Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges and Countermeasures

Philip Asuquo, Haitham Cruickshank, *Member, IEEE,* Jeremy Morley, Chibueze P. Anyigor Ogah, Ao Lei, Waleed Hathal, Shihan Bao, and Zhili Sun, *Senior Member, IEEE*

***Abstract*—Location-based Services (LBS) have gained popularity as a result of the advances in mobile and communication technologies. LBS provide users with relevant information based on their location. In spite of the desirable features provided by LBS, the geographic locations of users are not adequately protected. Location privacy is one of the major challenges in vehicular and mobile networks. In this article, we analyse the security and privacy requirements for LBS in vehicular and mobile networks. Specifically, this paper covers privacy enhancing technologies and cryptographic approaches that provide location privacy in vehicular and mobile networks. The different approaches proposed in literature are compared and open research areas are identified.**

***Index Terms*—Privacy, Authentication, Location-based services, Vehicular ad hoc networks, Mobile technologies.**

I. Introduction

Many years of advances in mobile and wireless network technologies have ushered in a variety of application domains of vehicular ad hoc networks (VANETs) resulting in disruptive changes to the way we live, work, and play. Examples of the applications of VANET technology abound including Intelligent Transport Systems (ITSs), Connected Autonomous Cars (CACs), and Internet of Things (IoT) such as Internet of Vehicles (IoVs) [1], [2], [3]. These application domains such as ITSs, IoVs, and CACs have attracted a great deal of attention in recent years both in the academia and industries [1], [2], [4]. The key feature of these application domains is that vehicles fitted with multiple sensors can collect various forms of data including the location information of drivers which can be analysed and exchanged with vehicles for various purposes including road safety, traffic management and user convenience [3], [5]. In the near future, it is expected that millions of vehicles will be connected through a complex vehicular network infrastructure to form IoVs using various technologies, both in industrial and domestic contexts [6], [7], [1], [8]. VANETs for ITS are characterised by dynamic mobility patterns, infrequent connectivity, and frequent topology changes in addition to the somewhat hostile environments in which wireless networks are deployed.

According to [9], IoT is not only being widely leveraged for smart parking solutions and traffic management but also for the entertainment of passengers, telematics solutions and fleet management. It is envisioned that IoT will help in the advancement of transportation management systems including electronic toll collections. The rapid acceptance and adoption of 'smart city' revolution by more cities in recent years have paved way for the continuous innovation towards improved standard of living in which ITS plays a vital role. IoT plays a key role in the integration, control and processing of information across transportation systems thereby creating real-time interactions [8] [10].

In addition to security threats specific to wireless networks, due to the location information embedded in exchanged messages, some location privacy threats to users/drivers exist too [2]. For instance, a malicious vehicle can track a driver for social profiling based on the location information contained in the exchanged safety messages. Malicious vehicles can also lie about their location information to deceive rescue workers in emergencies in order to evade prosecution in hit-and-run accidents [11], [10]. In emergency and rescue situations, accurate location information is needed to correctly direct rescue workers and the police for efficient emergency evacuation. A major threat to location privacy is the possibility of a location privacy attacker (PA) revealing the real identity of vehicles and their users using tracking algorithms which may expose users to social profiling. Malicious vehicles can also use location information to stalk other road users and reveal their personal identity (breach of identity privacy). Of course, the close-knit relationship between vehicle drivers and their vehicles implies that tracking vehicles is as good as tracking/following its driver's whereabouts.

A. Security and Privacy in Location-Based Services

In the context of location-based services in IoT, security and privacy threats related to location-based services have not been adequately addressed. IoT is not only an emerging technology, it is expected that several applications areas including manufacturing, healthcare and transportation will benefit from IoT systems [12]. In vehicular networks, IoT can be combined with cloud computing as an infrastructure service for vehicular cloud data. This is useful for disseminating information related to transportation such as monitoring road conditions tracking the location of the vehicle in real time and traffic control management. In recent years, the authors in [13], [14], [15], [16], [17] have proposed solutions aimed at improving the Intelligent Transport System (ITS) using IoT technologies. For example, the Intelligent Internet of Vehicles Systems (IIOVMS) proposed in [14] for the collection of traffic related information from external environments. In [15], a cloud architecture that combines IoT technology with a middleware is developed to enable innovation in automobile technologies. In [16], the authors develop an intelligent monitoring system to track the location of refrigerator trucks using IoT technologies. In [17], the authors develop a cloud enabling platform which is combined with IoT as an enabling infrastructure to support transport-related information including vehicle location tracking and monitoring.

B. Relation to Existing Surveys

Several authors have surveyed the various approaches to security and privacy in IoT systems [18] [19],[20]. In [18], the authors provide an in-depth evaluation of threats and their countermeasures for Global Navigation Satellite System and Non-GNSS systems. They survey a wide range of security and privacy solutions based on localisation and positioning in the IoT systems. They also give an insight on the legal and technical requirements for localisation and positioning in IoT systems. In [20], the authors present a comprehensive overview of enabling technologies in IoT, architectures as well as security and privacy related issues. In addition, fog/edge computing based on IoT is introduced and the authors clearly distinguish between IoT and cyber-physical systems. The roadmap from vehicular networks to smart transportation looks promising. While vehicular network architecture supports specific applications such as safety and traffic efficiency, internet connectivity may not be fully available. With the support of IoT systems, it is envisaged that convergent evolution of IP and mobile networks will provide a common infrastructure for a broad set of applications. In vehicular networks, the authors in [21] provide a detailed survey of authentication schemes and outline some privacy-preserving schemes. They examine and categorise proposed solutions based on their suitability for various conditions. The authors in [22] pay attention to pseudonym schemes proposed for vehicular networks. Their survey covers pseudonym schemes based on cryptographic approaches such as public key and identity-based cryptography as well as symmetric authentication schemes. In contrast, this paper surveys research that is relevant to location privacy in mobile and vehicular networks. We specifically provide a detailed analysis of existing privacy enhancing schemes, cryptographic approaches and privacy-preserving authentication schemes proposed for location privacy in vehicular and mobile networks. Furthermore, we address the open issues and challenges in security and location privacy in vehicular networks.

The rest of the paper is organised as follows. In section II, we describe the security and privacy requirements for vehicular and mobile networks. In section III, we present the adversary models, location privacy metrics and attacks discussed in literature. In section IV, we discuss the existing location privacy/security schemes in mobile vehicular networks. We distinguish four major categories of location privacy enhancing schemes and also discuss privacy-preserving authentication schemes. In section V, we discuss privacy enhancing schemes in mobile networks and cryptographic approaches that address location privacy of users. In section VI, we further identify the challenges and open issues. Finally, we conclude our review in section VII.

II. Definitions, Security and Privacy Requirements for Location-Based Services

In vehicular and mobile, the security and privacy requirements have strong dependencies with other requirements such as basic system requirements which constrain and influence privacy. We identify the following properties necessary for security and privacy in vehicular and mobile networks.

A. Definitions

a) On-board Unit (OBU): The OBU otherwise known as the On-board Equipment (OBE) is installed on a vehicle and composed of various sensors and electronic components through which various forms of data can be collected, processed and exchanged for safety purposes.

b) Road-side Unit(RSU): The Road-side Units (RSU) takes the form of an access point which is used together with a vehicle and extends the telecommunication infrastructure as well as facilitate the routing of messages in an efficient manner. The number of RSUs, manner of their deployment and placement is key to ensure that maximum number of vehicles have enough coverage. They can be located at intersections and point-of-interest (PoI) locations where they form connectivity with vehicles within their communication range.

c) Trusted Third-Party(TTP): A Trusted Third-Party (TTP) is defined by the joint technical committee of the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC) (ISO/IEC) as an entity trusted by users/vehicles for security functions. The security functions may include support for the issuance, use of and verification of digital certificates and signatures, and confidentiality services.

d) Certificate Authority (CA): Vehicle to vehicle or vehicle to infrastructure communication between vehicles and the infrastructure are not only required to be secure but also trustworthy. During communication, some vehicles may become selfish or malicious. Such malicious deviate from normal protocol and disrupt network activity such as transmitting fake location data. To mitigate such situations, a higher level TTP called a Certificate Authority (CA) is used to bootstrap the vehicle registration. The TTP also issues vehicles with pseudonym certificates which facilitates accountability and revocation.

e) Registration Authority (RA): Depending on the deployment specifics, a separate third-party which is known as the Registration Authority (RA) may be needed to provide authentication and authorization services to both vehicles and LBS providers.

f) V2V: Vehicle to vehicle communication is one form in which vehicles exchange messages with each other. Vehicle to vehicle communication is particularly useful since it allows short and medium range communication with no need for infrastructure (e.g. RSU support).

g) V2R: Different from V2V communication, the vehicle to infrastructure (V2R) communication paradigm is a mode of VANET message exchange which facilitates communication between vehicles and the infrastructure.

B. Security Requirements

1) Authentication: The authentication process in vehicular and mobile networks should be privacy-preserving. A user must be authenticated when it requests joining the LBS i.e. when it sends a request to the Service Provider (SP) through a nearby RSU or Base station. A privacy-preserving key management scheme is desirable for LBS in vehicular and mobile networks. Messages exchanged between entities should be authenticated and integrity-protected.

2) Confidentiality: Confidentiality is necessary to protect LBS contents from passive eavesdroppers. Confidentiality guarantees the delivery of messages to designated recipients or authorised parties. Data confidentiality can be applied by using encryption techniques based on secure key management system.

3) Traceability and Revocation: A user that abuses the network should be traceable by an authority. The revocation of the misbehaving user by the authority should be timely. This reduces the impact of the misbehaving user on the network.

4) Efficiency: The cryptographic protocols used in vehicular and mobile networks should be computationally efficient. The key management scheme must incur limited computational overhead. To ensure effective operation, lightweight key management scheme should be used.

C. Privacy Requirements

1) Short-term linkability: Short-term linkability is a desirable property in ITS applications [23]. Assuming a vehicle sends two or more messages within a small time frame δt, the receiving vehicle should be able to verify that these messages came from the same source. Enforcing short-term linkability ensures that a compromised OBU cannot impersonate multiple vehicles and launch a Sybil attack [24]. In vehicular networks, vehicles frequently broadcast messages with their speed, current location and acceleration. These messages are used to build up a trajectory of nearby OBUs. The location privacy of users is not affected by short-term linkability because the small time increment δt does not impact the location privacy of the vehicle [25].

2) Long-term unlinkability: A basic location privacy requirement for vehicular networks is long-term unlinkability. An adversary must not be able to link messages sent by a vehicle to the attributes of that vehicle such as location, type of car and applications. Tracking protection must be implemented to protect the users from linkability of two or more successive positions. In mobile networks, the service provider should be unable to link two or more successive positions of the user.

3) Anonymity: Anonymity focuses on the protection of the user's identity. It is a term used to mean the ability of the user to access a resource or service without disclosing its user identity. This means that the subject may perform an action without disclosing its user identity to third-parties. Anonymity techniques provide means to know the set of users that cannot see the identity of someone performing certain actions. Hence, when the action of a user is anonymous, another subject will not be able to determine either the identity or even a reference to the identity of the user.

4) Pseudonymity: Pseudonymity is a technique used to ensure that a user may use access a resource or service without disclosing its identity, but can still be accountable for that use. Since the user is accountable for the use, it can be regarded as conditional pseudonymity or reversible pseudonymity. Accountability is achieved if the user's real identity is directly linked to a reference (an alias or pseudonym) held by an entity such as the certificate authority, or by providing an alias that will be used for processing purposes, such as an account number. Conditional pseudonymity is required where the identity information of violators need to be revealed by law enforcement authorities for liability purposes. Similarities exist between pseudonymity and anonymity. While both protects the identity of the user, pseudonymity uses a reference to the user's identity for accountability.

5) Accountability(Non-repudiation): Anonymity is conditional on good reputation. While anonymity protects the location privacy of users, a misbehaving or faulty vehicle that caused an accident needs to be identified for possible prosecution. Note that pseudonyms are linked to information that allows the certificate authority to establish a forensic evidence against a misbehaving user for the purpose of accountability.

6) Location Privacy: The exact location information of the user must be protected from unauthorised entities. The user's trajectory which contains location data of the user's present and past locations including points of interest must not be revealed to unauthorized entities.

III. Adversary Models, Location Privacy Metrics and Location Privacy Attacks

A. Adversary Models

Location privacy approaches proposed in literature share common characteristics. Several privacy metrics consider some sort of adversaries. The authors in [26] point out that the more knowledgeable the adversary is, the lower the location privacy. We classify the adversaries described in literature as follows:

1) Global/Local: The range of an adversary is used to determine if it is a global or local adversary. Global adversaries have access to the whole network. Local adversaries are limited to a part of the network. For example, eavesdroppers can have access to a limited number of RSUs deployed at road intersections [27].

2) Active/Passive: An active adversary can meddle with the network by injecting or modifying messages. Passive adversaries cannot modify messages, they only read and observe information transmitted by participating nodes in the network [22].

3) Static/Adaptive: Static adversaries choose an attacking technique or strategy before launching an attack regardless of how the attack progresses. Adaptive adversaries observe the network by learning the system configuration and parameters.

In location privacy, most threat models use adaptive adversaries which are described in the context of location privacy as inference attacks [28], [29], [30], [31].

4) Internal/External: An internal adversary is considered to be a part of the network while the external adversary is always as a global passive attacker. In the context of LBS, untrusted LBS servers and TTP (anonymizers) are examples of internal adversaries. Many authors assume that LBS servers are untrusted [32], [33], [34], [35], [36].

B. Location Privacy Metrics

Several privacy metrics have been proposed in literature [26]. However, this survey focuses on the privacy metrics used in the evaluation of the various approaches to location privacy discussed in this report.

1) Anonymity Set Size: Anonymity set size was introduced by the authors in [37]. They define anonymity set as the set of users with the probability of sending a particular message which is seen by a global observer. This global observer is assumed to have compromised a set of nodes. the authors point out that the anonymity set size is a good indicator of the level of anonymity provided. This concept was used in modelling the security of Dining Cryptographers (DC) Networks. According to [26], the anonymity set size counts the number of users that could be a targeted individual p. It is described as the size of the area where the targeted user p can blend.

$$Priv_{ASS} \equiv |AS_t|$$

where $|AS_t|$ is the anonymity set of the targeted node. One of the disadvantages of anonymity set size is that it does not take prior knowledge into consideration. It solely relies on the number of users in the system. However, the combination of anonymity set size and normalized entropy [38] provides a better privacy guarantee.

2) Entropy: In location privacy, entropy is the quantitative measure of the of the attacker's uncertainty. The measure of the quality of the cloaked location [39]. As a measure of privacy, it can be described as the actual size of the of the anonymity set. The authors in [40] describe Entropy as the additional information needed by the adversary to identify the user. As shown in the equation below, the estimated probabilities of the adversary are indicated by the random variable X for every user in the anonymity set. Entropy is very useful when privacy is measured more than once. In location privacy, entropy is computed continuously as a result of the continuous tracking by adversaries. The authors in [41], [42] use entropy as a measure of the accuracy of an adversary in disclosing the user's position. Entropy can be expressed mathematically as;

$$Priv_{ENT} H(X) = -\sum_{i=1}^{N} p_i log_2(p_{(i)})$$

where N represents the number of nodes in the anonymity set and p_i represents the probability of i being the targeted node based on the adversary's estimation. In [43], normalised entropy (degree of anonymity) is used for mix-zones. Normalised entropy is the ratio of the entropy obtained from the road network to the entropy obtained from the theoretical mix-zone with the same anonymity set. Pairwise entropy has also been used in a similar way. Pairwise entropy is the entropy between two users who are the only members of an anonymity set. Pairwise has two mapping set, two mapping probabilities and two events (entry and exit) [43], [44].

