly referred as privacy or secrecy. It is the safeguard of information from unauthorized access. Typically, it is achieved by restricting access to the information through techniques of authentication and information encryption. Unauthorized entities can subsequently use network or user's information to cause system degradations through the following aspects [15].

1) Traffic Analysis: This is the most common type of attack where attacker simply observes encrypted network transmissions to carefully extract communication patterns through deep analysis. Traffic analysis can help an attacker to know about the volume and frequency of messages in a VANET to indirectly infer traffic conditions and further target a marked victim. This can also lead to information that can subsequently be used to launch further sophisticated attacks such as DoS / DDoS.

2) Eavesdropping Attack: In this technique, the attacker passively records private information of a VANET node or meta-data from the network. This information can be car owner's identity, location, traveling habits, or frequently visited spots, which can further be utilized to launch complex attacks on any vehicle of interest [16].

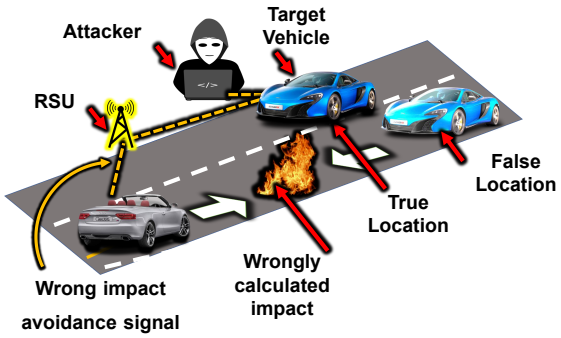

Fig. 3. False location generation by attacker

C. Masquerading

In this type of attack the attacker impersonates as a genuine vehicle (or RSU) to eavesdrop classified information or inject malicious packets in a VANET. This can lead to compromising the true identity and travelling profile of a user. Different variants of masquerading attacks are discussed in the subsequent paragraphs.

1) Sybil Attack: During a Sybil attack, a fake node is forged which adopts identities of real users and utilizes this imposter behavior to flood fake and potentially hazardous traffic [17]. For example, a VANET node may be forced to change routes due to false warnings of road-congestions or accidents ahead, relayed through a Sybil attack.

2) Tunneling Attack: It is a type of wormhole attack where multiple distant nodes in a VANET gets connected, thereby creating a tunnel or an additional communication channel inside a network. Subsequently, the scattered nodes (in terms of mutual distance) communicate like neighbors, further colluding to generate malicious network traffic without getting detected.

3) GPS Spoofing: This is a very specific kind of location (with or without identity) masquerading attack where the GPS module installed in the OBU of a vehicle is targeted to broadcast wrong location information. Such an attack can create ghost nodes in a localized region, which may result into major network degradation, owing to increased data traffic (warnings / information message) for the compromised users [5]. Compromised vehicle may also confuse other vehicles and disrupt the whole traffic flow pattern as shown in Fig. 3.

D. Data Modification

Data modification attacks primarily compromise the data-integrity of a vehicle or support infrastructure in the VANET, leading to incorrect data of registered vehicles in the network. Different variants of this attack are discussed below.

1) Data Fabrication/Alteration: For ensuring smooth and real-time communication among resource-constrained VANET nodes, existing protocols and implementations may show leniency towards the use of robust encryption and authentication algorithms. Such loopholes can be exploited by an adversary to inject malicious data or modify parameters of healthy data generated by other nodes [18].

2) Replay Attack: This particular approach deals with recording certain broadcasted messages and then retransmitting the same with a delay. For protocols not equipped with anti-replay services such as time-stamps or random nonce values, replaying of old data can be accepted as a genuine message. This can be exploited by an adversary to bypass authentication mechanisms within VANETs by forcing its nodes to react to the outdated information.

IV. Location Privacy Protection Schemes

Location privacy (as per [19]) is defined as the extent to which the ID of any entity remains uncorrelated to its behavior, location and special characteristics. In VANETs, every vehicle is required to transmit a beacon message which contains vital information including its speed and location (acquired through GPS) [20]. This information is required to provide location-based services (LBS) by the administrator / TA and authorized third-party service providers. The beacon message is of the format *(ID,t,s)*. Here *ID* is the vehicles identity, *t* is the time stamp and *s* is the state vector of the vehicle, which contains the above-mentioned information. This information is then utilized by many VANET applications such as collision avoidance, emergency services in case of accident, and navigation systems etc. As this beacon message is continuously required by the network, it means each vehicle is continuously transmitting its identity which, in most cases, closely relates to the driver or the owner of the vehicle.

