In-Network Trajectory Privacy Preservation

XINYU JIN, Florida International University
MINGMING GUO, Florida International University
NIKI PISSINOU, Florida International University
SEBASTIAN ZANLONGO, Florida International University
BOGDAN CARBUNAR, Florida International University
S.S. IYENGAR, Florida International University

Recent advances in mobile device, wireless networking, and positional technologies have helped location-aware applications become pervasive. However, location trajectory privacy concerns hinder the adoptability of such apps. In this article, we survey existing trajectory privacy work in the context of sensor networks, location-based services and geo-social networks. In each context, we categorize and summarize the main techniques according to their own feathers. Furthermore, we discuss future trajectory privacy research challenges and directions.

Categories and Subject Descriptors: **C.2.0 [Computer-Communication Networks]**: General

General Terms: Design, Algorithms, Security.

Additional Key Words and Phrases: trajectory privacy, sensor networks, location-based service, geo-social networks

1. INTRODUCTION

Recent years have brought a significant growth of location-aware devices, including smart phones, sensors and radio-frequency identification tags. The age of combining location sensing, data processing, social communication in one device, leads to endless possibilities and a realization of location-aware applications. Location-aware devices continuously/periodically transmit data tagged with spatial and temporal coordinates, known as "trajectory information". Entities that receive or capture such information can track devices over time and space, leading to an undesirable trajectory privacy leakage. In worse scenarios, if adversaries can intercept this information, they can monitor the trajectory path and capture the location of the users or nodes, which severely threaten users' or nodes' safety. As sensing, computing and communication become more ubiquitous, trajectory privacy becomes a critical piece of information and an important factor for commercial success. The more confidently a system hides the trajectory information of a location-aware device, the wider the range of location-aware applications. The location-aware applications will remain elusive unless Trajectory Privacy Preservation (TPP) mechanisms are developed. TPP solutions have drawn tremendous attention from the research community.

In this article, we review existing work on TPP in the contexts of stationary and mobile Wireless Sensor Networks (WSNs), Location-based Service (LBS), Geo-Social Networks (GeoSNs). We focus on the concept named in-network computing. "In-network computing" here is defined as operations and algorithms are conducted on data streams while undergoing transmission among network nodes. We focus on TPP algorithms and protocols and the defenses they provide against trajectory privacy attacks that occur before the data reach an offline database. The algorithms are designed to operate in networks without offline trajectory data support -- in online or nearly online manner. Under this premise, complex, centralized and time-consuming trajectory data manipulation and computing operations are not well fitted.

For sensor networks, we divide our survey into two parts, stationary and mobile sensor networks. For stationary WSNs, the location privacy of a source node as well as sink are crucial since attackers may catch or follow the moving object that monitored by the network, such as protected animals, soldiers, etc. by detecting the signal from a source node with its location coordinate included or by compromising the base station which holds all the information. In mobile WSNs, either the sensor node or base station is moving or both are moving, the trajectory data contains valuable information to the service acquirers and thus becomes the target of the adversaries. The recent development in these two areas are investigated and organized with specific criteria.

Location-based Service (LBS) offer users and providers a unique opportunity to make use of real-time location data in order to learn about their surroundings. LBS is the key enabling technology that enables next generation content consumption such as Point of Interest (POI) discovery, car navigation, tourist city guides and so on. However, these services often come at the cost of compromised user privacy, potentially allowing mobile users' movements and schedules to be tracked. Significant progress has been made in the past several years concerning LBS privacy.

Author's addresses: X. Jin, Department of Electrical and Computer Engineering, Florida International University, 10555 W. Flagler Street, Miami, FL 33174; M. Guo, N. Pissinou, S. Zanlongo, B. Carbunar and S.S. Iyengar, School of Computing and Information Sciences, Florida International University, 11200 SW 8th St, Miami, FL 33174.

With the incredibly fast spread of online social networks and the evolution of real-time geocoding and geotagging technology, Geo-Social Networks (GeoSNs) are becoming increasingly popular. GeoSNs such as Foursquare and Yelp, provide convenient interfaces for users to share their trajectory data with families, friends, and even the public. However, the trajectory privacy leakage during such sharing experience may lead to serious privacy and safety vulnerabilities. There is only little effort made in this area which needs more participation.