3) k-Anonymity: Location k anonymity is achieved when the exact locations of the user are extended to the cloaked regions so that each region covers at least k-users. Although a formal model for k-anonymity was first presented for statistical databases in [45], It has been used widely used for location privacy in mobile networks. In location k-anonymity, the user 's privacy is protected by the utilisation of the current location rather than the historical locations. The location cloaking strategies CliqueCloak [46], HilbertCloak [47], Casper [48] offer location k-anonymity.

4) Cloaking Granularity: Cloaking granularity is proposed to address the shortcomings of location k-anonymity. In cloaking granularity, the area of the cloaked region must be larger than the user-specified threshold [49]. Location k-anonymity does not prevent the disclosure of the user's information, it protects the user's identity (out of k users). Cloaking granularity prevents the user's information from being disclosed but fails to protect the users from identity-related attacks when the user's location is known publicly.

5) Success Rate of an Adversary: An adversary's success rate is a location privacy metric that measures the probability that an attacker is successful in tracking a targeted user. The authors in [26] point out that an adversary who is successful can compromise a communication channel or identify a message sender.

6) Expected Estimation Error: This metric measures the success of the adversary in reconstructing the targeted trajectory [50]. In location privacy, the expected estimation error of the adversary is computed by the expected distance between the true outcome x_c and estimated distance x using a distance metric d. In [50], the posterior probability is used to compute the expectation of the adversary's estimates x which is based on observations o.

$$Priv_{AEE} \equiv \sum_{x} Pr(x|o)d(x, x_c)$$

Generally, error based metrics quantify an adversary's error when creating his estimate.

7) Mean Time To Confusion (MTTC): Mean time to confusion uses entropy to measure the duration that an adversary's uncertainty is below a specified threshold. This is the time taken by an adversary to correctly follow a trace [41].

8) Flow-based Metric: Flow-based metric uses the statistics of the mix-zone to theoretically evaluate the effectiveness of the mixing provided by mix-zones [51], [52].

9) Accuracy of Obfuscated Area: The relevance metric models the relative accuracy loss of a given measure with respect to the maximum accuracy that would have been achieved in a perfect environmental condition [53].

10) Technological Relevance: This metric measures the accuracy of the location measurement provided by the LBS provider [54].

11) Tracking Uncertainty: This metric measures the probability that the sample location belongs to a targeted vehicle [41].

C. Privacy Attacks in LBS

In this section, we define the location privacy attacks in Mobile Services and Vehicular Networks identified in the literature.

Trace Analysis attack: In this type of attack, the historical cloaking regions are linked to the mobility pattern of the user. The LBS server can derive probabilities of the mobile user being at different locations of the cloaked region [39].

Colluding attack: Bogus location proofs are generated when two nodes collude with each other. For example, if a malicious node m_1 needs to prove that he is in a false location, he can have another colluding node to mutually generate bogus location proofs for him [35].

Location linking: An attack where the location information included in the query of the user is used as a quasi-identifier to reconfirm the identity of the user is described in [42] as a location linking attack.

Query sampling: The authors in [34] present this attack as a location privacy attack where an adversary uses the knowledge of the user's locations to link the user location to a particular query.

Snapshot location attack: The authors in [30] and [47] discuss inference attacks which are similar to trace analysis attacks. The future location of a user is traced through inference based on the user's movement in the past.

Query Tracking Attack: In continuous LBS, the queries have a lifetime which makes it possible for queries to be traced. A mobile user that is cloaked with other users at different instances during the lifetime of the query is susceptible to query tracking attacks [49].

Trajectory Attack: When an attacker uses a published trajectory from the LBS-server to deduce the trajectory of the user [55], [56]. Trajectory attacks can still be possible even if the identifier of the user has been removed [49].

De-obfuscation Attack: In de-obfuscation attack, an adversary evaluates the relevance gain or loss after a de-obfuscation attempt [53].

Timing Attack: The adversary observes the time of entry and exit for each mobile user [43].

Transition Attack: The adversary uses previous observations to estimate the transition probability for each possible turn in the intersections [44].

Reconstruction Attack: The adversary tries to reconstruct the actual trace by assigning probabilities to events that are possibly related to the trajectory of the user [57].

Inference Attacks: Similar to trace analysis attacks, Adversaries trace past movements to determine future locations [58], [28], [31].

IV. Location Privacy/Security in Vehicular Networks

In this section, a review of the proposed approaches to location privacy and security are discussed. We divide this section into two groups; privacy enhancing schemes and privacy-preserving authentication schemes that address location privacy.

A. Privacy Enhancing Schemes That Address Location Privacy

1) Mix-zones Approaches in Vehicular Networks: Mix-zones enhance location privacy using anonymous communication zones. These zones are mostly road intersections where the speed and direction of a vehicle is likely to change. When a vehicle enters a mix-zone, it stops sending messages and updates its pseudonym. The effect of changing pseudonyms frequently in location privacy is examined by the authors in [59]. In this approach, traffic is generated on non-trivial road maps with realistic parameters. The authors assume that the antennas are positioned by attackers in the network to overhear communication. In their analysis of the effectiveness of mix-zones, they conclude that the optimal frequency of pseudonym change depends on the attributes of the mix-zones such as the location, size and the number of entry points.

In [60], mix-zones are created using cryptographic techniques CMIX at road intersections within the broadcast distance of the RSUs. The CMIX protocol distributes symmetric keys using traditional asymmetric cryptography for the establishment of the cryptographic mix-zones. In the Cmix-zone, all broadcast messages by vehicles are encrypted with the symmetric key distributed by the RSU. The authors claim that CMIX makes it difficult for an attacker to link the identity of a vehicle since the same key is used by all vehicles.

A context mix model is introduced in [28], [61] to protect location privacy in vehicular networks. They argue that even pseudonyms are changed at random intervals, several approaches can be used by the attacker to identify the nodes. They describe the mix-zones in [62] as mix-context situations and include the use of context information such as speed, direction and number of vehicles to initiate a pseudonym change. To protect vehicles from location tracking, they define a threshold for the minimum entropy to identify the best opportunity for a pseudonym change. The user or the application where the pseudonym change is triggered is used to define the minimum entropy.

To achieve receiver-location privacy in VANETs, the authors in [63] propose a social-tier-assisted message forwarding protocol (STAP). STAP protects receiver location privacy from active global attackers by disseminating messages to social tiers. Similar to the works in [64], [65], they use social spots to observe busy intersections in a city environment. The social tier is a virtual tier formed by social spots. RSUs are deployed at social spots and a virtual tier is formed with them without knowledge of the location of the receiver. When the receiver enters one of the social spots, it can successfully receive the message that was disseminated to the social tier. The receiver holds the family of the pseudo-IDs which are unlinkable and the pseudo-IDs are repeatedly used in the mutual authentication between the RSUs and the receivers at social spots.

In [64], [65], the authors propose changing of pseudonym at social spots (PCS) as a strategy to achieve high location privacy. Vehicles temporarily gather at social spots such as free parking lots that may be close to a shopping mall or at road intersections when the traffic light turns red. They state that a social spot becomes a mix-zone if pseudonyms are changed by all the vehicles before leaving that spot. An indistinguishable information is broadcast as safety message which shows the location of the vehicle as a social spot at a velocity of 0 with an unlinkable pseudonym. They show that when pseudonyms are changed by all the vehicles simultaneously, the high density makes it difficult for attackers to track the vehicles. However, pseudonym changing at social spots does not provide sufficient privacy protection when the vehicle density is low.

In [51], a user-centric game-theoretic mix-zone approach is introduced to measure the evolution of location privacy over time and evaluates its behaviour in mobile, vehicular and delay tolerant networks. They argue that even though the cost of location privacy is reduced by selfish nodes, it can also threaten the efficiency achieved by multiple pseudonyms in non-cooperative scenarios. They carry out an analysis on static games using a complete information to get pure and mixed Nash Equilibria. Using a Bayesian approach, they study an incomplete information scenario where nodes have no complete knowledge of the pay-offs of neighbouring nodes. They look for a symmetric equilibrium where all the nodes cooperate with the same probability and analyse a dynamic version of the game showing how it copes with uncertainty. The pseudonym changes are coordinated by Pseudo-game protocols which are designed to implement pseudonym change strategies.

Lu *et al*. [66] propose a MixGroup scheme for location privacy. Based on sporadic observations, they exploit meeting opportunities to change pseudonyms and improve location privacy. Observations are made from real vehicle traces based on social spots and sporadic observations. MixGroup is used to construct an extended pseudonym group region where vehicles can change their accumulated pseudonyms. Each group has a group leader and a group identifier. When a vehicle enters a group, the group leader will assign a group ID with a certificate and a private key to the new vehicle after authentication. The group ID, certificate and the private key are used for changing pseudonyms and broadcasting safety messages. An entropy-optimal negotiation procedure is used to facilitate the process of exchanging pseudonyms among vehicles. They quantitatively measure the risk and benefits associated with the pseudonym exchange using a pre-defined pseudonym entropy.

2) Silent Period Schemes in Vehicular Networks: A user-centric scheme for mitigating location tracking is proposed in [67]. In the Swing technique, the pseudonyms are changed by the vehicles when their speed and directions are changed. This makes it difficult for an attacker to correlate the locations of the node before and after an update by utilizing the movement predictions of the nodes. In the Swap technique, location privacy is maximised by the exchange of the vehicle identifiers. The vehicles exchange their pseudonyms with a probability of 0.5 during an update and then enter a silent period. However, indistinguishability is only achieved by the cooperating vehicles from the vehicle that initiated the pseudonym change.

In [68], authors pay attention to the mitigation of unauthorized location tracking and LBS profiling from service providers. They identify the vulnerabilities from accumulated location history of vehicles over time. They also consider the vulnerabilities associated with additional information from visited locations from places of interest using geographical maps thereby enabling profiling of personal interest. They propose a scheme (AMOEBA) based on the group navigation of vehicles for user and location privacy. AMOEBA uses a group concept to provide location privacy. A random silent period is used to provide unlinkability between the locations of a vehicle. They consider a scenario where a target vehicle joins the network and broadcast safety messages. This target vehicle remains silent and updates its pseudonym from C to C′ then broadcast with C′ after a random silent period. If a neighbouring vehicle also updates its pseudonym from D to D′, the attacker can be misled to track the vehicle as the target as illustrated in the scenario in Fig. 1.

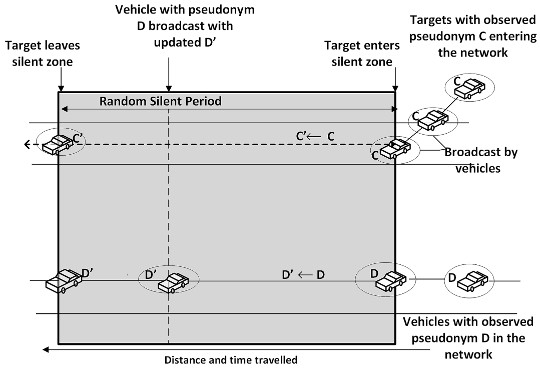

Vehicle with pseudonym D broadcast with updated D′
Target leaves silent zone
Target enters silent zone
Targets with observed pseudonym C entering the network
Random Silent Period
C′
C′← C
C
C
C
Broadcast by vehicles
D′
D′
D′ ← D
D
D
Vehicles with observed pseudonym D in the network
Distance and time travelled

Fig. 1: Effect of random silent period by a vehicle joining the network

In [69], the author discusses the general issues on pseudonym changing in VANET. They focus on the influence of the mobility of the vehicles on pseudonym changes by adjusting the silent period based on the mobility of the vehicle. They identify two parameters (node re-interaction and quiet time) which must be assessed to improve the efficiency of location privacy achieved by pseudonyms. These parameters are mainly influenced by the node mobility characteristics. In order to achieve a high degree of unlinkability between the pseudonyms, they claim that an optimal interval for pseudonym change must be adapted to the node interaction interval.

Different from the approaches in [69], [68], a silent period technique SLOW (silent on low-speed) is proposed in [70]. The SLOW protocol does not need an infrastructure or cooperation from neighbouring vehicles. When the speed of the vehicle drops below a pre-defined threshold, vehicles do not transmit messages. They define this period as the silent period where vehicles can change their pseudonyms.

They describe a scenario in an urban area that is crowded whenever a group of vehicles stop at the traffic signal point. They also create mix-zones at the points where there are maximum uncertainties about a vehicle. The authors claim that SLOW ensures a smooth synchronization process when the pseudonym is changed in the silent period. SLOW also reduces the burden of large verification of digital signatures when the vehicle density is large.

The authors in [71] look into the tracking of broadcast communication of vehicles by adversaries. They propose a location privacy scheme (CARAVAN) to unlink the locations of a vehicle. They describe two tracking methods (simple and correlation tracking) used by adversaries to link two possible locations of a vehicle and take into account the mobility and application features of VANETs. CARAVAN combines a silent period enhancement technique with group navigation to prevent the tracking of vehicles. The group navigation provides unlinkability between the vehicle's pseudonym and the LBS application that is accessing the service. When an application request is received from a vehicle, this request is forwarded by the group leader using its own address to the registration authority. through the RSU. A session key is provided by the registration authority to both the LBS provider and the vehicle after the validation of the application request. The entire communication between the vehicle and the LBS provider is encrypted by this key.

3) Caching Schemes in Vehicular networks: To prevent untrusted LBS from tracking the user locations, the authors in [72] introduce an intermediary server (CacheCloak) between the LBS and the user. The CacheCloak server mediates the flow of data by returning a cached data or getting a new one from the LBS server when there is a request from a user for a location-centric data. CacheCloak generates a predicted path for the user which extends till both ends are connected to other paths in the cache. They claim that an attacker is unsuccessful trying to track the location of a user anonymized by the CacheCloak scheme as a result of the newly generated path triggered by the scheme. However, the proposed CacheClock scheme cannot meet the demands of real-time applications and complete service availability.

The authors in [73] point out that majority of the end users are not aware of the implications of LBS and end up disclosing their personal data unintentionally. They introduce a generalized approach (Cache) to minimize the privacy threats associated with LBS. In Cache, the location enhanced content can be pre-fetched before it is needed. This content can be accessed locally from the mobile device when needed. On each location request, the user can share general geographic information rather than its current location. They carry out a feasibility analysis to show that location data can be potentially cached. One of the disadvantages of the proposed scheme is its unsuitability for real time applications such as applications that require the user to check in to a particular location from a server. Another downside of the Cache scheme is the limitation in the size of the cells in the content download, update and priority grids which is defined by the developer of the application.

In [74], authors propose a framework that enhances the privacy of LBS in vehicular communication. The focus on dedicated short-range communications and explore the unique features of queries from in-vehicle users. In this approach, the data is periodically broadcast by RSUs. The vehicles download the data which are cached by the OBU. When POI information is requested by an in-vehicle user, it checks with the OBU to avoid issuing incoherent queries or duplicates to the LBS server. The authors point out that if an attacker obtains LBS information, the trajectory and point location privacy are leaked. They develop a POI query probability model based on space-related feature of LBS queries. Three broadcasting content selection algorithms are developed using knowledge-based pre-caching and an adaptive updating method to enhance the location privacy of users. In a detailed performance analysis, they claim that their proposed scheme can protect location privacy by reducing the number of queries needed for LBS.

4) Obfuscation Approaches in Vehicular Networks: In [41], a delay is introduced into the anonymization process. The basic idea is using a path confusion algorithm to perform a posteriori analysis of the path of the users. Assuming two users pass through an intersection similar to [62] at time t_0 and t_1 respectively where $t_0 < t_1 < t_0 + t_{delay}$. The posteriori analysis is performed at t_{delay}. The paths intersect in a way that anonymity is created. Although two users were not in the location at the same time, the user location is not known by the LBS until both have crossed the intersection point. In this scheme, the real time operation is compromised by the introduction of delay. If the anonymity accumulated after t_0 + t_{delay} is insufficient, the path confusion algorithm may not release the location of the user to the LBS.