Compromise of location information can further facilitate the adversary to cause harm to the driver/ owner of the vehicle. For the safety of the driver, the identity of the vehicle needs to be masked or de-coupled with its location. For this purpose, many algorithms/ schemes have been suggested. This section further discusses some of the recent location privacy proposals and offers a detailed comparative analysis of their features.

Location privacy schemes can be broadly categorized into two types ; Identity Perturbation (Anonymization) and Location Perturbation (Obfuscation), as shown in Figure 4. Both Anonymization and Obfuscation approaches are similar from operational and security perspectives as the both can strengthen the location privacy at the cost of service quality. However, they entirely differ with regards to their implementation approaches. Anonymization primarily focuses on concealing user IDs through hiding the mapping between users and observed location. User mapping is switched periodically with the aim to discourage, and even foil, statistical analysis. This statistical analysis is empowered from continuous time series which may be matched with a user's prior history. On the other hand, in obfuscation based techniques, the location privacy is ensured through intentional sharing of inaccurate location information over the network.

In anonymization technique, pseudonym mappings are frequently changed to disrupt formation of a continuous time series which may be subjected to statistical analysis. Unfortunately, rapid exchange of pseudonyms directly compro-

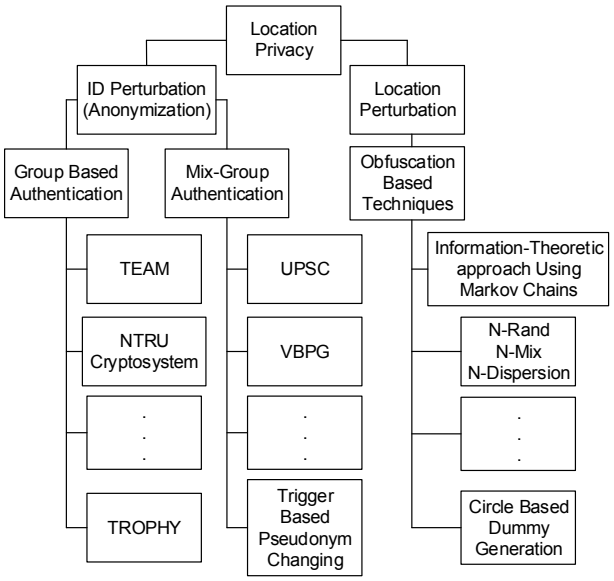

Fig. 4. VANET privacy preserving techniques

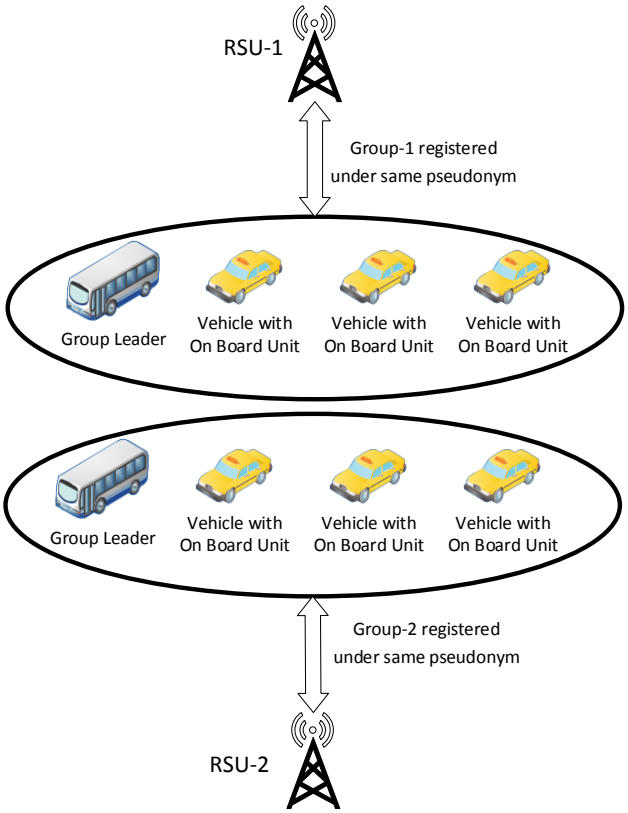

Fig. 5. Separate groups in the vicinity of near-by RSUs with different group leaders

mises usability and functionality. This can adversely affect certain services, for example personalized recommendations for refueling or dining, computed on the base of personality-specific historical data. In obfuscation-based system, the inherent feature of location inaccuracy hinders navigation or precise location based services such as ride-sharing, since the pinpoint location of a user is not available to the service provider. These tradeoffs require the choice of technique to be made carefully in view of applications of interest. This section further discusses a few of the prominent and more recent anonymity and obfuscation techniques used for privacy protection in VANETs.