This survey is organized as follows. In Section II, we overview the fundamentals of Privacy Preservation In Stationary WSNs; In Section III, we focus on Trajectory Privacy Preservation in Mobile WSNs; Section IV surveys Trajectory Privacy in Location-based Services, and finally we cover Trajectory Privacy in Geo Social Networks in section V.

2. PRIVACY PRESERVATION IN STATIONARY WSNS

Privacy preservation has so far been studied in stationary WSNs (sWSNs) in many existing works under the assumption that both the sensor nodes and the base station/sink are static. According to the taxonomy of privacy preservation techniques for WSNs in [Li et al. 2009], there are two main types of privacy concerns, data-oriented and context-oriented concerns. Data-oriented concerns focus on the privacy of data collected from, or query posted to, a WSN. Compared to data-oriented privacy concerns, context-oriented concerns concentrate on contextual information, such as the location and timing of traffic flows in a WSN. In this particular paper, context-oriented privacy is named as trajectory privacy in sWSNs. As data-oriented privacy is not the focus of this review, we introduce some existing works in brief in the following subsection.

2.1 Trajectory Privacy in sWSNs

In this subsection, we study the existing algorithms proposed to protect trajectory privacy in sWSNs. As an overview, we provide the following taxonomy in Figure 1.

2.1.1 Source Location Privacy in sWSNs

The location of a source node is crucial in the case that attackers may catch or follow the moving object that monitored by the sWSNs, such as protected animals, soldiers, etc. The existing techniques fall into three categories: routing path randomization, cryptographic technique, and dummy traffic injection. We review these techniques as follows.

2.1.1.1 Routing Paths Randomization

This main idea of this technique is to prevent attackers from tracking back the message source location by adding random routing hops en route to the sink. Researchers described the Panda-Hunter Game to study location privacy of the data source node [Kamat et al. 2005]. In order to hide the location of the Panda from adversaries who try to capture the panda by back-tracing the routing path of the event message, Phantom random walk routing is proposed. This routing protocol works in the way that when the source sends an event message, the message is firstly unicasted randomly or in a directed random fashion for certain hops before it is flooded or routed to the sink. To improve the randomness of the routing paths, Greedy Random Walk (GROW) is proposed. GROW requires the sensor node to randomly route the message to one of its neighbors, which has not participated in the previous random walk [Schwiebert and Shi 2006].

Li et al. studied a dynamic routing protocol which explicates the restricted random selection of intermediate nodes for message forwarding [Li and Ren 2010]. The authors suggest that in small scale WSNs, routing through single-intermediate nodes is efficient. Such intermediate nodes are randomly selected by the source and need to be away from the source with a minimum distance restriction. However, this method is not suitable for large-scale networks since attackers may deduce that the source is located within a circle region. The excessive long random routing paths cost unnecessary network resources as well. Therefore, the authors suggest angle-based and quadrant-based multi-intermediate nodes selection, where multiple intermediate nodes are selected based on their relative angle and distance to the source according to the sink. This method performs better in terms of message delivery ratio and privacy preservation. However, since the source node needs to predetermine the selected intermediate nodes and the quadrant reference frame, the computation could become a high cost for the source. Ligthfoot et al. design a STaR (Sink Toroidal Region) routing protocol for protecting the source node [Lightfoot et al. 2010]. There are two steps in STaR. The first step is to randomly select an intermediate node belonging to a pre-defined area that is not far from the sink. The second step is the packer transmission from the selected node to the sink using shortest-path routing. This protocol is simple to implement and also achieves good privacy preservation. It is also effective with respect to delivery delay and energy

consumption. However, the adversary can easily track the source node if it obtains the information of the sink toroidal region after long-time observation.