A mutual obfuscating path (MOP) [75] is proposed for location privacy in connected vehicles. MOP is used to retrieve spatio-temporal information in real time. Different from other approaches, MOP does not make use of the intersections in the user's path. MOP takes advantage of the dedicated short range communication (DSRC) radios to obfuscate location tracking. They consider a communication range of $200 - 400m$ as the DSRC beacon when two vehicles communicate using the LBS server to determine whether the MOPs can be generated. MOP is performed when a vehicle receives a beacon. As explained in [75], assuming vehicle A wants to mutually obfuscate the path with vehicle B, the kinematic information such as the current location loc^B_{cur}, speed $speed^B_{cur}$ and the direction dir^B_{cur} are used to define a threshold for the convergence time T_{thld}. The MOP process requires cooperation from neighbouring vehicles. According to the authors, a selfish or non-cooperative vehicle threatens its own privacy by not cooperating since the LBS uses posteriori reasoning to guarantee the mutual obfuscation of all connected paths.

In Table 1, we provide a detailed summary of location privacy enhancing schemes, privacy metrics used and location privacy attack addressed in for vehicular networks.

B. privacy-preserving Authentication Schemes that address Location Privacy in Vehicular Networks

In this section, we discuss privacy-preserving authentication schemes that achieve location privacy. These privacy-

TABLE I: Summary of Privacy Enhancing Schemes that address Location Privacy in Vehicular Networks

Category	**Strategy**	**Privacy Metric**	**Location Privacy attack addressed**	**Issues Addressed**
mix-zone	Buttyan *et al.* [59]	Entropy	Movement tracking	Evaluates the success probability of an attacker based on traffic density.
mix-zone	CMIX [60]	Adversary success ratio & Entropy	Location tracking	Addresses indistinguishability, location privacy in the context of traffic congestion & vehicle density.
mix-zone	Context mix model [61]	Average tracking time	Inference attacks	Pseudonym changing based on traffic density.
mix-zone	STAP [63]	Delivery ratio & delay	Location tracking	Focus on location privacy of the receiver.
mix-zone	PCS [65]	Anonymity set size	Location tracking	Anonymity set analysis for small and large social spots.
mix-zone	Freudiger *et. al.* [51]	Upperbound	Trace analysis	Measures evolution of location privacy with game-theoretic model.
mix-zone	MixGroup [66]	Entropy	Region-based location tracking & trajectory reconstruction	Enhancement of location privacy by the integration of group signatures and the construction of a pseudonym changing region.
Silent Period	Swing & Swap [67]	Entropy	Location tracking	Maximizing & increasing location privacy .
Silent Period	AMOEBA [68]	Entropy	Simple and correlation tracking	Addresses location privacy by mitigating location tracking and user privacy by providing anonymous access to LBS.
Silent Period	Eichler [69]	Average required quiet time	N/A	Uses node re-interaction and quiet time to increase the degree of unlinkability
Silent Period	SLOW [70]	Tracking success rate	Syntactic and semantic linking	Ensures synchronized silent period and pseudonym change for many vehicles.
Silent Period	CARAVAN [71]	anonymity set size	Simple and correlation tracking	Addresses location privacy threats due to location tracking attacks.
Caching Scheme	Cache [73]	Pre-fetching & disconnected operation	N/A	Adjust the size of the geographical content to improve user location privacy.
Caching Scheme	CacheClock [72]	Location entropy	Location tracking	Predicted paths are extended until they intersect with other paths in the cache to prevent location tracking.
Obfuscation Scheme	Path confusion algorithm [41]	Mean time to confusion & tracking uncertainty	Trace analysis	Guarantees a defined maximum time for all vehicles including vehicles in low density areas.
Obfuscation Scheme	MOP [75]	Location entropy & tracking success	Location tracking	The true path of the vehicles are hidden over long trajectories.

preserving schemes are based on symmetric and asymmetric key cryptography in vehicular networks.

1) Symmetric Key Authentication Schemes (SKAS): Symmetric encryption is often referred to as single key cryptography. In symmetric encryption, a single key is used the sender and receiver in the encryption process where both parties must agree on a single (shared) secret key. In VANETs, Symmetric Key Authentication Schemes (SKAS) use symmetric key cryptography for message authentication. Each vehicle uses its key or a group key that is shared for message verification.

In [76], the authors identify information contained in the message broadcast by vehicles as the position of the vehicles, speed and direction. They point out that this information can lead to tracking of vehicles by an adversary and highlight the necessity of protecting this information which is sent as broadcast messages by vehicles. They propose a privacy-preserving group communication PPGCV scheme for VANETs. PPGCV is based on a security threshold scheme and a probabilistic key distribution technique. In PPGCV, a new group key can be calculated and a compromised key list updated even if the vehicle has missed the group rekeying process. PPGVC has two phases: the key bootstrapping phase and the group rekeying phase. In the key bootstrapping phase, each vehicle in the network chooses a set of keys randomly from a key pool. This set of keys is used as key encrypting keys (KEKs) and an additional key is added for group communication. The group rekeying phase is initiated when the revocation of a vehicle's membership needs to be carried out by the key server. To achieve location privacy, each vehicle selects random keys from its key set and the IDs of those keys that have been broadcast. In PPGCV, the computation of the threshold scheme results in a high computational overhead.

Inspired by [77], a time efficient and secure vehicular communication protocol (TSVC) is proposed by the authors in [78]. A symmetric MAC operation is performed at the receiver to authenticate the source of the message. Different from the approach in [76], a short MAC tag is attached to each message to reduce the traffic density. To generate a MAC with neighbouring vehicles, a vehicle broadcasts a commitment of hash chain which is authenticated by other vehicles. The speed of the MAC verification of TSVC helps in the reduction of low ratio. More emphasis is laid on the privacy of the data source since each vehicle has a list of anonymous public/private keys alongside with their public key certificates at the initial stage. They claim that it is difficult to track the driver with the anonymous certificate due to the short lifetime of the public key certificate. The proposed scheme addresses only the privacy of the data source, TSVC is vulnerable to trace analysis attacks as TTPs can reveal the identity of the targeted vehicle by using its pseudo-ID to perform a database lookup.

The authors in [79] propose two schemes (RAISE and COMET) to preserve privacy in VANETs. RSU-aided Authentication Scheme (RAISE) and Cooperative Message Authentication Schemes (COMET) are targeted at VANET applications. RAISE adopts the property of k-anonymity where a message cannot be linked to a vehicle. The RSUs assist the vehicles in the authentication of messages. Key agreement and mutual authentication are first performed when a vehicle enters the region covered by the RSU. This is followed by a short MAC generated by the sender and shared between the sender and the RSU. The authors claim that communication overhead is reduced compared to other approaches and that there is an improvement in the efficiency of the authentication when RAISE is used. In the early deployment of VANETs where RSUs may not be widespread, a supplementary scheme COMET is used to verify a small percentage of the message signatures based on their computational capacities. Although location privacy has not been explicitly addressed, the authors look into user related privacy information such as the travelling route, name of the driver, model of vehicle and the licence plate. RAISE is highly dependent on infrastructure and no provision has been made for key revocation.

The authors in [80] point out that PKI cannot provide certain security requirements such as location privacy. They introduce complementary security mechanisms that can meet the security requirements of location privacy. The proposed privacy scheme is based on random encryption period (REP) [81]. This approach relies on a security threshold scheme and a probabilistic key distribution. They point out that location privacy can only be achieved if the OBUs changing their certificates have an anonymity set size that is greater than one. REP is triggered when there is a request by an OBU to change its certificate. REP uses a secret key to create an encryption zone around the OBUs and this group key is shared between the OBUs. REP also prevents adversaries from overhearing messages when there is a certificate update, this action decreases the probability of tracking an OBU.

A dynamic privacy-preserving key management scheme (DIKE) is proposed in [82]. Each vehicle is authenticated before joining an LBS. A pseudo-ID is used to hide the identity of a vehicle during the service session. To achieve privacy preservation, a privacy-preserving authentication mechanism is used which also provides restriction for double registration entries. The service session key update procedures is divided into different time slots, each time slot holds a different session key. To reduce key update delay, the forward secrecy technique is used to update the new key session autonomously. A dynamic threshold technique is used to achieve backward secrecy. The authors claim that the proposed scheme is more flexible and can resist possible collusion from the vehicles that leave the LBS session.

2) Asymmetric Key Authentication Schemes (AKAS): Asymmetric Key Authentication Schemes (AKAS) use Public Key Cryptography (PKC) or digital signatures for signing and verification of messages. In AKAS, two keys (public and private) are used for encryption and decryption. A message encrypted by the public key can only be decrypted by the corresponding private key. AKAS can be classified into two categories: Public Key Infrastructure (PKI)-based and Identity (ID)-based authentication. The PKI-based authentication relies on accessibility to infrastructure to verify, revoke and add new certificates. ID-based authentication uses ID-based crypto-systems to reduce communication overheads. ID-based authentication simplifies the process of managing certificates by using the identity of the vehicles in signing and verifying digital signatures [83].

In [83], the authors propose group signatures and identity-based signatures to address security and conditional privacy preservation. The group signature is used to secure the communication between the OBUs. The senders anonymously sign the messages and their identities can only be revealed by the authorities. To authenticate the messages sent by each RSU, identity-based signatures are used to digitally sign each message. GSIS consist of four phases, the first phase is the registration of members by the membership manager who generates a private key for each vehicle. In the second phase, the message is signed by the vehicle and processed in the third phase. A time-stamp is used to verify the signature and membership traceability is achieved in the fourth phase using the real identity of the message signer.

In [84], an efficient and a robust pseudonym-based authentication scheme is proposed. The authors point out that messages produced by a vehicle over a protocol selectable period can be linked. However, messages generated at different time intervals t_1, t_2 cannot be linked if $t_2 > t_1 + \gamma$ (where γ is the protocol selectable period). They point out that when γ is shorter, it is difficult to track the messages. They propose a hybrid signature scheme which combines group signatures (ECDSA) and a pseudonym scheme. Each vehicle is equipped with a group public key and a group signing key. These keys are certified by the authorities without revealing any information identifying the vehicle. This scheme uses a self-generating pseudonym scheme to eliminate the need for storing, refilling and correspondent private keys. Although a targeted vehicle becomes less traceable as γ becomes smaller in dense environments, vehicles will incur more computational and communication cost based on this approach.

An efficient conditional privacy-preserving (ECPP) scheme is proposed in [85]. ECPP addresses unlinkability attack, which is described in this context as the moving track attack on the location of the OBU. They develop a probabilistic model to characterize the risk from compromised RSUs. They assume that 0.2% of the RSUs can be compromised at most since the RSUs are robust in reality. The Location privacy is guaranteed using the short time certificate. A short group signature scheme based on verifier local-revocation [86] is constructed to provide anonymous authentication. They claim that the short-term certificate guarantees the location privacy of the OBU since the location of the OBU cannot be judged.

In [87], authors propose a location privacy scheme using blind signatures to hide the identity and trajectory of moving vehicles. They use a fast blind signature based on elliptic curve cryptography to generate fast signatures and define the overlapped radiation range of two APs as a blind zone. In Fig. 2, we illustrate the working principle of the blind zone with many vehicles moving into the blind zone. AP 2 does not know which AP the vehicles are handed over from and the vehicles in the serving area cannot be distinguished. In the proposed scheme, the authentication credentials used by the vehicles to perform handover are blind to the APs that are not associated with the serving area. If a vehicle v moves from one AP serving area AP_i to another AP_{i+1}, the vehicle sends a message through AP_i. AP_i is responsible for sending authentication information about v to AP_{i+1} in advance which is regarded as a pre-authentication. AP_{i+1} signs the message without knowing its contents. Movement tracking is avoided with tracking probability. They use a tracking probability to describe the probability that a vehicle is being tracked and formulate the tracking probability as, $P(n, s) = \prod_{i=1}^{\frac{s}{d}} \frac{1}{n_i} \approx \frac{1}{n^{\frac{s}{d}}}$ where d is the diameter of an AP's radiation range, n is the average number of vehicles over the total blind zones and s is the total distance travelled. They show that the more the average number of vehicles over the total blind zones the more efficient the tracking probability.

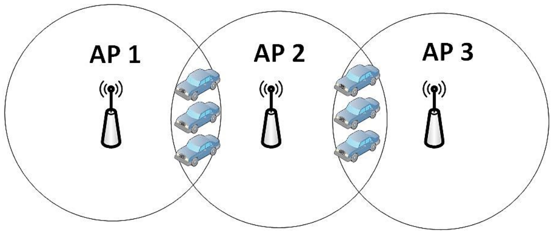


Fig. 2: The blind zone

In [25], authors propose temporary anonymous certified keys (TACKs) to provide privacy in VANETs. In TACKs, the OBU uses a private/public key pair to sign broadcast messages. These signatures ensure a short-term unlinkability and message integrity. This is because the signature is generated only by the owner of the private key and a single key pair is used by the OBU for a short period of time. They agree that group signatures and region based certificates provide long-term unlinkability. However, they argue that cryptography does not provide protection against correlation attack. In correlation attack, an adversary observes the temporal and spatial correlations between the different keys to track target vehicles. An adversary can associate an old key with a new one if the keys are changed by a single OBU at a time. TACKs addresses long-term unlinkability using the anonymity set size. They use a traffic model with Poisson distribution rate of $\lambda = [0.5, 0.8]$ to analyse vehicles moving along the highway. They describe the number of vehicles entering a new region and changing keys simultaneously as $X \sim$ Poisson $(\delta.\lambda)$ based on the batching response for δ seconds. They use iterated expectations to determine the size of the anonymous set after the OBU has changed its region.

In [88], a Light-weight Privacy-Preserving protocol (LPP) is proposed to provide mutual authentication for V2V and V2I communications. LPP integrates chameleon signature with ECDSA to provide security and privacy for VANET communication. They point out that unlinkability may not be guaranteed as the public key issued by the signer for verification may be peeped by attackers. The authors redesign the chameleon hash signature with Abelian group formed by the points on the elliptic curve [89]. The proposed LPP consist of three phases: the mutual registration phase, the authentication phase and the tracking phase. In the mutual registration phase, The OBUs and the RSUs register to a CA where related secret information is preloaded. In the mutual authentication phase, the RSU initiates authentication with the OBU by establishing a pair-wise key between each other. The tracking phase is initiated when there is a dispute event to be resolved by the CA. They claim that LPP achieves anonymity and unlinkability using the pair-wise key which produces encrypted certificates.

An authentication framework with privacy preservation is proposed by the authors in [90], [91]. This scheme uses an ID-based cryptography and self-defined pseudonyms to preserve location privacy. An ID-based Offline Online Signatures (IBOOS) scheme is used to authenticate V2V communication while an ID-based signature scheme is used for V2R and R2V authentication. They focus on identity revealing and location tracking attacks. The authors claim that by updating the pseudonyms frequently during communications, the proposed scheme successfully defends the vehicles against location tracing and user profiling.

A decentralized lightweight authentication scheme TEAM (Trust-Extended Authentication Mechanism) is proposed by the authors in [92] for highly dynamic environments. TEAM does not use a central authority to authenticate vehicular communications, the concept of transitive trust is adopted to improve the authentication procedures. They address movement tracking attacks in V2V communication and classify vehicles based on trust relationship. A dynamic identification process is used to prevent the attacker from tracing the vehicle's physical position. The session key is generated using a pseudo-random number. They claim that when the OBU has no access to service, it uses random silent period scheme to enhance its location privacy.

We summarize the cryptographic approaches proposed in literature for Vehicular networks in Table II.

V. Location Privacy/Security in Mobile Networks

In this section, we review the existing works on location privacy approaches for mobile networks. We divide this section into two categories. The first category discusses the location privacy enhancing technologies proposed in literature. The second category presents the cryptographic schemes that address location privacy in mobile networks. We also review the different techniques for preventing location related attacks.