A. Group Based Authentication

In group authentication schemes the vehicles are divided into small groups and each group is assigned a group leader as proposed by [21]. Chuang et al. [22] presented Trust-extended Authentication Mechanism (TEAM), a group based authentication scheme in which members need to be in the same vicinity . Each member authenticates to the leader, and then the leader authenticates itself to the TA through RSU, thus hiding the identity of the group members as depicted in Fig. 5. The group leaders may change at the intersections, so that after taking a turn, a new group is formed [23]. The group leaders can be authorized public transport vehicles i.e. buses, routine taxi services or even known patrol police vehicles [24]. If a certain vehicle stops or departs itself from its group, it can switch group in a similar fashion as a mobile phone switches between base stations. However, the leaders keep the vehicle's ID to themselves and the same is not revealed to the RSU or the TA. This scheme poses extra computational load at the leader vehicles since they are acting similar to gateways.

A recent research [25] presents a novel approach known as Trustworthy VANET ROuting with grouP autHentication keYs (TROPHY) using symmetric and asymmetric cryptography for authentication within group members and with the TA. In this approach, all standard group based authentication features are used with a slight difference of leader assignment. Here, the task of group leader is carried out by a Key Distribution Centre (KDC) which acts as a central entity to handle and verify all cryptographic transactions of its group members. The authors in [25] implemented this concept on Ubuntu Linux with Optimized Link State Routing (OLSR) protocol. Data packets were disseminated using UDP, while the group authentication was performed over TCP using MD5 hash function with 128 bit output. MI et al [26] presented a group based privacy preserving scheme based on postquantum secure oblivious transfer protocol which is devised based on efficient NTRU cryptosystem. Similar group-driven trust and authentication approaches have also been presented / discussed in several other research efforts [27]–[32], each offering the feature of location anonymity through diverse means, besides preserving requisite location based services.

Table I compares and critically analyzes the location privacy techniques discussed in this paper. It summarizes the pros and cons of each approach with reference to various operational

TABLE I
COMPARISON BETWEEN VANET LOCATION PRIVACY TECHNIQUES

Technique Feature	Group based	Mix-Group	Obfuscation
Ease of implementation at OBU / RSU	Yes	Yes	Yes
Performance in low traffic conditions	High	Low	Low
Computation at OBU (On-Board Unit)	Low	Medium	Medium
Computation at RSU (Road-Side Unit)	Medium	Medium	Low
Performance in urban (multi-velocity multi-direction) model	High	High	High
Performance in freeway (same velocity same direction) model	Low	Medium	High
Customized recommendation services	No	No	Yes
Accurate Location based services	Yes	Yes	No

and security parameters, such as the ease of implementation, performance under low, heavy and highway traffic scenarios, and quality of personality specific (customized) and location based services. Taking a critical look on group based authentication, this scheme is suitable for traffic patterns with similar velocities and movement. In other words, a group which very frequently reconfigures itself, due to vehicles adding and exiting a group, is likely to put computational load on the leader OBU. On the other hand, if the malicious member becomes part of a certain group, it can compromise location privacy of respective group members over a specific period of time.

Group based authentication scheme has a number of advantages as well as disadvantages in extending location based value services while preserving location privacy, as summarized in Table I. Foremost, this scheme is relatively easier to implement. Although the computational load with group leader is heavier than standard OBUs, this factor can be resolved through assignment of leadership to routine vehicles with better processing resources. The scheme, if considered in low and high traffic, should perform equally well. However, if a user stays in a specific group for longer durations (e.g. as in case of freeways or motorways) and members of a group remain the same, then the targeted vehicle can be tracked. Therefore, performance in freeway traffic is considered weak. Furthermore, since the TA cannot access the true ID of a vehicle, it can not send customized services to the vehicle.

B. Mix-Groups Authentication

Simple Mix-Group scheme involves creation of mix-zones at various spots in the city where the vehicles can enter and leave. The vehicles simultaneously change the pseudonyms while entering the mix-zone so that its ID is changed while leaving the same mix-zone. Thus, the tracker is unable to track the vehicle which enters the mix-zone under a certain pseudonym and leaves with a different pseudonym, as proposed by Yu et al [33], [34]. However, the problem arises when the traffic density is low. In this case, building many mix-zones within a city at various spots may solve the privacy protection problem.

Another similar strategy was presented by Boualouache and Moussaoui [35], referred as Urban Pseudonym Changing Strategy (UPCS). In this technique, silent mix-zones (SM) are created at various signaling intersection points in the city. This approach requires the traffic density to be high. A limitation of this scheme is that, in between the mix-zones, the target remains traceable and thus, exposes itself to the location privacy attacks.