In [Ren and Tang 2011] and [Li et al. 2012], researchers proposed similar schemes using dynamic routing with hierarchical connected dominating sets. The algorithm works in the way that the source node randomly selects an intermediate node as the first relaying node. The messages are then forwarded through other nodes in the same level of Connected Dominating Sets (CDS) to the sink or a Network Mixing Ring (NMR), which blends messages from different sources. This method provides a high level of location privacy, and also guarantees the message is delivered efficiently. The drawback is that each node needs to consume power and memory to compute and record the CDS topology which leads to a shorter lifetime of nodes forming the NMR. [Yao and Wen 2008] proposed a directed random walk algorithm to solve the source location privacy issue. In this scheme, each sensor node is assumed to know its neighbors' relation positions. Upon observing an event, the node sends a packet by unicasting to a parent node with equal probability. The intermediate node who receives the packet will forward it to its parent nodes with the same probability. Every hop is greedy until the message arrives at the sink or base station. This scheme does not consume too much energy for each node and is easy to implement if sacrificing real-time transmission. [Spachos et al. 2011] introduced the opportunistic mesh networking technique to increase the source location privacy. Based on the concept of cognitive network, the node in the opportunistic mesh networks can observe the network conditions and then choose the node which is available to relay the packets. Due to the uncertainty on the node selection on the routing path, it is difficult for adversaries to find the source location. The drawback is that the source node will consume energy quickly and the delivery latency becomes high.

[Kang 2009] aims to protect the privacy of both source nodes and the base station by designing the secure path for each node to route to the next node. Each node categorizes its neighbors into certain sets and gives them probability for transmission. As the distance increases between the source node and the sink, the number of secure paths enhances exponentially, and thus it is very hard for an adversary to trace both of them. This scheme is very effective in large-scale sensor networks. By properly defining system parameters, the delivery delay and the strength of protection can be well balanced. [Song et al. 2011] proposed the Source Traceability Elimination for Privacy scheme by using heterogeneous links. This scheme makes use of Wormhole Pairs (WHPs) to protect the source location. The event message can be sent through the WHP link without using a regular channel to a long-distance destination. Generally, the global attackers do not know the WHP's phantom pattern, so it is difficult for them to track the source location. This method will not generate excessive traffic overhead and can be deployed in hybrid sensor networks. However, this method is vulnerable if the adversary knows the WHP's phantom pattern.

2.1.1.2 Cryptographic Techniques

A straightforward technique is to use cryptographic techniques to encrypt users' identities and data. Although symmetric and Public Key Cryptography (PKC) have already been applied in resource-constrained environments, there are still concerns in the implementations. For example, symmetric cryptography requires complex protocols that suffer from other constraints. "Software realizations of PKC lead to relatively long duty cycles (operating intervals) which in turn require a significant amount of energy. Computation is negligible if the PKC is performed by power efficient hardware accelerators. In such cases the corresponding transmission power becomes much more significant and dedicated hardware is required" [Peter et al. 2008].

Furthermore, only relying on cryptographic methods cannot resolve trajectory privacy issues in an effective and efficient way. Although the adversary does not have the knowledge of encrypted sensor data, data packets headers are usually left unencrypted for routing purposes where the source identity is revealed. In the case when data packet headers are also encrypted, the adversary still can obtain some public information of users, such as working and home addresses. Researchers have already shown how the adversary can crack users' encrypted/anonymized identities [Machanavajjhala et al. 2007, Chow et al. 2007] with adequate background knowledge.

An effective cryptographic method to prevent such encryption cracking to some extent is to encrypt or change the header or node identities every hop en route of message transmissions [Pongaliur and Xiao 2011]. The authors proposed the Source Privacy under Eavesdropping and Node compromise Attacks (SPENA) scheme to protect against the super-local eavesdropper and possible compromised nodes. The SPENA employs a one-way hash function for encrypting the source packets. The packets are rehashed by the dynamically selected intermediate nodes. Finally, the base station verifies the packets. The key point here is to dynamically select rehashing nodes on the routing path to alter the packet structure. Considering all the packets going through the selected node, it is expensive for the adversary to perform accurate analysis on every hop, which leads to good