TABLE II: Summary of Authentication Schemes that address Location privacy in Vehicular Networks

Scheme	Cryptographic method	Communication Pattern	Non-Repudiation	Emergency Communication	Mechanism for Privacy Preservation	Location Privacy attack addressed
GSIS [83]	Group & ID-based Signatures	V2V & V2I	Yes	Yes	Anonymity-based	long-term Unlinkability
Hybrid [84]	Group Signature & ECDSA	V2V	Yes	No	Pseudonym-based	Long-term tracking
PPGVC [76]	HMAC	V2V	Yes	No	Anonymity-based	N/A
TSVC [78]	HMAC	V2V	No	No	Pseudonym-based	Source node privacy
RAISE [79]	HMAC	V2V & V2I	Yes	No	Pseudonym-based	Trace analysis
REP [81]	PKI	V2V & V2I	Yes	No	Pseudonym-based	Location tracking
ECPP [85]	ID-based Cryptography	V2V & V2I	Yes	No	Anonymity-based	Movement tracking
Zhang *et al.*[87]	Blind Signatures-ECC	V2I	Yes	No	Anonymity-based	Movement tracking
TACKs [25]	ECDSA-based PKI	V2V & V2I	Yes	No	Pseudonym-based	Correlation attacks
LPP [88]	EC-Chameleon Hash	V2V & V2I	Yes	No	Pseudonym-based	Unlinkability
Lu *et al.* [90]	ID-Based Cryptography and Signatures	V2V & V2I	Yes	No	Pseudonym-based	Location tracking
TEAM [92]	SHA-512	V2V	No	No	Anonymity-based	Movement tracking
DIKE [82]	ID-based Signatures	V2V & V2I	No	No	Pseudonym-based	Collusion attacks

A. Location Privacy Enhancing Schemes in Mobile Networks

1) mix-zones in Mobile Networks: The concept of mix-zone was introduced by [62] and refined in [93] by the same authors. In the mix-zone model, the identity of a user is anonymized by putting a limit to the positions a user can be located. They define a mix-zone for a connected spatial region for a group of users. The model assumes that there is a middle-ware system that is trusted which is placed between the location services and third-party applications. The third-party applications are provided with anonymized location information using the middle-ware mechanism. The anonymity set technique is applied to location information collected at different intervals. The mix-zone model prevents the tracking of long-term movement of a user. Evaluation results show that there is a higher degree of unlinkability over a larger and more populated area between pseudonyms. However, they identified their drawbacks as the quantitative measure of the location privacy used. According to them, the size of the anonymity set only is an upper bound estimate and recommended the use of location entropy which is derived from historical data. The authors in [52] clearly point out that the success of the adversary in tracking location information is relatively high even if the mix-zones are placed in optimal locations. This is because the users must remain silent inside the mix-zones with no communication with the LBS. This approach also increases the linkability of user queries since the size of mix-zones are kept small.

In [52], a mix-zone is modelled as an optimization problem. They consider a network with a Trusted Authority (TA) that is responsible for the security and privacy of the network. Based on the mobility profile of mobile nodes, they propose a metric for evaluating the effectiveness of possible mix-zone locations. An analysis of the optimal placement of mix-zones is carried out with combinatorial techniques to maximise the achieved location privacy.

MobiMix [43], [44] is proposed for mobile users travelling on road networks. They point out that where there is a high uncertainty in the trajectories followed by users, mix-zones can be constructed as road intersections. Compared to the approach in [62], they identify the challenges imposed by the road network on the anonymity provided by mix-zones. As an example, they use the timing information of the user's entry and exit into the mix-zone. The non-uniformity of these transitions at road intersections are also taken into considerations. These constraints give adversaries information to predict the mapping between old and new pseudonyms. They argue on the construction of mix-zones and take certain factors into consideration including; the geometry of the zones, the temporal and spatial resolution of the location exposure, the statistical behaviour of the user population and the constraints on the movement pattern of the users. A suite of mix-zone construction technique is developed to guarantee a certain level of privacy regarding unlinkability between the old and new pseudonyms.

2) Obfuscation-based Approaches in Mobile Networks: Location privacy threats may be reduced by degrading the precision of location information [94]. In [95], authors propose an obfuscation and a negotiation approach for location privacy. A framework for obfuscated LBS is defined with a computationally efficient mechanism for balancing high-quality information needs against the individual needs for location privacy. They use imprecision to degrade the quality of location information. Negotiations are used to ensure that the service provider of the LBS has access to only the services associated with it. Negotiation also provides guaranteed satisfaction to mobile and location-aware systems.

A spatial obfuscation approach is presented in [96], [53]. They propose a location privacy technique that protects user's privacy according to their application context and preferences. A new dimensional metric called *relevance* is introduced. This metric provides a measure of the privacy of location measurement and a dimensional technology dependent measure of the location accuracy. The main contribution of this approach is the protection of the user's path privacy. One advantage of this obfuscation approach is that it provides location privacy without using a TTP, a user can define the obfuscation area. However, there is a degradation in the precision of user's position. Cheng et *al*. [30] studied the trade off between privacy and precision. They propose an intuitive model for cloaked location data representation. Their work focuses on location-based range query (LRQ). The current location of a user within a fixed distance is used for the notification of any object of interest when issuing an LRQ. LRQ is a type of query commonly used in applications using LBS. To cloak location data, they propose an imprecise location-based range query technique (ILRQ). ILRQ provides probabilistic certainties to queries indicating the degree of confidence in these queries. They introduce patching and delaying to prevent the location of the user from being deduced. Patching combines the previous cloak locations with current cloak location. Delaying technique is based on the delaying the timing requirements, the request is suspended until the location that is cloaked fits into the maximum bound.

The authors in [57] argue that the distortion actual trajectory of the users and the envisaged reconstructed trajectory, the better the location privacy that will be achieved. They point out that the degree of location privacy by a privacy-preserving mechanism depends on how ineffectual the attacker is in the reconstruction of the locations of the users overtime. They propose a distortion-based metric to measure the location privacy of mobile users. This metric measures the user's location privacy using the distortion level in each part of the reconstructed trajectory of the user by the attacker.

The authors in [97] point out that the user's location privacy information can be obtained by observing the sequence of successive query request. They propose a comprehensive trajectory privacy approach with ambient conditions to cloak user's location depending on the privacy profile of the user. They use an r anonymity mechanism to pre-process a set of trajectories that are similar. This is done to blur the user's actual trajectory. To protect the privacy of the user, k-anonymity is combined with the road segments. To hide the trajectory of the user, they introduce a time-obfuscated technique which breaks the sequence of issuing time for the queries to confuse the LBS about the user's trajectories.

3) Location Cloaking in Mobile Networks: One of the most popular approaches used in protecting location privacy is the location cloaking technique. In [42], the authors formulate a metric for location anonymity. They clearly point out that depending on the trusted entities, anonymization in LBS must be tackled at different levels in the network. They propose an adaptive interval cloaking technique (Interval Cloak) for location broker services that are centralized. They point out that disclosing the exact snapshot location can result in location linking attacks. In this type of attack, the adversary obtains location-based information from the user query to re-identify the user. A quadtree-based algorithm is introduced to reduce location resolutions which guarantee k-anonymous location information.

A spatio-temporal cloaking based on k-anonymity model is proposed by [46], [98]. Different from the approach in [42], which makes use of a uniformed k for all messages; they use efficient algorithms to support customizable k per message. Based on the specific privacy requirements, a different k anonymity value is used to identify each message. They propose a new cloaking algorithm called CliqueCloak. In order to maintain the desired k-anonymity property, a preferred spatial and temporal tolerance level is specified by each message. To anonymize a message that originates from a mobile user, the spatial location information contained in the message is changed into a two-dimensional spatial box. The cloaking algorithm converts the time-stamp of the message into a temporal interval based on the message's anonymity constraint specification.

A Peer-to-Peer spatial cloaking algorithm is presented in [99]. In this approach, mobile and stationary users can enable LBS without revealing their exact location information. Mobile users form a group with neighbours before requesting for LBS using single or multi-hop routing. The spatial cloaked area is computed as the entire region that covers the neighbouring nodes. The two modes of operations supported are; the on-demand mode and the proactive mode. In the on-demand mode, the cloaking algorithm is executed by the mobile nodes when they need to access information from the LBS server. In the proactive mode, mobile clients look around occasionally to find the desired number of peers. To get information from the LBS server, they cloak their exact locations into spatial regions.

The authors in [99] propose a new framework called Casper [48] for providing privacy to mobile and stationary users. Casper has two main components; a privacy-aware query processor and a location anonymizer. The privacy-aware processor is placed in the LBS database server. This is done specifically to deal with cloaked spatial area instead of the exact location information. The anonymizer smears the exact location information of the users. Three query types are introduced to the LBS server; private queries over private data, private queries over public data and public queries over private data. A privacy-aware processor is introduced to produce a unified framework for the new query types. They also point out that scalability and accuracy are achieved with a large number of users with different privacy requirements.

In [100], authors investigate the problem with location cloaking to meet the specified privacy requirements of the user for continue LBS queries. They propose a mobility-aware cloaking technique to resist trace analysis attacks. The mobility-aware cloaking technique consists of 3 components; a mobility location cloaker, a progressive query processor and a result refiner. The mobility location cloaker cloaks the location of a user to a region while the progressive query processor evaluates the result superset for the location-based query. The result refiner filters the superset to produce the same query result for the user.

In [34], the authors identify the limitations of the applicability of existing privacy location techniques. They point out that existing works do not differentiate between location and privacy queries. They propose a new spatial cloaking algorithm that clearly differentiates between location and query privacy using snapshots and location-based queries. The proposed approach provides support for private LBS to users with public locations. Spatial cloaking is performed when queries are issued rather than rigorously cloaking every single location update. The main objective of this approach is to anonymize the link between the user's location and the location-based queries. This anonymization protects the user's location from adversaries trying to link the user's location to the submitted query.

The authors in [101] argue that the complete knowledge of the entire system poses a serious threat if the anonymizer is compromised. They clearly point out that proposed techniques may fail to provide spatial anonymity for some distribution of user locations. To preserve the anonymity of users, they propose a decentralised architecture called PRIVE for issuing spatial queries to LBS. Based on the Hilbert space-filling curve, they develop a k-ASR construction algorithm that guarantees the anonymity of the queries issued even if the location of the user is known by the adversaries. They also develop a distributed pool for mobile systems to form a fault-tolerant overlay network through self-organisation.

A framework is proposed by [55] to provide anonymity guarantee while requesting for LBS. They identify two main issues: the assumptions made in each scenario about the knowledge of the attacker and the quasi-identifiers in LBS request. They clearly point out that attacks are not properly characterized and defined. To this effect, they define the notions of attack, defence function and safe request based on the attacker's perceived knowledge. They model different types of knowledge that may be available to the attacker and develop a generalized algorithm that assumes knowledge about the location of users.

In [102], a PRIVACYDGRID approach is presented in mobile information delivery systems. This approach supports anonymous location-based queries and provides a unified location anonymization framework. They develop a profile model with privacy preference which allows mobile users to define their preferred location privacy requirements. They also develop cloaking algorithms for k-anonymity and location l-diversity models for the PRIVACYDGRID framework. A bottom-up and top-down search technique for cloaking regions are combined to lower the anonymization time.

A non-exposure cloaking algorithm is proposed by [103], this algorithm is specifically designed for k-anonymity. The proximity of information among users is used to perform the cloaking rather than their mobile coordinates. Two problems are formulated by cloaking users without exposing their accurate locations: secure bounding and proximity k-clustering. An optimal progressive bounding algorithm is proposed for secure bounding which they claim is cost effective. A t-connectivity k-clustering algorithm is proposed for k-clustering to isolate clusters. Authors claim that these privacy aware algorithms are robust and efficient under various system settings and proximity topologies.

In [47], two cloaking algorithms are proposed to prevent location identity inference of users issuing spatial queries to LBS. The first cloaking algorithm - Nearest Neighbour Cloak (NNC) is a version of the Center Cloak which is resistant to anonymizing spatial region attacks. The NNC first determines the anonymity set containing user and his k-1 nearest neighbours. A random user is then selected from the anonymity set to compute a new set which includes the random user and his k-1 nearest neighbours. The second cloaking algorithm - Hilbert Cloak (HC) satisfies reciprocity which is an important property for spatial k-anonymity. Each user issues a query with an anonymity degree which is associated with anonymizing set and spatial region. The HC provides privacy guarantees under query distributions involving all users thereby providing a formal guarantee for the anonymization strength.

Another related work is [104], the authors look into applications that require frequent update from users. The anonymity probability distribution is taken into consideration during the computation of the cloaked region. They adopt the entropy of information theory to compute the level of location anonymity. They argue that k-anonymity protection is not guaranteed even if the cloaking area contains k entities. The probability of the users being in the cloaked region is considered in this approach as they point out that the users have different weights in terms of their contribution to the anonymity effect. They claim that the cloaking region is a k-anonymity region if its entropy goes beyond the level that is needed for k-anonymity protection.

To reduce the cloaking area and frequency of location updates, a trajectory cloaking algorithm is proposed by [56]. The trajectory cloaking algorithm is a depersonalizing time-series sequences of location samples. They use historical data as footprints to perform k-anonymity cloaking. A footprint is this context is location sample of the user collected periodically. The main objective of the proposed approach is to prevent an adversary from degrading the quality of the current location cloaking by taking advantage of the historical cloaked regions.

The authors in [39] consider the problem of continuous queries from LBS. They point out that trace analysis attacks are from linking historical cloaking regions with user mobility patterns. They design two cloaking algorithms MaxAcc_Cloak and MinComm_Cloak to control the generation of cloaking regions. MaxAccCloak maximises the accuracy of the query results while MinComm_Cloak is designed to reduce communication cost. Finally, they use bulk and progressive query processing modes to return query results in an incremental manner.

The authors in [105] propose a traffic monitoring system design which is based on the concept of virtual trip lines (VTLs). VTLs are geographic markers stored in the user's mobile system. When a probe vehicle passes, VTLs trigger a speed and location update. The authors claim that this approach improves location privacy by restricting the VTL server to follow a set of rules on the trip line placements. The mobile device only generates updates in areas that are regarded as less sensitive. Road categories are used to cloak temporal information and VTL updates are sent probabilistically. The proposed traffic monitoring system enables location privacy by the separation of location and identity-related processing. This privacy by design methodology ensures that a single entity does not have access to both streams of data.

An incremental clique-based cloaking algorithm (IClique-Cloak) is proposed in [49] to defend against location dependent attacks. They show that existing solutions are concerned with the snapshot of user locations hence cannot effectively prevent location dependent attacks. They adopt k-anonymity and cloaking granularity as privacy metrics. The effects of continuous location updates during location cloaking is incorporated by ICliqueCloak. Their solution incrementally maintains the maximum cliques needed for location cloaking in an undirected graph which considers the effects of continuous location updates.

In [106], the authors propose a semantic tree-based algorithm to generate social relationship among users when obscured trajectories are provided. They model obscure regions from the cloaking algorithm as a semantic region tree assign weight values to regions based on their popularity. They use a real trajectory dataset to show that their proposed approach can identify ties successfully.

An enhanced location privacy scheme is proposed in [107]. In this approach, the LBS provider and the user carry out a mutual transformation between the pseudo-location and the real location. The spatial transformation is distributed periodically by a function generator. Although a trusted entity (anonymizer) is deployed, the authors claim that fully trusted entities are not required to enhance location privacy.