Another variant of the standard Mix-Group technique is the Velocity Based Pseudonym Changing (VBPG) strategy [36]. This scheme suggests changing of pseudonyms on the basis of velocity groups. Here, the groups are created based on the individual velocities of respective cars. Cars in the vicinity of same RSU and having roughly the same velocity are grouped together and thus are authenticated with TA using the same pseudonym. This makes it difficult for the attacker to identify and track an individual vehicle within a specific group.

The UPCS and VBPG techniques are similar in a way that both follow the fundamental features of mix-group. UPCS can be considered a subset of VBPG as it follows essentially the same basic approach as of VPBG i.e changing user IDs as they enter or leave the mix group. However, VBPG also incorporates the variable of user velocity in addition to its location, to ensure pseudonym exchange among nodes with similar movement patterns and thus, enhances resistance against malicious pseudonym tracking.

In a recent work presented by Zidani et al. [37], the authors implemented privacy protection by changing the pseudonym based on the number and predicted positions of nearby vehicles. Similarly, the work presented by Wang et al. [38] followed a trigger-based pseudonym exchange technique aiming to thwart vehicle tracking through beacon messages, besides reducing pseudonym storage overhead for VANET nodes. A number of other similar efforts [39]–[52] also adopted mix-group based anonymity approaches, implemented via pseudonym-driven dynamic ID allocation for authenticating legitimate VANET nodes while concealing their location information.

Uncertainty (or in other words, Entropy) is the strength of preservation of location privacy pseudonym schemes. Mix-Group schemes focus on combining closely located hot-spots of the transports to an extended pseudonym-evolving region. Uncertainty is enhanced by expanding the area of the region for vehicle accumulation, thus enhancing privacy preservation. Mix-Group offers a good resistance to brute force cryptanalytic attacks due to encryption and authentication mechanisms. Time-stamps prevents replay attacks and also protects against adversary portraying as a valid RSU or forging RSU messages.

In case of low regional traffic (for swapping pseudonyms), an attacker can eavesdrop on the safety messages by OBUs and can subsequently record their time and frequency to map probability distributions and successfully track a target

vehicle. However, Mix-Group operates on multi-pseudonyms, thus allowing a vehicle to exchange pseudonym with passing by vehicle or with a new zone. If this exchange happens over a significantly large group, it becomes very difficult for any attacker to continue tracking a specific vehicle. For unauthenticated traffic in mix-groups, forged data delivery is possible within a group. However, the same can be prevented if each vehicle signs its message, thus identifying and rejecting spoofed malicious messages. Moreover, pseudonym counterfeiting or fabrication can also be avoided by implementing digital certificates at the OBU level. Similar approach has also been discussed by [53].

Focusing on broader advantages, as covered in Table I, Mix-Group schemes are easy to implement. However, frequent changing of pseudonym requires good computational resources at OBU and RSU level. In low traffic environments, the tracking probability is increased since the number of members participating in exchanging the pseudonym are less. In an urban model, the scheme is likely to perform well. However, in freeway / motorway environment, VBPC technique is not much effective since vehicles do not cross each other frequently. Moreover, in VBPC approach, creation of mix-zones can be exploited to track a vehicle with known velocity by computing its entry and exit times. As far as customized services are concerned, since true ID of the vehicle is never revealed, identity-driven customized user services are not possible. However, accurate location based services can be easily extended to the users.

C. Obfuscation Based Approaches

In obfuscation technique, tracking can be made difficult by lowering the accuracy of location data and by increasing the time interval of messages transmitted by beacon installed on the OBU. This approach is effective in those scenarios, where LBS does not require accurate location information for provisioning of acceptable level of quality of service (QOS).

Takbiri et al. [54] presented an information-theoretic approach using Markov chains, which induces certain pre-calculated location error. The amount of error is computed by ensuring availability of LBS, while reducing the location accuracy and then assigning a new pseudonym. The selection of pseudonym is also randomized by permuting all the possible pseudonyms first. The stated approach assumed that users have very limited knowledge about the numbers and characteristics of other available users, constituting overall traffic population. A simple distribution is applied in which each user's location is reported with intentional error associated with certain probability. This probability is randomly generated for each user. If $Z_u^{(n)}$ is the vector representing the noisy (obfuscated) version of the location of a user u and $Z^{(n)}$ is the combination of $Z_u^{(n)}$ for all users then the relationship between these vectors is represented below by equation 1.

$$Z_u^{(n)} = \begin{bmatrix} Z_u^{(n)}(1) \\ Z_u^{(n)}(2) \\ \cdot \\ \cdot \\ \cdot \\ Z_u^{(n)}(m) \end{bmatrix}, Z^{(n)} = [Z_1^{(n)}, Z_2^{(n)}, ..., Z_n^{(n)}] \quad (1)$$

As already described, a random variable $R_u^{(n)}$ is to be generated, which is uniformly distributed between values of 0 and 1. $R_u^{(n)}$ is the probability that location of a specific user is changed by obfuscation. This change is called system's "noise level". The location and velocity of each user can be expressed as a Probability Distribution Function (PDF) [55]. The function of obfuscation aims to change PDF of every user. The change in the PDF of user's location remains unknown to an attacker. This obfuscation function is designed to remain independent of user historical data and thus does, not hold any correlation with it. User locations are considered as independent and identically distributed variables and are modeled through Markov chains in order to capture user dependency across time [54]. There are r possible locations, which corresponds to the number of states of the Markov chain.