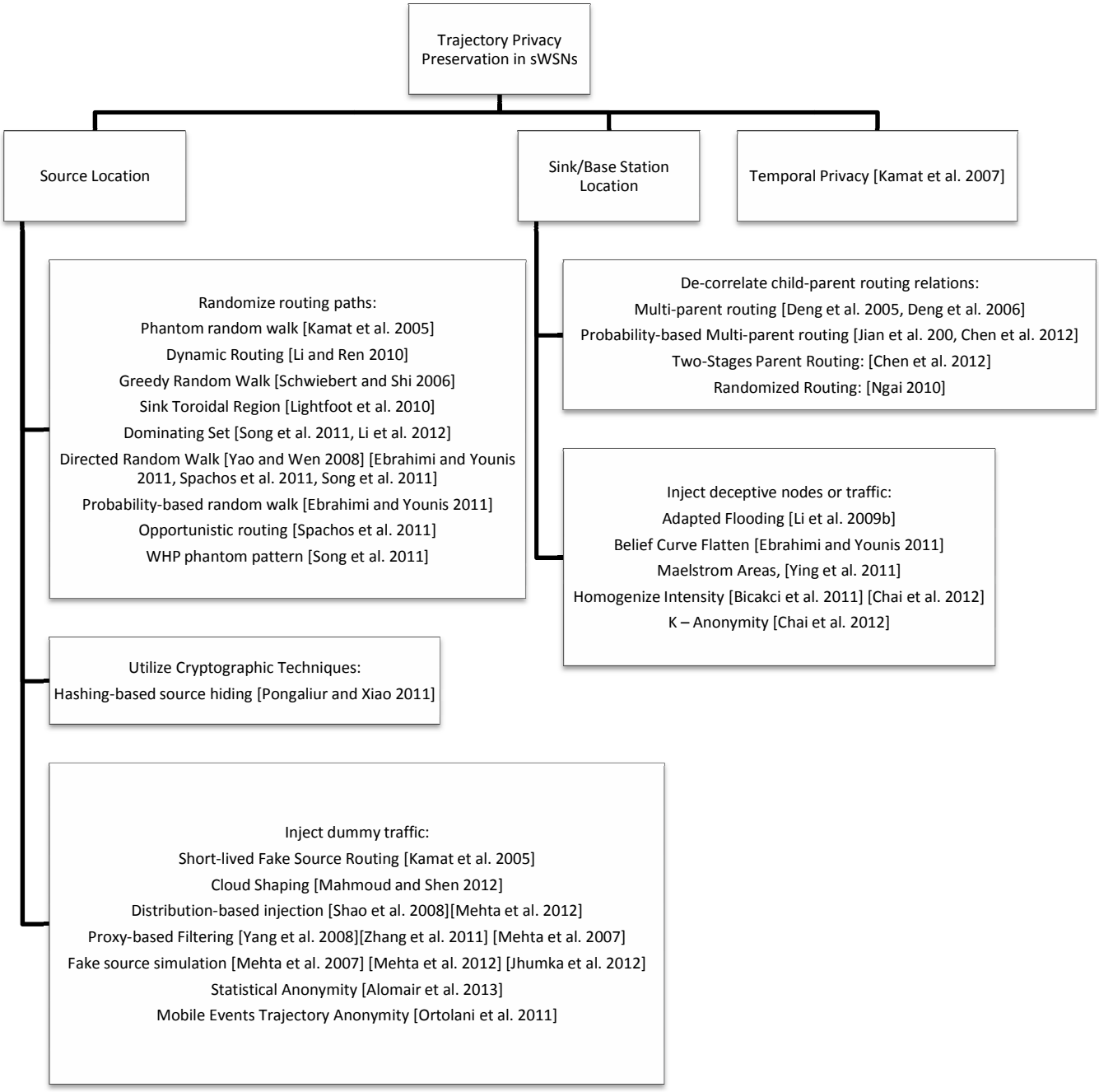
privacy preservation of the source identification. However, such technique faces the issue of synchronizing the encryption between nodes and the BS in implementations.

2.1.1.3 Dummy Traffic Injection

Dummy traffic injection is another widely used technique to preserve source location privacy in sWSNs. The main purpose is to perturb the network traffic to make the real and fake events undistinguishable. Generally, this technique includes fake message injection and fake source simulation.