4) Dummy-based techniques In Mobile Networks: The main aim of the dummy technique is to protect the actual location of the user by sending multiple false location information together with the actual position of the user to the location server [108]. In this approach, users generate false position data (dummies) that is sent along with the true position of users to the service providers. They present two dummy generating algorithms to protect the user's privacy from the service providers. The first algorithm is the Moving in a Neighbourhood (MN) algorithm and the later is Moving in a Limited Neighbourhood (MLN). The neighbourhood of the current position of the dummy decides the next position of the dummy in the MN approach while in the later approach, the next position of the dummy is also decided in the neighbourhood but limited by the density of the region. In addition to these dummy algorithms, they propose a cost reduction technique to reduce the communication cost.

The monitoring of long-term movement pattern of mobile users can lead to the exposure of their trajectory path. The authors in [109] argue that when a user's trajectory is identified, the location of the user is exposed. To protect the location privacy of the user, they propose two techniques that generate movement patterns that are inconsistent in a long run. The random and rotational pattern schemes are used to generate dummy trajectories which are based on the user's profile. While the random pattern generates dummies randomly with consistent movement pattern, the rotational pattern creates intersection among moving trajectories.

To guarantee location privacy in large regions, the authors in [29] propose a Privacy-Area Aware Dummy-Based location privacy (PAD). This approach offers privacy region guarantees. PAD uses dummy locations that are created intentionally based on a virtual grid or circle. This grid covers the actual location of the user while their area is controlled by the algorithm that created the dummy locations. The PAD approach uses the front-end of the server side which is integrated into the client/server mobile service system. To reduce the communication cost, a compact format is used to organise the query results. This does not only reduce the communication cost but also eases the refinement on the client side. The authors also point out that k-anonymity does not guarantee location privacy since it depends on the density and distribution of mobile users. They suggest that the constraints in the privacy area should be taken into consideration. PAD combines the number of locations in a query sent to the server and the area of the region which covers those locations. PAD offers some level of granularity in location privacy since the dummy generation algorithms are controllable and configurable.

The authors in [110] propose a privacy-aware monitoring framework that deals with location updates and monitors the system's privacy, efficacy and accuracy at the same time. A common interface is used in monitoring the different types of spatial queries such as the kNN and range queries. There is no assumption of the mobility pattern of users. The exact position of the user is encapsulated in a bounding box which makes the query results indistinguishable. This information is updated to the server by the client-location updater.

A user-centric technique (DUMMY-Q) for privacy protection is proposed by [111]. This technique does not require any trusted third-party and simply operates on the user side. DUMMY-Q issues multiple counterfeit queries to confuse the adversary about the user's location. A dummy query generating algorithm called the pool-builder is used to randomly select a set of dummy service attribute values which is the set of locations assumed to be the user's future snapshots of the continuous LBS query. They also address the resource limitations in mobile networks by using a quad-tree based scheme to convert and store query information in binary form to support efficient retrieval and achieve a high compression ratio.

The authors in [112], [113] propose dummy-based privacy-preserving techniques which are based on assumptions that the movement plan of the user is known in advance. In a more realistic and refined approach [31], they propose a dummy-based privacy-preserving technique to anonymize the location of users in real environments. They assume that a mobile user pre-fetches the data map of his neighbourhood and the registration ID of the user is shared with the dummies in the LBS. When a location-based service request is initiated by the user, dummies are generated around the user in the shape of a grid to satisfy the requirement of the anonymous area. The movement of dummies is based on the location of the user and the geographical information which assures the requirement of the anonymous area and decides the next location of the dummies.

The authors in [32] combine spatial cloaking and dummy based techniques to prevent privacy attacks. They make observations based on the trust on a location anonymizer which may cause problem arising from a single point of failure. Due to a system overhead issue, the authors try to minimize the size of the cloaking region which may reveal the user's privacy. They propose an efficient privacy-preserving scheme DUMMY-T which generates a set of realistic dummy locations for each snapshot. They use a path constructing algorithm which guarantees location reachability by taking the maximum distance of the moving mobile users into consideration.

5) Caching Schemes in Mobile Networks: The authors in [114] propose a collaborative privacy scheme to enhance user location privacy in mobile services. In this scheme, mobile users combine with each other to improve their privacy without the need for a TTP. The mobile crowd acts as the TTP in this context. Users minimize their location data by hiding in the crowd. They develop and evaluate a scheme $Mobicrowd$ that enables users to reduce their exposure and hide in the crowd while receiving location-based information. The develop an analytical framework to evaluate the location privacy of the proposed scheme in portable devices. This scheme uses an untrusted LBS server for evaluation which makes it difficult to guarantee the location privacy of the first user. Again the cache hit ratio may be too low considering the fact that it is related to the cache service information.

Similar to the approach proposed in [114], Mobicache is proposed by [115] to provide k-anonymity and collaborative content caching for user location privacy in mobile devices. They focus on cache service information to improve the cache hit ratio. They also introduce a dummy selection algorithm (DSA) to select dummy locations from queried cells randomly for users that send location request to untrusted LBS servers. Furthermore, they harmonise the DSA to make more contributions to the cache hit ratio by choosing locations.

The authors in [33] rigorously explore content caching solutions to improve location privacy. They propose a caching-aware dummy selection algorithm (Ca-DSA) to maximise location privacy. CaDSA combines the dummy selection and caching technique to enhance privacy. They consider the LBS as an untrusted infrastructure with the motive of deducing the location information of the user. Considering a more comprehensive set of factors such as normalised distance and the freshness of data, they propose an enhanced CaDSA to maximise location privacy by determining the optimal set of dummies for the cache hit ratio.

6) Coordinate Transformation in Mobile Networks: In [116], a coordinate transformation approach is used to protect user's privacy. In a coordinate transformation approach, the coordinates of any point in one coordinate system are converted to coordinates of the same point in another coordinate system. One single transformation function is shared by all users. This approach is suitable for a trusted entity or closed group where all members trust each other. The evaluation of each event is limited to the relative position of members. It is not stated whether a user can belong to two or more groups.

Another approach based on coordinate transformation is proposed by [117]. In this approach, simple geometric operations are performed by mobile users before sending them to the location server. To restore the original position, the transformation function is distributed among clients. On the other hand, it is impossible to match the positions of the different users that were obfuscated with different transformations such as performing range queries.

7) Information Access Control in Mobile Networks: In this approach, the locations of the user are sent to the LBS provider. Rule-based policies are used to restrict access to the stored location data by the LBS provider. Three types of location-based queries are supported by this approach; user location queries, enumeration queries and asynchronous queries. The user location query is used for querying a specific user's location identified by their unique ID while the enumeration query queries the list of users at specific locations which are expressed as symbolic or geometric attributes. The asynchronous queries are used for querying the event information such as the entry and exit of users in specific areas. The LBS maintains all the locations of the user in this technique [118], [119].

A location-based access control (LBAC) policy is presented in [120]. LBS is integrated with a generic access control model to enable the location-based credentials of the user requesting for the LBS services to be validated. In this approach, a service level agreement is formulated based on a temporal validity of each access request and the notion of confidence level. The authors claim that LBAC can be applied to a broad variety of policies in LBS. However, they still point out some issues concerning the specification and enforcement of security and privacy constraints on location-based information.

In [121], an access control policy is extended to incorporate the concepts of LBS. They point out that locations can be specified at different levels of granularity. The role of the user is used to determine if the user has access to some resources. They also identify the constraints imposed by some role-based entities on access control such as the dynamic separation of duties and role hierarchy.

Another location-based access control scheme is presented in [54] to protect the location privacy of users. They categorize privacy in LBS into identity, position and path privacy. They introduce the notion of relevance to accommodate peculiar characteristics of privacy-aware LBS. This approach is combined with a location obfuscation technique and it allows users to manage their privacy preferences for specific purposes and applications.

An access control model (GEO-RBAC) designed for the military environment is proposed in [122]. Although GEO-RBAC is developed specifically to address stringent security requirements, the location privacy of the user is also protected with the integration of an access control system that provides trusted location data. GEO-RBAC provides trustworthy location information by ensuring that location privacy is authenticated with a high level of assurance. To ensure secure location identification, several issues including availability, usability and strong location assurance are addressed. However, one major limitation of this approach is that it makes use of near field communication (NFC) communication which is an RFID-based proximity-constrained technology with a very limited broadcast range of about $10m$. We summarize the privacy enhancing schemes for mobile networks proposed in literature in Table III & IV.

B. Cryptographic-based Approaches

1) Private Information Retrieval (PIR): To support private location dependent queries, a novel framework is proposed by [123]. In this approach, privacy is achieved using a cryptographic technique and no trusted third-party is required. They provide privacy guarantees against correlation attacks. They

TABLE III: Summary of Privacy Enhancing Schemes that address Location Privacy in Mobile Services

Category	Strategy	Privacy Metric	Infrastructure Requirements	Location Privacy attack addressed	Issues Addressed
mix-zone	Beresford *et. al.* [62]	Anonymity set	1	Trace analysis and correlation attacks	Makes it difficult for users to be tracked along their trajectories.
mix-zone	Freudiger *et. al.* [52]	Location Tracking	2	Tracking success	Uses a mix-zone deployment strategy and an optimized algorithm to improve location privacy.
mix-zone	MobiMix [44]	Entropy & anonymity set size	1	Transition & timing attacks	Uses a set of mix-zone placement algorithms and constructions to user provide privacy.
Obfuscation	Duckham *et. al.* [95]	Size of obfuscation set	1	N/A	Provides a formal framework that defines obfuscated LBS.
Obfuscation	[96]	Relevance	1	Deobfuscation attacks	Allow users to express their privacy preferences intuitively.
Obfuscation	Patching & delaying [30]	Imprecise location-based range query	2	Inference attacks	Uses imprecise queries to hide the identity of the issuer of the query and enable the evaluation of cloaked information.
Obfuscation	Shokri *et. al.* [57]	Distortion-based metric	N/A	Reconstruction attacks	Estimates the user's location privacy as the level of distortion in his actual trace reconstructed by the reversal of privacy-preserving mechanisms.
Cloaking	IntervalCloak [42]	Anonymity set size	1	Location tracking attacks	The resolution of the location-based information is adjusted to meet specified anonymity constraints within a region.
Cloaking	CliqueCloak [98]	Success rate & relative anonymity level	2	linking attacks	Enables mobile clients to specify their minimum anonymity level and maximum spatial & temporal tolerance level when requesting for LBS services.
Cloaking	P2P Spatial Cloaking [99]	Anonymity set size	2	N/A	A mobile node forms a group of peers before requesting for LBS using single or multi-hop routing.
Cloaking	Casper [48]	Anonymity set size	3	N/A	Casper is a TTP application that enables users to register a specified privacy profile, a location anonymizer is used to blur the exact location of the mobile user into a cloaked area.
Cloaking	iPDA [100]	Entropy	1	Trace analysis attacks	Uses an optimal mobility-aware cloaking technique to prevent trace analysis attacks.
Cloaking	Chow *et. al.* [34]	Continuous Queries & cloaked spatial region area	1	Query sampling and query tracking attack	Uses a spatial cloaking technique to to distinguish between location and query privacy.
Cloaking	Prive [101]	Anonymity set size	2	Inference attacks	Prive is a decentralised system for query anonymization, it guarantees anonymity under any user distribution.
Cloaking	Bettini *et al.* [55]	Anonymity set	1	Inference attacks	Identification of the potential classes of attackers and a formal framework for privacy preservation based on the level of privacy defined by the user.
Cloaking	PRIVACYGRID [102]	Anonymization success rate & Relative anonymity and relative diversity levels	3	Inference attacks	PRIVACYGRID allows users to define their privacy requirements with regards to controlling the processing of queries and hiding their locations.
Cloaking	Hu *et al.* [103]	Anonymity set size	2	Correlation attacks	Cluster-isolated (t-connectivity and $k-clustering$) algorithms are used to define the privacy profiles of users.
Cloaking	NNC & HC [47]	Anonymity set size	2	Inference attacks	Spatial queries are processed using a prohibitive linear computation.

develop algorithms for exact and approximate private NN search and the query execution is optimized by data mining.

A hybrid approach for private location-based query is proposed by [124]. This approach protects the user and the LBS database. They provide a strong privacy by generalizing the user location to coarse-grained cloaked regions and apply a PIR protocol to the queries from the cloaked region. Two cryptographic protocols are used to protect the users against imprudent disclosure of the POI locations. To efficiently support PIR, two algorithms are introduced to provide solutions for exact and approximate NN queries.

The authors in [125], [126] propose major performance improvements to the approaches in [123], [124]. The mobile users use an oblivious transfer method to determine their position within the grid. The user's ID and the associated symmetric key for the block of data are contained in the transfer. A communication efficient PIR is executed is executed by the user in the private grid to retrieve the appropriate block. The symmetrical key obtained in the previous stage is used to decrypt this block. Authors claim that their approach provides protection for the user and the server since the server cannot determine the location of the user. The data of the server is also protected since an attacker can only decrypt the data block from the PIR using the encryption key from the previous stage. Based on a fixed number of nearest neighbours k, [127] look into query privacy using a Rabin crypto-system to prevent mobile users from retrieving more than one data per query. They allow LBS queries based on the location and single POI type attribute only. They assume that mobile users can get location from satellites anonymously and there is an anonymous channel for the mobile user to send queries and services from the LBS provider. They propose three algorithms (query generation, response generation and response retrieval) to provide location privacy for the user against the LBS provider.

Opposed to the approach in [127], the authors in [128] argue that queries with multiple POI type attributes are not supported in this approach. They study the kNN queries where the users query the LBS provider about the k nearest POIs using his current location. They propose a solution built on the Paillier public-key crypto-system which can provide both query and location privacy. This approach allows users to retrieve one type of POIs such as approximate k nearest car parks without revealing the POI that is retrieved to the LBS provider. They use RSA to provide data privacy and support sequential queries. For private location-based queries, they add

TABLE IV: Summary of Privacy Enhancing Schemes that address Location Privacy in Mobile Services CONTD.

Category	Strategy	Privacy Metric	Location Privacy attack addressed	Issues Addressed
Cloaking	Xu *et al*. [104]	Entropy	N/A	Entropy is used to measure the degree of anonymity of a cloaked region with high QoS guaranteed.
Cloaking	Xu *et al*. [56]	Anonymity set size	Trajectory attacks	Ensures anonymity by providing k-anonymity trajectory protection when a user requests for LBS services.
Cloaking	MaxAccu & MinComm_Cloak [39]	Entropy	Trace analysis attacks	The mobility-aware algorithms improve the quality of location cloaking without compromising much on the communication cost.
Cloaking	VTL [105]	Time-to-confusion & distance-to-confusion	Trace analysis attacks	The identity of the user is hidden from external traffic monitoring server using geographic markers and an associated cloaking technique.
Cloaking	ICliqueCloak [49]	Entropy k anonymity & cloaking granularity	Location Dependent attacks	An undirected graph is used to maintain the maximum number of cliques required for location cloaking.
Cloaking	Peng *et. al*.	Success rate	Inference attacks	Uses a function generator in the distribution of spatial transformation between LBS providers and users.
Dummy	MN & MLN [108]	Anonymity set	N/A	Location data is made indistinguishable by generating false location data.
Dummy	You *et al*. [109]	Anonymity set	Location tracking	Dummies are inserted into the user's trajectories based on their privacy profiles.
Dummy	PAD [29]	Anonymity set	Inference attacks	PAD ensured region based privacy and also reduces communication cost.
Dummy	DUMMY-Q [111]	Query success rate	Snapshot attack	A pool builder is used to query dummies based on the query context information.
Dummy	Hara *et. al*. [31]	Anonymity set	Inference attacks	Dummies are generated to anonymize the user location within a range that is predetermined.
Dummy	Dummy-T [32]	Entropy	Inference attacks	Historical data is protected from adversaries with background information using dummy generating algorithm.
Caching Scheme	Mobicrowd [114]	Expected estimation error	Bayesian Inference attacks	Hides a fraction of the LBS queries to enhance the location privacy of the users.
Caching Scheme	MobiCache [115]	Entropy & cache hit ratio	Location information attack	Combines DSA with cache scheme to improve location privacy.
Caching Scheme	CaDSA [33]	Average uncertainty	Inference attacks	Combines k-anonymity, caching and side information to achieve location privacy.

a generic solution with multiple attribute types.