Whitman et al. [56] presented three novel obfuscation techniques, namely the N-Rand, N-Mix and N-Dispersion algorithms. The performance of these algorithms was measured and compared in terms of average distance, maximum and minimum distance between the original locations as well as the obfuscated paths. Another recent work presented by Arif et al. [57] implemented location privacy with the help of the Circle Based Dummy Generation (CBDG) algorithm while leveraging a trusted third party. The proposed approach benefits from both the obfuscation and anonymity methods through the exchange of location information among nearby vehicles in a two step authentication process. A number of other similar efforts [58]–[68] employed a diverse range of obfuscation mechanisms to conceal precise location data while still being able to offer the appropriate quality of services.

Reviewing the pros and cons of obfuscation schemes, as summarized in Table I, its implementation is considered easy since an algorithm (once designed) can be repeatedly implemented at OBUs. In low traffic conditions, even with relative noise, an attacker can still track the target vehicle within range set by the system noise level. However, in urban dense environments, and freeway / motorway setup, the confusion factor increases thereby hiding the location of a specific user. This scheme offers extension of customized services to users since TA can uniquely identify the user. However, the offered services can not cover the location based services since the location inaccuracies prevent revealing of precise user location.

Based on the detailed analysis of the three techniques presented in this section, the following conclusions can be drawn regarding the pros and cons of these techniques:

- Selection of the most optimal location privacy technique largely depends on the quality and type of services as well as the available computational resources of the VANET nodes.
- In case customized, user-specific and history-driven recommendation services are aimed by the supported LBS, obfuscation is the right choice.
- If precise LBS services are desired then selection of either group-based or mixed-group techniques are likely to yield the desired results.
- For low traffic conditions or with VANET nodes exhibiting similar velocities and traffic patterns, as observed on highways, group-based authentication is a preferred choice as compared to the mix-group technique.
- Mix-group authentication scheme carries more computational overheads as compared to the group-based schemes due to the frequent changing of pseudonyms.

V. Related Work

The quest for location privacy in VANETs is as old as the introduction of VANETs themselves. Many researchers have explored this domain with an aim to develop effective and efficient location privacy schemes using a multitude of approaches. Additionally, a number of survey papers have also been published to analyze and categorize the advancements made in this area. This section briefly discusses some of the existing survey papers covering the related domains.

In a recent review presented by Arshad et al. [69], the authors discussed privacy attacks and reviewed the algorithms devised to catch malicious vehicles instead of preserving their location information, which is the focus of our work. Chen et al. [39] discussed privacy techniques for location based services and threats, in particular for IoT environment and more specifically for GNSS-based systems. Other efforts [70], [71] reviewed and analyzed location-privacy protection, while focusing on mobile applications. Contrarily, our work primarily focuses on privacy-mechanism for Vehicular Adhoc Networks.

Bariah et al. [29] presented a survey to cover the overall security issues in VANETs. Their work also discussed the privacy schemes involving anonymity, allotment of pseudo-random IDs and situation model-based user code distribution. Since the survey is generalized to cover all VANET related privacy issues, the area of location privacy remains to be analyzed in depth. Similarly, the survey presented by Qu et al. [31] primarily reviewed the authentication and privacy methods inside VANETs, besides analyzing different approaches to detect and revoke malicious nodes.

Ferrag et al. [58] bifurcated location based attacks into two categories and labeled them as *forgery attacks* (misleading bogus messages generated deliberately to track certain targets) and *global external attacks* (eavesdropping and tracking a user by gaining access to its velocity and direction). The researchers also categorized recent techniques into the domains of mixed group authentication and obfuscation. Liu et al. [72] reviewed various privacy protection approaches while categorizing them into four groups, namely: cryptographic mechanisms, anonymization mechanisms, obfuscation mechanisms and reducing location information sharing.