Kamat et al. developed a simple scheme named Short-lived Fake Source Routing. It requires each node acting as a fake source by sending fake packets with a predetermined probability [Kamat et al. 2005]. This method is effective to prevent local adversaries who can observe the traffic pattern in a small area. However, it is possible for global adversaries who have the information of the entire network transmission rate and traffic patter to identify the fake packets. The Cloud-based privacy preserving scheme proposed by Mahmoud and Shen introduced the method which protects the source location by creating a cloud around the real source node with a random shape, and hides the real traffic pattern by injecting fake traffic within the shape [Mahmoud and Shen 2012]. The random traffic pattern within the cloud makes tracking the packet to the data source almost impossible. Such methods serve better source privacy than routing-based schemes. However, this technique is ineffective against global adversaries that can monitor the transmission rate of each sensor node and thereby identify those that are only sending out dummy data.

To address this problem, Shao et al. proposed the statistic-based dummy message injection [Shao et al. 2008]. In this method, all the nodes not only send fake messages with intervals following a certain distribution, but also the real events. In this way, the global adversary cannot distinguish the real events from fake messages. A similar algorithm was proposed in [Mehta et al. 2012], where sensor nodes send packets periodically and independently, including real or dummy packets.



- *Figure 1 Trajectory Privacy Preservation in sWSNs*

Although this baseline scheme provides event source un-observability, it is also prohibitively expensive for sensor networks. The huge number of dummy messages not only consumes the constrained energy of sensor nodes for transmissions, but also leads to high channel collision and consequently a low delivery ratio of real event messages. To address this issue, researchers proposed a Proxy-based Filtering Scheme (PFS) and a Tree-based Filtering Scheme (TFS) further more in which some sensors are selected as proxies to filter dummy messages before they reach the base station [Yang et al. 2008]. Zhang et al. propose an all proxy scheme which makes every sensor node have both sensing function and proxy-based filtering [Zhang et al. 2011]. The purpose is to ensure that dummy messages are never forwarded. Because of the filtering function performed by each node, the dummy packet is dropped whenever it is received by nodes. In this way, the network overhead and energy consumption can be reduced and higher message delivery rate can be achieved.

Another method to protect data source location privacy is fake source simulation proposed in [Mehta et al. 2007], [Mehta et al. 2012]. In the source simulation approach, a set of virtual objects will be simulated in the field. Each of them will generate a traffic pattern similar to that of a real object. In this way, there will be multiple movement patterns similar to that of real events. In such method, the tradeoff between the trajectory privacy level and power consumption needs to be well designed. Arshad et al. proposed two parameters, named message rates and fake message transmission duration, when using the fake source simulation technique to preserve source location privacy [Jhumka et al. 2012]. When the base station first receives the event message, it broadcasts a FakeNode message to select a fake source node within certain hops. Through controlling the two parameters, the privacy protection can be achieved at different levels. The higher values of the parameters, the higher the privacy level. This method is restricted by grid-structured networks.

[Alomair et al. 2013] designed a statistical framework for the anonymity of source location in WSNs. This framework offers a new concept called interval indistinguishability, which means that the real event can be incorporated in the fake message schedule in order to hide the real event. This framework also maps the statistical source anonymity to the binary hypothesis testing, and the adversary can match the data with its corresponding hypothesis. According to the probability of discovering the real event by the adversary, this framework provides the quantification for the statistical source anonymity. To improve anonymity, the authors proposed the same correlation between the real interval and fake interval about the internal transmission times. The drawback is that it is hard to completely hide real events due to their randomness. Ortolani et al. proposed a technique to protect the trajectory privacy of the mobile events observed in the sensor network while minimizing the delay of the transmission from the source location to the base station [Ortolani et al. 2011]. This scheme can make the real event unobservable to the adversary by carefully sending messages that mimic fake events. The mobility of the event is related to the generation of messages. The trajectory of the real event will be concealed by the trajectory of the dummy events. Even if the adversaries can notice the traffic of all the events, it is hard to differentiate the real from dummy events. Therefore, the real event can use the optimized path to reach the base station. This protocol can minimize the delivery latency for the base station to locate the event source.