2) Location Proof: A location-based authentication mechanism is proposed in [129]. This mechanism generates location signatures from the reception of raw GPS signals from satellites. Authors claim that the location signatures are very difficult to forge based on the variation of the received signals.

In [130], a system that can securely provide location privacy for mobile devices is presented. They design a protocol that computes the proximity of the mobile device to the location of the network. This protocol is developed by computing the round-trip signal propagation latency and it is able to preserve the identity of the mobile user and the verifier.

A trusted geo-tagging service is proposed for location privacy mobile services [131]. This approach specifically tags the content with trusted locations and the time-stamp metadata. They use content hashes to protect the content from modification by adversaries. The main function of the location proof in this approach is to identify the location of end users while the geo-tagging services add trusted location information to the contents.

In [132], a secure location proof is proposed for mobile users' location privacy. In this approach, mobile users and wireless Access Points (APs) exchange their public keys which have been signed. This is done to create time-stamped location proofs. They assume that wireless infrastructures such as WiFi or cell towers handle location proofs as such mobile users are capable of proving present and past location information.

The authors in [133] propose a location proof architecture with collision resiliency and location privacy protection. The proposed system requires three different trusted entities to provide privacy and security: a CDA (Cheating Detection Authority), a TTPL (Trusted Third-Party for managing Location information) and TTPU (Trusted Third-Party for managing User information). Each of the trusted entities has access to only one attribute, i.e either the either the user's location or its identity. They introduce a collision detection scheme (Veriplace) which works only when location proofs are requested by user frequently.

To provide location privacy for mobile services, the authors in [134] propose a scheme which relies on wireless APs for location proofs and witness endorsement from mobile peers with enabled Bluetooth services. This is done to prevent the forgery of location proofs by adversaries without colliding with other users. In this approach, the necessity of the multiple trusted parties is eliminated with two privacy-preserving techniques (hash chains and bloom filters) for protecting the integrity of the location proofs chronologically.

In [135], an alibi privacy-preserving system is proposed. This approach relies on the proximity of mobile users to create location proofs (alibi) for each other. The identity of the user is concealed during the creation of the location proof and revealed only when the alibi is presented to a judge. They develop a cryptographic commitment scheme to provide security and privacy of the alibi system by creating owner statements from the owner features in the verification section of the alibi privacy-preserving scheme.

In [35], co-located Bluetooth devices generate location proof and update it to a location server. Pseudonyms changed periodically to protect the source location information from each other. To protect the location of the users, the private information is distributed to the three entities involved in the LBS: the verifier, the location proof server and the CA. They claim that the user location privacy is guaranteed by every party. Users can also evaluate their real-time privacy levels from the user-centric location privacy model and decide when to accept location proof request based on their location privacy levels.

A Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme is proposed by [136]. This scheme is based on a distributed architecture where ad-hoc mobile users generate location proofs for each other. The authors claim that STAMP ensures the non-transferability and integrity of location proofs and users are in control of the location granularity of their spatial-temporal provenance proofs. They integrate the distant bounding protocol into the proposed scheme to prevent users from collecting location proof on behalf of another user. A trust model based on entropy is developed to prevent generation of fake proofs and prover-witness collusions.

3) Key Management: In [137], the authors use a simple public-key cryptography to control access to location information. This proxy-based approach uses a Location Information Preference Authority (LIPA) as a trusted party to examine the constraints chosen by the user and make decisions on the distribution of location information. They use an online location gatherer to construct tokens for the location information. This token contains the location information and constraints encrypted with the public key of LIPA. The location gatherer digitally signs the information to provide access control. The LBS receives a token when requesting for access, this is followed by the signature verification and establishment of the location information subjects. The token is then submitted to LIPA to verify that the LBS requesting for the service has access to the location information requested.

The authors in [138] extend the logical key hierarchy (LKH) [139] scheme where the key distribution centre maintains a tree of keys to support encryption of location information at multiple levels. They present a framework that enables users to share their location information with different levels of user control which is integrated into LBS. They present some techniques to support hierarchical dissemination of location information by encrypting the location information with different keys and distributing them to the appropriate members while maintaining location privacy.

In [140], authors propose a scalable key management algorithm for LBS. First, they develop an efficient, secure and scalable key management protocol STauth for LBS. STauth reduces the number of keys that need to be distributed. They exploit the 3-dimensional spatial-temporal authorization model to construct authorization keys using hierarchical key graphs.

We summarize the cryptographic approaches proposed in literature in Table V.

VI. Drawbacks of Proposed Schemes

A. Location Privacy Schemes

In this section, we summarize the weaknesses of location privacy approaches in vehicular and mobile networks. mix-zones rely on a set of predefined spatial region for pseudonym exchange. In low density areas, these approaches suffer from low privacy protection which implies that location privacy cannot be guaranteed. In [62], the proposed approach requires careful control of the number of users within the mix-zone, which is difficult to achieve in practice. In a scenario where an adversary monitors more than 50% of the road intersections, location privacy is not guaranteed [59]. The mix-zone approach in [64], [65] provides vehicles with pseudonyms which are changed at social spots. The assumption that a social spot is continuously available to change pseudonyms is not always the case. The assumption is not applicable in a highway where there is a low density of vehicles at road intersections or assumed social spots. The unlinkability of users' queries is limited when the size of the mix-zone is kept small. The success rate of an adversary is still relatively high even if the mix-zones are optimally placed [52]. The authors in [66] argue that if vehicles change pseudonym in inappropriate events, the location privacy of these vehicles are not protected by mix-zones concept.

In [59], the silent period contradicts the main objective of vehicular communications. Refraining from broadcasting safety messages during silent periods can result in a negative QoE for LBS users. Random silence periods are still susceptible to traffic analysis attacks. Adversaries use prior state of targeted vehicles to link vehicles during silent periods. In silent periods, there is a possibility of tracking vehicles by deducing their spatial and temporal correlation as a result of the maximum silent period being constrained [66]. In [141], the authors point out that even when vehicles change their pseudonyms simultaneously after the silent period, the complete trajectory can be reconstructed.

Cacheclock [72] relies on a centralised anonymity server. If this third-party server is compromised, the actual user trajectory can easily be identified when there are no other users in the predicted path. In MobiCache [115], an adversary can use side information to deduce location information of a targeted user. Cloaking approaches provide effective location privacy when the LBS server is not queried so often. A user can be exposed if a server is queried frequently over time. Assuming one of the k users in the spatial area is inconsistent throughout the set of cloaked requests, the location privacy of that user is not guaranteed. In a centralized location cloaking approach such as [123], the major drawback is the anonymizer

TABLE V: Summary of Cryptographic Schemes that address Location Privacy in Mobile Networks

Category	**Strategy**	**Privacy Metric**	**Location Privacy attack addressed**	**Issues Addressed**
PIR	Nearest neighbour *et al.* [123]	K-degree of anonymity	Correlation attacks	Nearest neighbour approximation using Hilbert ordering and cloaking region.
PIR	Nearest neighbour [124]	Communication cost& overhead	User identity disclosure	User location is generalised into coarse grained regions and provides protection for both the users and the database. & vehicle density.
PIR	Oblivious transfer & PIR [126], [125]	Performance based on communication efficiency	User identity disclosure	Privacy-preserving location data query and acquisition
PIR	k nearest neighbours [63]	Computation complexity & communication overhead	Location and data privacy	LBS allows user retrieve location information based on user request.
PIR	k nearest neighbours [128]	Computation complexity & communication overhead	Query and location privacy	Location information retrieval based on user-specific request.
Location proof	Variation of received signals *et. al.* [129]		Protection against location forging attacks	Location data are generated based on varying GPS data from aerial satellites.
Location proof	Brent and Edward [130]	Formal proof	Integrity and privacy protection	Location proof is based on triangulation by third-party location verifiers.
Location proof	Trust-based location content provisioning [131]	System is based on a PKI infrastructure	Privacy protection and protection against location forging and modification.	Contents with trusted location information are geo-tagged for later retrieval
Location proof	Saroiu & Wolman [132]	NA	Collusion attacks	Addresses collusion attacks using hard-to-forge personal information.
Location proof	VeriPlace [133]	Protocol evaluation through simulations	Protection against location cheating, and defence against wormhole attacks	Design of an architecture enables users to collect proofs for being at a location.
Location proof	Hasan and Burns [134]	Percentage of revealed location information	Protection against tampering and collusion attacks by malicious users	Use of bloom filters and hash chain based systems for location provenance.
Location proof	Alibi system [135]	Validated on an Android platform	Sybil-alibi attack	Addresses a privacy-preserving alibi mechanism that conceals user identity during alibi creation.
Location proof	APPLAUS [35]	Various performance parameters (e.g. overhead ratio)	Collusion resistant location privacy	Use of periodically(statistically) changing pseudonyms for privacy protection.
Location proof	STAMP [136]	Various performance metrics (e.g. entropy and collusion-detection accuracy)	Collusion attacks	Ad-hoc mobile users generate location proofs for each other in a distributed setting.
Key management	Gajparia *et al.* [137]	Re-keying efficiency (e.g. re-keying overhead)	NA	Hierarchical encryption of location information based on group membership.
Key management	Sun *et al.* [138]	Message delivery and key management overhead	NA	Based on providing keys to group members that allow them to decrypt location information for their use.
Key management	STauth [140]	Throughput & response time	Denial of Service attacks	Exploits spatio-temporal authorisation model to construct secure hierarchical key graphs

which acts as a proxy between users and the LBS server per query. This process creates a single point of attack and failure. In Spatial cloaking approach [34], the anonymity server may generate very large cloaked area resulting in performance degradation. This is as a result of the mobility of users in the k-region who are in the same cloaked area but move in different directions. Location cloaking has been very effective against adversaries with background knowledge. However, constructing cloaking regions and receiving responses from the LBS server will lead to network degradation. It becomes a bottleneck since all the submitted queries go through the server. In [108] and [95], the location privacy threats are even more significant. This is because the LBS server knows the precise location of the user which is given in the anonymity set. The exact location of the user can be revealed by monitoring a sequence of queries. In location cloaking, when a large anonymity set is formed, it increases the communication cost between users. Again, one general assumption that is made in this approach is that all users registered for this service are trusted in order to form the cloaked region.

In dummy-based approaches, realistic locations are not considered when generating the dummies or trajectories. Based on the location where the dummy is generated, the LBS provider can easily filter out the location. Dummy queries confuse adversaries that target a user location, implementing an optimal solution for generating dummy queries remains an open problem. In [33], the caching scheme is combined with a dummy selection algorithm to provide location privacy. This approach requires the cooperation of LBS participants or users.

B. Cryptographic Approaches

The authentication schemes [79], [87], [81] that provide location privacy pay more attention to optimising the communication cost. These schemes focus on the authentication of messages in a timely manner. If invalid messages exist, an additional overhead may be introduced as a result of the delay in verification. In TACKs [25], vehicles are authenticated by the registration authority with a short life time. This region-based certificates issued by the registration authority have a short life time and only valid within the region covered by the registration authority. IEEE standards for Wireless Access in Vehicular Environments (WAVE) [142] requires vehicles to periodically broadcast their location, direction and speed at every $100-300sec$. privacy-preserving authentication schemes such as TACKs [25] are not suitable for safety applications in VANETs. This scheme requires the registration authority to delay for some time before sending a certificate to a vehicle requesting for service updates [143]. In RAISE [87], vehicles have to store a large number private and public keys as well as their corresponding certificates. In areas with high density of vehicles, it will be difficult for the RSU to transmit many certificates in addition to other services it provides. The PIR techniques guarantee perfect privacy and support for partial queries. However, their major weakness is the computational complexity and high computational overhead it incurs [123]. Another drawback in PIRs is their reliance on hardware with a limited secure coprocessor and computational power. One advantage of the PIR scheme is that it does not require a TTP server. It uses a cryptographic technique to provide location privacy. The question whether LBS queries can be performed over encrypted data still raises issues. Many approaches have been proposed for security and privacy in vehicular networks. However, there are still several challenges that need to be addressed before the realization of connected cars and autonomous driving. One major problem identified is how to keep a balance between security and privacy. CRL is used basically for the revocation of malicious users. Although caching techniques have been combined with hashing techniques to improve the availability of revocation services, the privacy information of the user can be compromised during the process of checking the certificate status. The privacy-preserving authentication schemes can expose the user to adversaries. Authentication may expose the precise location of a user in real-time to TTP to ensure that it intervenes when an issue arises. Drivers may not want to be monitored by TTPs since it violates their privacy. However, this will be different for connected and autonomous cars as data will be recorded using event data recorders. As vehicles are expected to report their routes, efficient data aggregation techniques must be implemented without leaking any private information of the vehicles.

VII. Open Issues

In the previous sections, we reviewed several approaches to enhance location privacy. We also identified several challenges. One major challenge regarding the protection of location data of users is the trade off between security and privacy. The complete realisation of smart transportation which includes connected and connected autonomous vehicles could lead to critical changes in driving experience by the integration of smartness into ITS applications [144]. This raises a huge privacy concern because of the periodic beaconing information about the network. We discuss some of these challenges below.

- A major issue in location privacy techniques is the measure of the effectiveness of location privacy. Different privacy metrics have been discussed in Section III which are used in the context of mobile and vehicular networks. Privacy metrics such as entropy can be difficult to compute and this raises a question about its suitability for practical applications. Although so many metrics have been proposed for location privacy, most of them have either been validated with limited simulations or just proposed mathematical theories. There are no standard metrics, validation tool or methodology that have been adopted to validate the level of privacy provided by proposed schemes. As pointed out in [22], there should be a comprehensive study that highlights the suitability of these metrics to specific scenarios.
- Another key area is the evaluation of the impact of these privacy enhancing technologies on safety applications. For example, in disaster stricken areas such as the recently witnessed Hurricane Harvey [145] where over half a million vehicles were destroyed as a result of the flooding. Safety application should be able to make real-time decisions such as warning the users of upcoming dangers. For vehicular networks, these messages are always transmitted using beacons. If a privacy enhancing scheme such as silent period discussed in section IV is used, this interruption could result in a delay in the broadcast of real-time safety information.
- Very little work has been done on pseudonym revocation. There are questions regarding the issuance and management of pseudonyms. For example, if a user is compromised and its pseudonym is revoked, it can still use other pseudonyms to provide privacy. If all the certificates are revoked, it is not clear how is this process controlled by the authorities taking into consideration the impacts of the revocation of a user's identity.
- Location privacy enhancing schemes that are based on k-anonymization, cloaking and obfuscation usually introduce a trade-off between privacy and accuracy and most services may require real-time location information especially in modern tracking applications. In mobile networks, there are significant numbers of TTPs which are assumed as trusted entities and these TTPs process location updates. In situation where an adversary can access the data from the TTP, the user's location data is compromised.
- The collection of location data is necessary for navigational purposes especially for smart transportation. However, there is a growing concern about the collection of sensitive location data and the risk of harm. For example, revealing an individual's historical location and destination information which may reveal sensitive

information about the individual based on real time traffic data and points of interest along the individual's planned route. Location privacy can be violated by combining the location information with personal information about the user for marketing purposes. Based on inference drawn from the location data of a vehicle, data privacy may be violated through customized advertising.