The above discussed surveys are few of the most relevant reviews conducted in recent times and provide valuable contribution by enlightening readers about various trends in ensuring location privacy. However, most of this literature seems to divert from core location privacy issues towards either focusing on attack models or discussing generalized VANET security challenges / solutions. Furthermore, a comprehensive and high-level comparative analysis seems to be missing, which can empower researchers and VANET developers to select suitable privacy techniques, based on their location-based service / application. The main motivation behind this work is to provide an operational level critical analysis of available location privacy techniques based on their implementation features and security vs service tradeoffs. Our work therefore, aims to assist system designers in selecting the optimum technique for their design while catering for its inherent tradeoffs.

VI. Conclusion

Data privacy threats, being passive in nature, are surreptitious, asymmetric and global. Modern-day cyber-physical systems, including VANETs, offer very lucrative targets to steal private and personally-identifiable information, thus further expanding these threat vectors and attack techniques. All multi-staged and sophisticated attacks rely on information-gathering through breach of data privacy. Consequently, location-privacy breach of a mobile VANET node can lead to safety-critical physical attacks, such as stalking and mugging. This survey paper presented an overview of different security techniques for preserving location privacy in VANETs. We initially reviewed the basics of VANET's architecture and threat categories. Followed by that, we critically analyzed some of the recent protection techniques to preserve location privacy, while discussing their operational and security tradeoffs under a range of network constraints. Maintaining location privacy of drivers and passengers is an active research area and there is a dire need to further improve the privacy mechanisms to make them robust yet efficient under varying conditions. The pace of embracing modern road safety and convenience technologies, including driverless and (Collaborative) Internet of Vehicles, will largely depends upon field-worthy and fool-proof techniques to effectively safeguard the private information of the users.

References

[1] W. H. Organization, *Global status report on road safety 2015*. World Health Organization, 2015.

[2] M. Alam, J. Ferreira, and J. Fonseca, "Introduction to intelligent transportation systems," in *Intelligent Transportation Systems*. Springer, 2016, pp. 1–17.

[3] H. Bhatia, "125 Million+ Connected Cars Shipments by 2022; 5G Cars by 2020," https://www.counterpointresearch.com/125-million-connected-cars-shipments-2022-5g-cars-2020/, 2018, accessed: 2018-09-14.

[4] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE communications surveys & tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[5] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[6] A. Dua, N. Kumar, and S. Bawa, "A systematic review on routing protocols for vehicular ad hoc networks," *Vehicular Communications*, vol. 1, no. 1, pp. 33–52, 2014.

[7] Z. Lu, G. Qu, and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," *IEEE Transactions on Intelligent Transportation Systems*, 2018.

[8] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET 1," 2013.

[9] Z. He, "Structure based or structure free? Topology management in VANETs," in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on*. IEEE, 2012, pp. 1–4.

[10] K. Verma, H. Hasbullah, and A. Kumar, "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," in *Advance Computing Conference (IACC), 2013 IEEE 3rd International*. IEEE, 2013, pp. 550–555.

[11] R. Minhas and M. Tilal, "Effects of jamming on IEEE 802.11 p systems," 2010.

[12] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[13] D. Goyal, "Design and Analysis of Secure VANET Framework preventing Black Hole and Gray Hole Attack," 2016.

[14] F. Sabahi, "The security of vehicular adhoc networks," in *2011 Third International Conference on Computational Intelligence, Communication Systems and Networks*. IEEE, 2011, pp. 338–342.

[15] M. S. Al-Kahtani, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)," in *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*. IEEE, 2012, pp. 1–9.

[16] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2012.

[17] J. Grover, V. Laxmi, and M. S. Gaur, "Sybil attack detection in VANET using neighbouring vehicles," *International Journal of Security and Networks*, vol. 9, no. 4, pp. 222–233, 2014.

[18] A. Rawat, S. Sharma, and R. Sushil, "VANET: Security attacks and its possible solutions," *Journal of Information and Operations Management*, vol. 3, no. 1, p. 301, 2012.

[19] G. P. Corser, H. Fu, and A. Banihani, "Evaluating location privacy in vehicular communications and applications," *IEEE transactions on intelligent transportation systems*, vol. 17, no. 9, pp. 2658–2667, 2016.

[20] T. Peng, Q. Liu, D. Meng, and G. Wang, "Collaborative trajectory privacy preserving scheme in location-based services," *Information Sciences*, vol. 387, pp. 165–179, 2017.

[21] Y. Lu, B. Zhou, F. Jia, and M. Gerla, "Group-based secure source authentication protocol for VANETs," in *GLOBECOM Workshops (GC Wkshps), 2010 IEEE*. IEEE, 2010, pp. 202–206.

[22] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE systems journal*, vol. 8, no. 3, pp. 749–758, 2014.