- There is need for transparency and control over the use and sharing of location data. It is not very clear how this data will be used, shared and who has the right to control data. Location data is recognised as one of the identifiers of personal data in Article 4(1) of the GDPR [146]. There is still an uncertainty about sensitive location data. It is not clear how the consent granularity proposed in Article (9) of the GDPR [147] will deal with privacy violations.
- Although software in vehicles is not a new development, there were no connectivities between vehicles. An average vehicle today has up to 100 Electronic Control Units [ECUs] for monitoring and controlling of the electronic system. The authors in [148] identified several malware in the form of executable codes in connected vehicles as a result of complex interdependencies. This means that the software in a vehicle has some substantial number of bugs and these may be more acute with additional software.

VIII. Conclusion

In this article, we presented a comprehensive review of location privacy in LBS. We described and discussed security and location privacy requirements in vehicular and mobile networks. We introduced a taxonomy along the dimensions of privacy metrics, adversary models and compared many recent publications. We categorised the current research into two groups: privacy enhancing schemes and cryptographic approaches for location privacy in vehicular and mobile networks We further identified the challenges and open issues in location privacy for vehicular and mobile networks. We identified and discussed four categories of location privacy enhancing schemes in vehicular networks. We also looked at two categories of privacy-preserving authentication schemes that address location privacy in vehicular networks. In mobile networks, we described five categories of privacy enhancing schemes and three cryptographic approaches that address location privacy. To the best of our knowledge, this survey provides a comprehensive overview of privacy enhancing schemes and cryptographic solutions that address location privacy.

References

[1] M. Gerla, E. K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 241–246, March 2014.

[2] M. Raya, P. Papadimitratos, and J. p. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications*, vol. 13, pp. 8–15, October 2006.

[3] H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, pp. 164–171, June 2008.

[4] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, pp. 1832–1843, Dec 2017.

[5] Y. Cao, S. Yang, G. Min, X. Zhang, H. Song, O. Kaiwartya, and N. Aslam, "A cost-efficient communication framework for battery-switch-based electric vehicle charging," *IEEE Communications Magazine*, vol. 55, pp. 162–169, May 2017.

[6] E. C. Eze, S. Zhang, and E. Liu, "Vehicular ad hoc networks (vanets): Current state, challenges, potentials and way forward," in *2014 20th International Conference on Automation and Computing*, pp. 176–181, Sept 2014.

[7] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of internet of vehicles," *China Communications*, vol. 11, pp. 1–15, Oct 2014.

[8] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu, and W. Zhao, "A real-time en-route route guidance decision scheme for transportation-based cyberphysical systems," *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 2551–2566, March 2017.

[9] *Global Intelligent Transport System (ITS) Market 2017-2021, Intelligent Transport System meets IoT to Promote Smart, Scalable and Safe Urban Mobility, September 2017.*

[10] Y. Cao, Y. Miao, G. Min, T. Wang, Z. Zhao, and H. Song, "Vehicular-publish/subscribe (v-p/s) communication enabled on-the-move ev charging management," *IEEE Communications Magazine*, vol. 54, pp. 84–92, December 2016.

[11] J.-H. Song, V. W. Wong, and V. C. Leung, "Secure Location Verification for Vehicular Ad-hoc Networks," in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*, pp. 1–5, IEEE, 2008.

[12] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[13] S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, and A. Lei, "A lightweight authentication and privacy-preserving scheme for vanets using tesla and bloom filters," *ICT Express*, 2017.

[14] Y. Leng and L. Zhao, "Novel design of intelligent internet-of-vehicles management system based on cloud-computing and internet-of-things," in *Proceedings of 2011 International Conference on Electronic Mechanical Engineering and Information Technology*, vol. 6, pp. 3190–3193, Aug 2011.

[15] E. Qin, Y. Long, C. Zhang, and L. Huang, *Cloud Computing and the Internet of Things: Technology Innovation in Automobile Service*, pp. 173–180. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.

[16] Y. Zhang, B. Chen, and X. Lu, *Intelligent Monitoring System on Refrigerator Trucks Based on the Internet of Things*, pp. 201–206. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

[17] W. He, G. Yan, and L. D. Xu, "Developing vehicular data cloud services in the iot environment," *IEEE Transactions on Industrial Informatics*, vol. 10, pp. 1587–1595, May 2014.

[18] L. Chen, S. Thombre, K. JÃď'rvinen, E. S. Lohan, A. AlÃľ'n-Savikko, H. LeppÃď'koski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, "Robustness, security and privacy in location-based services for future iot: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[19] R. H. Weber, "Internet of things âĂŞ new security and privacy challenges," *Journal of Computer Law and Security Review*, 2010.

[20] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, pp. 1125–1142, Oct 2017.

[21] M. Riley, K. Akkaya, and K. Fong, "A survey of authentication schemes for vehicular ad hoc networks," *Security and Communication Networks*, vol. 4, no. 10, pp. 1137–1152, 2011.

[22] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 17, pp. 228–255, Firstquarter 2015.

[23] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, VANET '04, (New York, NY, USA), pp. 29–37, ACM, 2004.

[24] J. R. Douceur, "The sybil attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, IPTPS '01, (London, UK, UK), pp. 251–260, Springer-Verlag, 2002.

[25] A. Studer, E. Shi, F. Bai, and A. Perrig, "Tacking together efficient authentication, revocation, and privacy in vanets," in *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, SECON'09, (Piscataway, NJ, USA), pp. 484–492, IEEE Press, 2009.

[26] I. Wagner and D. EckhoïňĂ, "Technical privacy metrics: a systematic survey," *arXiv, 1512.00327, December 2015. (arXiv: 1512.00327)*, 2015.

[27] M. Humbert, M. H. Manshaei, J. Freudiger, and J.-P. Hubaux, *Tracking Games in Mobile Networks*, pp. 38–57. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[28] M. Gerlach, “Assessing and improving privacy in vanets,” in *Proc. 4th Workshop ESCAR, Nov. 2006, pp. 1âĂŞ9*, 2006.

[29] H. Lu, C. S. Jensen, and M. L. Yiu, “Pad: Privacy-area aware, dummy-based location privacy in mobile services,” in *Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access*, MobiDE ’08, (New York, NY, USA), pp. 16–23, ACM, 2008.

[30] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, *Preserving User Location Privacy in Mobile Data Management Infrastructures*, pp. 393–412. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.

[31] T. Hara, A. Suzuki, M. Iwata, Y. Arase, and X. Xie, “Dummy-based user location anonymization under real-world constraints,” *IEEE Access*, vol. 4, pp. 673–687, 2016.

[32] B. Niu, S. Gao, F. Li, H. Li, and Z. Lu, “Protection of location privacy in continuous lbss against adversaries with background information,” in *2016 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1–6, Feb 2016.

[33] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, “Enhancing privacy through caching in location-based services,” in *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 1017–1025, April 2015.

[34] C.-Y. Chow and M. F. Mokbel, “Enabling private continuous queries for revealed user locations,” in *Proceedings of the 10th International Conference on Advances in Spatial and Temporal Databases*, SSTD’07, (Berlin, Heidelberg), pp. 258–273, Springer-Verlag, 2007.

[35] Z. Zhu and G. Cao, “Toward privacy preserving and collusion resistance in a location proof updating system,” *IEEE Transactions on Mobile Computing*, vol. 12, pp. 51–64, Jan 2013.

[36] A. Solanas, J. Domingo-Ferrer, and A. MartÂt’Äśnez-BallestÂt’e, “Location privacy in location-based services: Beyond ttp-based schemes,” *In: International workshop on privacy in location-based applications (PiLBA âĂŹ08), Malaga, Spain*, 2008.

[37] D. Chaum, “The dining cryptographers problem: Unconditional sender and recipient untraceability,” *Journal of Cryptology*, vol. 1, pp. 65–75, Jan 1988.

[38] C. Diaz, C. Troncoso, and G. Danezis, “Does additional information always reduce anonymity?,” in *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society*, WPES ’07, (New York, NY, USA), pp. 72–75, ACM, 2007.

[39] J. Xu, X. Tang, H. Hu, and J. Du, “Privacy-conscious location-based queries in mobile environments,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, pp. 313–326, Mar. 2010.

[40] A. Serjantov and G. Danezis, *Towards an Information Theoretic Metric for Anonymity*, pp. 41–53. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003.

[41] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, “Preserving privacy in gps traces via uncertainty-aware path cloaking,” in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS ’07, (New York, NY, USA), pp. 161–171, ACM, 2007.

[42] M. Gruteser and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking,” in *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, MobiSys ’03, (New York, NY, USA), pp. 31–42, ACM, 2003.

[43] B. Palanisamy and L. Liu, “Mobimix: Protecting location privacy with mix-zones over road networks,” in *2011 IEEE 27th International Conference on Data Engineering*, pp. 494–505, April 2011.

[44] B. Palanisamy and L. Liu, “Attack-resilient mix-zones over road networks: Architecture and algorithms,” *IEEE Transactions on Mobile Computing*, vol. 14, pp. 495–508, March 2015.

[45] L. Sweeney, “K-anonymity: A model for protecting privacy,” *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10, pp. 557–570, Oct. 2002.

[46] B. Gedik and L. Liu, “Location privacy in mobile systems: A personalized anonymization model,” in *25th IEEE International Conference on Distributed Computing Systems (ICDCS’05)*, pp. 620–629, June 2005.

[47] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing location-based identity inference in anonymous spatial queries,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, pp. 1719–1733, Dec 2007.

[48] W. G. A. Mohamed F. Mokbel, Chi-Yin Chow, “The new casper: Query processing for location services without compromising privacy.,” No. 1-59593-385-9/06/09., (Seoul, Korea), Department of Computer Science and Engineering, University of Minnesota, Minneapolis, MN, ACM, September 2006.

[49] X. Pan, J. Xu, and X. Meng, “Protecting location privacy against location-dependent attacks in mobile services,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 24, pp. 1506–1519, Aug 2012.

[50] R. Shokri, G. Theodorakopoulos, J. Y. L. Boudec, and J. P. Hubaux, “Quantifying location privacy,” in *2011 IEEE Symposium on Security and Privacy*, pp. 247–262, May 2011.

[51] J. Freudiger, M. H. Manshaei, J. P. Hubaux, and D. C. Parkes, “Non-cooperative location privacy,” *IEEE Transactions on Dependable and Secure Computing*, vol. 10, pp. 84–98, March 2013.

[52] J. Freudiger, R. Shokri, and J.-P. Hubaux, “On the optimal placement of mix zones,” in *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies*, PETS ’09, (Berlin, Heidelberg), pp. 216–234, Springer-Verlag, 2009.

[53] C. A. Ardagna, M. Cremonini, S. D. C. di Vimercati, and P. Samarati, “An obfuscation-based approach for protecting location privacy,” *IEEE Transactions on Dependable and Secure Computing*, vol. 8, pp. 13–27, Jan 2011.

[54] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. d. Vimercati, and P. Samarati, “Managing privacy in lbac systems,” in *Advanced Information Networking and Applications Workshops, 2007, AINAW ’07. 21st International Conference on*, vol. 2, pp. 7–12, May 2007.

[55] C. Bettini, S. Mascetti, X. S. Wang, and S. Jajodia, “Anonymity in location-based services: Towards a general framework,” in *2007 International Conference on Mobile Data Management*, pp. 69–76, May 2007.

[56] T. Xu and Y. Cai, “Exploring historical location data for anonymity preservation in location-based services,” in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, April 2008.

[57] R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, “A distortion-based metric for location privacy,” in *Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society*, WPES ’09, (New York, NY, USA), pp. 21–30, ACM, 2009.

[58] J. Krumm, “Inference attacks on location tracks,” in *Proceedings of the 5th International Conference on Pervasive Computing*, PERVASIVE’07, (Berlin, Heidelberg), pp. 127–143, Springer-Verlag, 2007.

[59] L. Buttyán, T. Holczer, and I. Vajda, “On the effectiveness of changing pseudonyms to provide location privacy in vanets,” in *Proceedings of the 4th European Conference on Security and Privacy in Ad-hoc and Sensor Networks*, ESAS’07, (Berlin, Heidelberg), pp. 129–141, Springer-Verlag, 2007.

[60] J. Freudiger, M. Raya, M. F. P. Papadimitratos, and J.-P. Hubaux, “Mix-zones for location privacy in vehicular networks,” *WiN-ITS Vancover, British Columbia, Canada*, 2007.

[61] M. Gerlach and F. Guttler, “Privacy in vanets using changing pseudonyms - ideal and real,” in *2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring*, pp. 2521–2525, April 2007.

[62] A. R. Beresford and F. Stajano, “Location privacy in pervasive computing,” *IEEE Pervasive Computing*, vol. 2, pp. 46–55, Jan 2003.

[63] X. Lin, R. Lu, X. Liang, and X. Shen, “Stap: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in vanets,” in *2011 Proceedings IEEE INFOCOM*, pp. 2147–2155, April 2011.

[64] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, “Anonymity analysis on social spot based pseudonym changing for location privacy in vanets,” in *2011 IEEE International Conference on Communications (ICC)*, pp. 1–5, June 2011.

[65] 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, pp. 86–96, Jan 2012.

[66] 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, pp. 93–105, Jan 2016.

[67] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, “Swing & swap: User-centric approaches towards maximizing location privacy,” in *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*, WPES ’06, (New York, NY, USA), pp. 19–28, ACM, 2006.

[68] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “Amoeba: Robust location privacy scheme for vanet,” *IEEE Journal on Selected Areas in Communications*, vol. 25, pp. 1569–1589, Oct 2007.

[69] S. Eichler, “Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility,” in *2007 IEEE Intelligent Vehicles Symposium*, pp. 541–546, June 2007.

[70] L. ButtyÃąn, T. Holczer, A. Weimerskirch, and W. Whyte, “Slow: A practical pseudonym changing scheme for location privacy in vanets,,” *Proc. 1st IEEE VNC, Oct. 2009, pp. 1âĂŞ8*, 2009.

[71] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "Caravan: Providing location privacy for vanet," *International Journal of Ad Hoc and Ubiquitous Computing 2012; 10(4): 219âĂŞ229.*, 2012.

[72] J. Meyerowitz and R. Roy Choudhury, "Hiding stars with fireworks: Location privacy through camouflage," in *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, MobiCom '09, (New York, NY, USA), pp. 345–356, ACM, 2009.

[73] S. Amini, J. Lindqvist, J. Hong, J. Lin, E. Toch, and N. Sadeh, "Caché: Caching location-enhanced content to improve user privacy," in *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, MobiSys '11, (New York, NY, USA), pp. 197–210, ACM, 2011.

[74] B. Liu, W. Zhou, T. Zhu, L. Gao, T. H. Luan, and H. Zhou, "Silence is golden: Enhancing privacy of location-based services by content broadcasting and active caching in wireless vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 9942–9953, Dec 2016.

[75] J. Lim, H. Yu, K. Kim, M. Kim, and S. B. Lee, "Preserving location privacy of connected vehicles with highly accurate location updates," *IEEE Communications Letters*, vol. 21, pp. 540–543, March 2017.

[76] A. Wasef and X. Shen, "Ppgcv: Privacy preserving group communications protocol for vehicular ad hoc networks," in *2008 IEEE International Conference on Communications*, pp. 1458–1463, May 2008.

[77] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," 2002.

[78] X. Lin, X. Sun, X. Wang, C. Zhang, P. H. Ho, and X. Shen, "Tsvc: timed efficient and secure vehicular communications with privacy preserving," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 4987–4998, December 2008.

[79] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 57, pp. 3357–3368, Nov 2008.

[80] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, pp. 22–28, October 2010.

[81] A. Wasef and X. S. Shen, "Rep: Location privacy for vanets using random encryption periods," *Mob. Netw. Appl.*, vol. 15, pp. 172–185, Feb. 2010.

[82] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, pp. 127–139, March 2012.

[83] X. Lin, X. Sun, P. H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, pp. 3442–3456, Nov 2007.

[84] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*, VANET '07, (New York, NY, USA), pp. 19–28, ACM, 2007.

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

[86] D. B. abd H. Shacham, "Group signatures with verifier-local revocation," *In proceedings of the 11'th ACM conference on Computer and Communications Security (CCS), pp. 168-177, 2004*, 2004.

[87] C. Zhang, R. Lu, P. H. Ho, and A. Chen, "A location privacy preserving authentication scheme in vehicular networks," in *2008 IEEE Wireless Communications and Networking Conference*, pp. 2543–2548, March 2008.

[88] S. Guo, D. Zeng, and Y. Xiang, "Chameleon hashing for secure and privacy-preserving vehicular communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, pp. 2794–2803, Nov 2014.

[89] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic Curves in Cryptography*. New York, NY, USA: Cambridge University Press, 1999.

[90] H. Lu, J. Li, and M. Guizani, "A novel id-based authentication framework with adaptive privacy preservation for vanets," in *2012 Computing, Communications and Applications Conference*, pp. 345–350, Jan 2012.

[91] J. Li, H. Lu, and M. Guizani, "Acpn: A novel authentication framework with conditional privacy-preservation and non-repudiation for vanets," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, pp. 938–948, April 2015.

[92] M. C. Chuang and J. F. Lee, "Team: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Systems Journal*, vol. 8, pp. 749–758, Sept 2014.

[93] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, PERCOMW '04, (Washington, DC, USA), pp. 127–, IEEE Computer Society, 2004.

[94] J. Krumm, "A survey of computational location privacy," *Personal Ubiquitous Comput.*, vol. 13, pp. 391–399, Aug. 2009.

[95] M. Duckham and L. Kulik, *A Formal Model of Obfuscation and Negotiation for Location Privacy*, pp. 152–170. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.

[96] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, "Location privacy protection through obfuscation-based techniques," in *Proceedings of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, (Berlin, Heidelberg), pp. 47–60, Springer-Verlag, 2007.

[97] R. H. Hwang, Y. L. Hsueh, and H. W. Chung, "A novel time-obfuscated algorithm for trajectory privacy protection," *IEEE Transactions on Services Computing*, vol. 7, pp. 126–139, April 2014.

[98] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, pp. 1–18, Jan 2008.

[99] C.-Y. Chow, M. F. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based service," in *Proceedings of the 14th Annual ACM International Symposium on Advances in Geographic Information Systems*, GIS '06, (New York, NY, USA), pp. 171–178, ACM, 2006.

[100] J. Du, J. Xu, X. Tang, and H. Hu, "ipda: Supporting privacy-preserving location-based mobile services," in *2007 International Conference on Mobile Data Management*, pp. 212–214, May 2007.

[101] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Prive: Anonymous location-based queries in distributed mobile systems," in *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, (New York, NY, USA), pp. 371–380, ACM, 2007.

[102] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacygrid," in *Proceedings of the 17th International Conference on World Wide Web*, WWW '08, (New York, NY, USA), pp. 237–246, ACM, 2008.

[103] H. Hu and J. Xu, "Non-exposure location anonymity," in *2009 IEEE 25th International Conference on Data Engineering*, pp. 1120–1131, March 2009.

[104] T. Xu and Y. Cai, "Location anonymity in continuous location-based services," in *Proceedings of the 15th Annual ACM International Symposium on Advances in Geographic Information Systems*, GIS '07, (New York, NY, USA), pp. 39:1–39:8, ACM, 2007.

[105] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A. M. Bayen, M. Annavaram, and Q. Jacobson, "Virtual trip lines for distributed privacy-preserving traffic monitoring," in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, MobiSys '08, (New York, NY, USA), pp. 15–28, ACM, 2008.

[106] Y. Tian, W. Wang, J. Wu, Q. Kou, Z. Song, and E. Ngai, "Privacy preserving social tie discovery based on cloaked human trajectories," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, 2016.

[107] T. Peng, Q. Liu, and G. Wang, "Enhanced location privacy preserving scheme in location-based services," *IEEE Systems Journal*, vol. 11, pp. 219–230, March 2017.

[108] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *International Conference on Pervasive Services*, (Japan), Graduate School of Information Science and Technology, Osaka University NTT Communication Science Laboratories, NTT Corporation, 2005.

[109] T. H. You, W. C. Peng, and W. C. Lee, "Protecting moving trajectories with dummies," in *2007 International Conference on Mobile Data Management*, pp. 278–282, May 2007.

[110] H. Hu, J. Xu, and D. L. Lee, "Pam: An efficient and privacy-aware monitoring framework for continuously moving objects," *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, pp. 404–419, March 2010.

[111] A. Pingley, N. Zhang, X. Fu, H. A. Choi, S. Subramaniam, and W. Zhao, "Protection of query privacy for continuous location based services," in *2011 Proceedings IEEE INFOCOM*, pp. 1710–1718, April 2011.

[112] R. Kato, M. Iwata, T. Hara, Y. Arase, X. Xie, and S. Nishio, *User Location Anonymization Method for Wide Distribution of Dummies*, pp. 259–273. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.

[113] R. Kato, M. Iwata, T. Hara, A. Suzuki, X. Xie, Y. Arase, and S. Nishio, “A dummy-based anonymization method based on user trajectory with pauses,” in *Proceedings of the 20th International Conference on Advances in Geographic Information Systems*, SIGSPATIAL ’12, (New York, NY, USA), pp. 249–258, ACM, 2012.

[114] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J. P. Hubaux, “Hiding in the mobile crowd: Locationprivacy through collaboration,” *IEEE Transactions on Dependable and Secure Computing*, vol. 11, pp. 266–279, May 2014.

[115] X. Zhu, H. Chi, B. Niu, W. Zhang, Z. Li, and H. Li, “Mobicache: When k-anonymity meets cache,” in *2013 IEEE Global Communications Conference (GLOBECOM)*, pp. 820–825, Dec 2013.

[116] G. Treu, A. Küpper, and P. Ruppel, “Anonymization in proactive location based community services,” in *Advances in Pervasive Computing. Adjunct Proceedings of the Third Intl. Conference on Pervasive Computing*, (Munich, Germany), Österreichische Computer Gesellschaft, May 2005.

[117] A. Gutscher, “Coordinate transformation - a solution for the privacy problem of location based services?,” in *Proceedings 20th IEEE International Parallel Distributed Processing Symposium*, pp. 7 pp.– , April 2006.

[118] M. Youssef, V. Atluri, and N. R. Adam, “Preserving mobile customer privacy: An access control system for moving objects and customer profiles,” 2005.

[119] G. Myles, A. Friday, and N. Davies, “Preserving privacy in environments with location-based applications,” *IEEE Pervasive Computing*, vol. 2, pp. 56–64, Jan. 2003.

[120] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, “Supporting location-based conditions in access control policies,” in *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, ASIACCS ’06, (New York, NY, USA), pp. 212–222, ACM, 2006.

[121] I. Ray, M. Kumar, and L. Yu, “Lrbac: A location-aware role-based access control model,” in *Proceedings of the Second International Conference on Information Systems Security*, ICISS’06, (Berlin, Heidelberg), pp. 147–161, Springer-Verlag, 2006.

[122] E. Bertino and M. S. Kirkpatrick, “Location-based access control systems for mobile users: Concepts and research directions,” in *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, SPRINGL ’11, (New York, NY, USA), pp. 49–52, ACM, 2011.

[123] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, “Private queries in location based services: Anonymizers are not necessary,” in *Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data*, SIGMOD ’08, (New York, NY, USA), pp. 121–132, ACM, 2008.

[124] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, “Approximate and exact hybrid algorithms for private nearest-neighbor queries with database protection,” *GeoInformatica*, vol. 15, no. 4, pp. 699–726, 2011.

[125] R. Paulet, M. G. Koasar, X. Yi, and E. Bertino, “Privacy-preserving and content-protecting location based queries,” in *Proceedings of the 2012 IEEE 28th International Conference on Data Engineering*, ICDE ’12, (Washington, DC, USA), pp. 44–53, IEEE Computer Society, 2012.

[126] R. Paulet, M. G. Kaosar, X. Yi, and E. Bertino, “Privacy-preserving and content-protecting location based queries,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, pp. 1200–1210, May 2014.

[127] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, “Practical k nearest neighbor queries with location privacy,” in *2014 IEEE 30th International Conference on Data Engineering*, pp. 640–651, March 2014.

[128] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, “Practical approximate k nearest neighbor queries with location and query privacy,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, pp. 1546–1559, June 2016.

[129] D. E. Denning and P. F. MacDoran, “Internet besieged,” ch. Location-based Authentication: Grounding Cyberspace for Better Security, pp. 167–174, New York, NY, USA: ACM Press/Addison-Wesley Publishing Co., 1998.

[130] B. Waters and E. Felten, “Secure, private proofs of locations,” in *Secure Internet Programming Laboratory, Department of Computer Science, University of Princeton, NJ, USA*, 2003.

[131] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, “Location-based trust for mobile user-generated content: Applications, challenges and implementations,” in *Proceedings of the 9th Workshop on Mobile Computing Systems and Applications*, HotMobile ’08, (New York, NY, USA), pp. 60–64, ACM, 2008.

[132] S. Saroiu and A. Wolman, “Enabling new mobile applications with location proofs,” in *Proceedings of the 10th Workshop on Mobile Computing Systems and Applications*, HotMobile ’09, (New York, NY, USA), pp. 3:1–3:6, ACM, 2009.

[133] W. Luo and U. Hengartner, “Veriplace: A privacy-aware location proof architecture,” in *Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems*, GIS ’10, (New York, NY, USA), pp. 23–32, ACM, 2010.

[134] R. Hasan and R. C. Burns, “Where have you been? secure location provenance for mobile devices,” *CoRR*, vol. abs/1107.1821, 2011.

[135] B. Davis, H. Chen, and M. Franklin, “Privacy-preserving alibi systems,” in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, ASIACCS ’12, (New York, NY, USA), pp. 34–35, ACM, 2012.

[136] X. Wang, A. Pande, J. Zhu, and P. Mohapatra, “Stamp: Enabling privacy-preserving location proofs for mobile users,” *IEEE/ACM Transactions on Networking*, vol. 24, pp. 3276–3289, Dec 2016.

[137] A. S. Gajparia, C. J. Mitchell, and C. Y. Yeun, “The location information preference authority: Supporting user privacy in location-based services,” *IEICE Transaction*, 2004.

[138] Y. Sun, T. F. L. Porta, and P. Kermani, “A flexible privacy-enhanced location-based services system framework and practice,” *IEEE Transactions on Mobile Computing*, vol. 8, pp. 304–321, March 2009.

[139] S. Rafaeli and D. Hutchison, “A survey of key management for secure group communication,” *ACM Comput. Surv.*, vol. 35, pp. 309–329, Sept. 2003.

[140] M. Srivatsa, A. Iyengar, J. Yin, and L. Liu, “Scalable key management algorithms for location-based services,” *IEEE/ACM Transactions on Networking*, vol. 17, pp. 1399–1412, Oct 2009.

[141] K. Rabieh, M. M. E. A. Mahmoud, and M. Younis, “Privacy-preserving route reporting schemes for traffic management systems,” *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 2703–2713, March 2017.

[142] “Ieee standard for wireless access in vehicular environments–security services for applications and management messages,” *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, pp. 1–240, March 2016.

[143] A. Wasef and X. Shen, “Emap: Expedite message authentication protocol for vehicular ad hoc networks,” *IEEE Transactions on Mobile Computing*, vol. 12, pp. 78–89, Jan 2013.

[144] Y. Cao and N. Wang, “Toward efficient electric-vehicle charging using vanet-based information dissemination,” *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 2886–2901, April 2017.

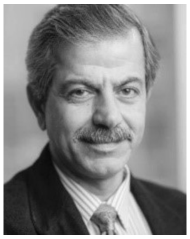
[145] M. Wagner and E. Grinberg, “Hurricane harvey’s aftermath: Live updates,” *CNN News room*, 2017.

[146] S. Bu-Pasha, A. Alen-Savikko, J. MÃď’kinen, P. Korpisaari, and G. Robert, “Eu law perspectives on location data privacy in smartphones and informed consent for transparency,” *European Data Protection Law, Volume.2, Version 3*, 2017.

[147] “Article 29 european commission data protection workng party on geolocation services on smart mobile-may 2011.”

[148] T. Zhang, H. Antunes, and S. Aggarwal, “Defending connected vehicles against malware: Challenges and a solution framework,” *IEEE Internet of Things Journal*, vol. 1, pp. 10–21, Feb 2014.

Philip Asuquo received his B.Eng degree in Computer Engineering from University of Uyo, Nigeria and MSc in Computer Network Technology from Northumbria University, Newcastle, UK. He received his PhD in Electronic Engineering at the University of Surrey, UK in 2018. His research interest includes Delay Tolerant Networks, Intelligent Transport Systems (ITS) and Wireless Sensor Networks. He is currently a Research Fellow at the at the Institute of Communication Systems, University of Surrey.

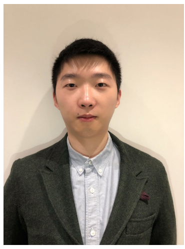


Haitham Cruickshank received a BSc degree in electrical engineering from the University of Baghdad, Iraq, in 1980, and MSc in telecommunications from the University of Surrey, UK and a PhD in control systems from Cranfield Institute of Technology, UK, in 1995. He is a senior lecturer at the Institute of Communication Systems, University of Surrey. His research interests are network security and privacy, satellite network architectures. He has been worked on several European research projects in the ACTS, ESPRIT, TEN-TELECOM, and IST programmes. He is a member of the Satellite and Space Communications Committee of the IEEE Communications Society, and is also a Chartered Electrical Engineer and IEE corporate.

Jeremy Morley Jeremy Morley is the chief Geospatial Scientist at Ordnance Survey. He has worked in geospatial research since the mid-90s. At Ordnance Survey, he leads the research and education team that carry out research in collaboration with universities. He is involved in GEOSEC: Lightweight Security and Privacy for Geographic Personal Data and Location Based Services with University of Surrey under PETRAS Cybersecurity of the Internet of Things Research Hub.

Chibueze Ogah received the BSc in computer science from the Ebonyi State University, Nigeria in 2005. He received the MSc degree (Distinction) in computer network technology from the University of Northumbria at Newcastle, UK in 2011. He is a PhD candidate at the Institute for Communication Systems, University of Surrey, UK. His research interests include security and privacy in vehicular networks, and Cisco routing protocols.

Ao Lei received his B.Eng degree in communication engineering at Harbin Institute of Technology, China and University of Birmingham, UK, in 2013, MSc degree in communication engineering at the University of York, UK, in 2014, and a PhD in Electronic Engineering from the University of Surrey, UK, in 2017. He is a Research Fellow at the Institute of Communication Systems since 2017. His research interests include security and privacy for vehicular networks, privacy protection for location based services and blockchain-based security and privacy frameworks. He is currently involved with two EU-funded Projects on security and privacy (PETRAS).



Shihan Bao received the B.Sc. degree in telecommunication engineering from Northumbria University, Newcastle upon Tyne, U.K, and the M.Sc. degree in communication system from University of Surrey, Guildford, U.K. He is currently pursuing the Ph.D. degree in electronic engineering at the University of Surrey, Guildford, U.K. His research interest includes the privacy-by-design in Internet-of-Things (IoT), and Low-Earth-Orbit (LEO) satellite based lightweight security structure.

Zhili Sun received his BSc in mathematics from Nanjing University, China and PhD from the Department of Computing, Lancaster University, UK, in 1991. He is a professor at the Institute of Communication Systems, University of Surrey, UK. His research interests include wireless and sensor networks, satellite communications, mobile operating systems, traffic engineering, Internet protocols and architecture, quality of service, multicast, and security. He has been principal investigator and technical coordinator in a number of projects within the European Framework Program including the ESPRIT BISANTE , TEN-Telecom, VIPTEN, GEOCAST, ICEBERGS, SATELIFE and EuroNGI.