[23] F. M. Salem, M. H. Ibrahim, and I. Ibrahim, "Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks," in *Networking and Services (ICNS), 2010 Sixth International Conference on*. IEEE, 2010, pp. 156–161.

[24] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications." in *VNC*, 2013, pp. 1–8.

[25] P. Cirne, A. Zúquete, and S. Sargento, "TROPHY: Trustworthy VANET routing with group authentication keys," *Ad Hoc Networks*, vol. 71, pp. 45–67, 2018.

[26] B. Mi, D. Huang, and S. Wan, "NTRU Implementation of Efficient Privacy-Preserving Location-Based Querying in VANET," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[27] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Profile matching protocol with anonymity enhancing techniques," in *Security and Privacy in Mobile Social Networks*. Springer, 2013, pp. 19–41.

[28] B. Ying, D. Makrakis, and H. T. Mouftah, "Privacy preserving broadcast message authentication protocol for VANETs," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1352–1364, 2013.

[29] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, "Recent advances in VANET security: a survey," in *Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd*. IEEE, 2015, pp. 1–7.

[30] T. Zhang and L. Delgrossi, *Vehicle safety communications: protocols, security, and privacy*. John Wiley & Sons, 2012, vol. 103.

[31] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[32] C. Dunbar and G. Qu, "A DTN routing protocol for vehicle location information protection," in *Military Communications Conference (MILCOM), 2014 IEEE*. IEEE, 2014, pp. 94–100.

[33] 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 Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 93–105, 2016.

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

[35] A. Boualouache and S. Moussaoui, "Urban pseudonym changing strategy for location privacy in VANETs," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 24, no. 1-2, pp. 49–64, 2017.

[36] I. Ullah, A. Wahid, M. A. Shah, and A. Waheed, "VBPC: Velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET," in *Communication Technologies (ComTech), 2017 International Conference on*. IEEE, 2017, pp. 132–137.

[37] F. Zidani, F. Semchedine, and M. Ayaida, "Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach for location privacy in VANETs," *Computers & Electrical Engineering*, vol. 71, pp. 359–371, 2018.

[38] S. Wang, N. Yao, N. Gong, and Z. Gao, "A trigger-based pseudonym exchange scheme for location privacy preserving in VANETs," *Peer-to-Peer Networking and Applications*, vol. 11, no. 3, pp. 548–560, 2018.

[39] L. Chen, S. Thombre, K. Jarvinen, E. S. Lohan, A. Alen-Savikko, H. Leppakoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala *et al.*, "Robustness, security and privacy in location-based services for future iot: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[40] N. Samama, "Indoor positioning with gnss-like local signal transmitters," in *Global Navigation Satellite Systems: Signal, Theory and Applications*. InTech, 2012.

[41] A. Puengnim, L. Patino-Studencka, J. Thielecke, and G. Rohmer, "Precise positioning for virtually synchronized pseudolite system," in *Indoor Positioning and Indoor Navigation (IPIN), 2013 International Conference on*. IEEE, 2013, pp. 1–8.

[42] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[43] H. Al Falasi and E. Barka, "Revocation in VANETs: A survey," in *Innovations in Information Technology (IIT), 2011 International Conference on*. IEEE, 2011, pp. 214–219.

[44] S. Biswas, J. Mišic, and V. Mišic, "ID-based safety message authentication for security and trust in vehicular networks," in *2011 31st international conference on distributed computing systems workshops*. IEEE, 2011, pp. 323–331.

[45] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008, pp. 1229–1237.

[46] I. Khacheba, M. B. Yagoubi, N. Lagraa, and A. Lakas, "CLPS: context-based location privacy scheme for VANETs," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 29, no. 1-2, pp. 141–159, 2018.

[47] J. Wang, Y. Shao, J. Zhu, and Y. Ge, "Spatio-temporal location privacy quantification for vehicular networks," *IEEE Access*, 2018.

[48] I. Memon and H. T. Mirza, "MADPTM: Mix zones and dynamic pseudonym trust management system for location privacy," *International Journal of Communication Systems*, p. e3795, 2018.

[49] M. T. Garip, P. Reiher, and M. Gerla, "BOTVEILLANCE: A Vehicular Botnet Surveillance Attack against Pseudonymous Systems in VANETs," in *2018 11th IFIP Wireless and Mobile Networking Conference (WMNC)*. IEEE, 2018, pp. 1–8.

[50] S. Wang and N. Yao, "A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs," *Wireless Networks*, pp. 1–17, 2018.

[51] 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," *International Journal of Communication Systems*, vol. 31, no. 1, p. e3437, 2018.

[52] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Vlpz: The vehicular location privacy zone," *Procedia Computer Science*, vol. 83, pp. 369–376, 2016.

[53] H. Farman, B. Jan, M. Talha, A. Zar, H. Javed, M. Khan, A. U. Din, and K. Han, "Multicriteria-Based Location Privacy Preservation in Vehicular Ad Hoc Networks," *Complexity*, vol. 2018, 2018.

[54] N. Takbiri, A. Houmansadr, D. L. Goeckel, and H. Pishro-Nik, "Limits of location privacy under anonymization and obfuscation," in *Information Theory (ISIT), 2017 IEEE International Symposium on*. IEEE, 2017, pp. 764–768.

[55] S. Shelly and A. V. Babu, "A probabilistic model for communication link reliability in vehicular ad hoc networks," in *Vehicular Electronics and Safety (ICVES), 2014 IEEE International Conference on*. IEEE, 2014, pp. 123–128.

[56] P. Wightman, W. Coronell, D. Jabba, M. Jimeno, and M. Labrador, "Evaluation of location obfuscation techniques for privacy in location based information systems," in *Communications (LATINCOM), 2011 IEEE Latin-American Conference on*. IEEE, 2011, pp. 1–6.

[57] M. Arif, G. Wang, and T. Peng, "Track me if you can? Query Based Dual Location Privacy in VANETs for V2V and V2I," in *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)*. IEEE, 2018, pp. 1091–1096.

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

[59] H. Kuusniemi, M. Z. H. Bhuiyan, M. Ström, S. Söderholm, T. Jokitalo, L. Chen, and R. Chen, "Utilizing pulsed pseudolites and high-sensitivity GNSS for ubiquitous outdoor/indoor satellite navigation," in *Indoor Positioning and Indoor Navigation (IPIN), 2012 International Conference on*. IEEE, 2012, pp. 1–7.

[60] G. Falco, G. A. Einicke, J. T. Malos, and F. Dovis, "Performance analysis of constrained loosely coupled GPS/INS integration solutions," *Sensors*, vol. 12, no. 11, pp. 15 983–16 007, 2012.

[61] S. E. Langel, M. Samer, F.-C. Chan, and B. S. Pervan, "Tightly coupled GPS/INS integration for differential carrier phase navigation systems using decentralized estimation," in *Position Location and Navigation Symposium (PLANS), 2010 IEEE/ION*. IEEE, 2010, pp. 397–409.

[62] L. Chen, Y. Li, and C. Rizos, "Stability analysis of tracking weak GPS signals through non-coherent ultra-tight GPS/INS integration," in *Proc. International Conference on Indoor Positioning and Indoor Navigation, Sydney, Australia*. Citeseer, 2012.

[63] D. Serant, D. Kubrak, M. Monnerat, G. Artaud, and L. Ries, "Field test performance assessment of GNSS/INS ultra-tight coupling scheme targeted to mass-market applications," in *Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing,(NAVITEC), 2012 6th ESA Workshop on*. IEEE, 2012, pp. 1–8.

[64] M. Langer and G. F. Trommer, "Multi GNSS constellation deeply coupled GNSS/INS integration for automotive application using a software defined GNSS receiver," in *Position, Location and Navigation Symposium-PLANS 2014, 2014 IEEE/ION*. IEEE, 2014, pp. 1105–1112.

[65] S. Kennedy and J. Rossi, "Performance of a deeply coupled commercial grade GPS/INS system from KVH and NovAtel Inc." in *Position, Location and Navigation Symposium, 2008 IEEE/ION*. IEEE, 2008, pp. 17–24.

[66] P. D. Groves, "Shadow matching: A new GNSS positioning technique for urban canyons," *The journal of Navigation*, vol. 64, no. 3, pp. 417–430, 2011.

[67] G. Corser, H. Fu, T. Shu, P. D'Errico, W. Ma, S. Leng, and Y. Zhu, "Privacy-by-decoy: Protecting location privacy against collusion and deanonymization in vehicular location based services," in *Intelligent Vehicles Symposium Proceedings, 2014 IEEE*. IEEE, 2014, pp. 1030–1036.

[68] 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 of Things Journal*, 2018.

[69] M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, H. Criuckshank, and Y. Cao, "A survey of local/cooperative-based malicious information detection techniques in VANETs," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 62, 2018.

[70] K. Fawaz and K. G. Shin, "Location privacy protection for smartphone users," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 239–250.

[71] M. L. Damiani, "Location privacy models in mobile applications: conceptual view and research directions," *GeoInformatica*, vol. 18, no. 4, pp. 819–842, 2014.

[72] B. Liu, W. Zhou, T. Zhu, Y. Xiang, and K. Wang, "Location Privacy-Preserving Mechanisms," in *Location Privacy in Mobile Applications*. Springer, 2018, pp. 17–31.