2.1.2 Sink/Base Station Location Privacy in SWSNs

Besides protecting the data-source location, another important challenge for trajectory privacy is the proper hiding of the base station's location. Based on the main technique developed in the algorithms, we studied the previous work in the categories shown in Figure 1.

2.1.2.1 De-correlate child-parent routing relations

Deng et al. used hop-by-hop re-encryption to hide the destination address. It is used to ensure that the external appearance of a packet changes as it moves forward through a multi-hop sensor network [Deng et al. 2006]. Packet encryption can hide a packet destination, but cannot hide its sender. By carefully monitoring the packet sending time of every node, an adversary may infer the parent-children relationships and obtain some information about data traffic flows to track down the base station's location. To prevent this attack, de-correlating child-parent relationship is introduced in [Deng et al. 2006]. First the transmission delay is divided into m slots, if there are m-1 child nodes and 1 parent node. Every node is assigned a slot and randomly chooses a time within its slot to send its packet. As well, multiple-parent routing scheme is proposed in [Deng et al. 2005], [Deng et al. 2006], where each node randomly selects one of multiple parent nodes to route data to the base station. The parent nodes list can be obtained by the flooding beacon messages. To further diversify routing paths and mitigate rate monitoring attacks, when a node receives a packet, it forwards the packet to one of its parent nodes with a certain probability [Jian et al. 2007].

Chen et al. presented two location privacy attacks to the base station, the Parent-based Attack Scheme (PAS) and the Two-Phase PAS, which are based on sensor nodes' parent-child relations [Chen et al. 2012]. The authors

proposed a Child-based routing protocol, where each node has the information about its child set but not parent set, and only transmits for the child nodes. A node updates its neighbors' broadcast keys regardless of whether it receives or transmits messages. Adversaries cannot infer each node's parent set and differentiate among them. The author also proposed a parent-free protocol in which two successive nodes in a route may not have a normal parent-child relation by routing indirect packets. This means the packets are translated by a third node close to both of the two successive nodes. Thus, it is hard for the adversary to find the base station based on child-parent relations. [Ngai 2010] defined a Randomized Routing with Hidden Address (RRHA) scheme to protect the location privacy of the sink/base station. This scheme will hide the identity and location of the sink from the sensor node. Packets will be routed through several paths randomly, and the sink will read the data silently when the packets are received. After passing the sink, packets will still be routed for a predefined number of hops. This method prevents the traffic analysis attack and the destination attack by concealing the sink. The drawback is that the successful delivery rate may decrease to some extent due to the fixed hop count.

2.1.2.2 Inject Deceptive Nodes or Traffic

Li et al. applied anonymous topology discovery and intelligent fake packet injection for protecting location privacy by [Li et al. 2009b]. Anonymous topology discovery means that the base station randomly chooses a fake base station to initiate the topology discovery process, and then the fake base station sends the topology to the real base station through a tunnel. Intelligent fake packet injection means that when a node transmits a real packet to another node, it sends out fake packets intelligently by combining randomness and constancy to defend the packet tracing attack. This scheme does not bring an excessive traffic load and complexity to the sensor network by optimizing the fake packet injection.

[Ebrahimi and Younis 2011] introduced a belief-based technique for protecting the privacy of the base station by using Deceptive Packets (DP) to make the Belief curve flatten for different network cells. Its purpose is to increase the location anonymity of the base station by diverting the adversary's attention. Belief means the level of anonymity of a node by collecting its evidence for being the end point of a transmission path. The technique also uses the cell-based method to decrease the resources consumption, such as storage, etc. The adversary will pursue the location of the base station within the cell with the highest belief value after computing each cell's belief value. This algorithm will select some nodes in the cells with low belief values, which are less than the threshold as the potential destinations for deceptive packets to mimic the base station. In this way, the belief curve becomes flattened and the high level of anonymity of the base station is achieved. [Chang et al. 2011] gave a Maelstrom method to prevent packet tracing and traffic analysis attacks. The idea is to distribute some maelstrom parts in the network, and these parts can act as the receiver to collect fake packets sent by other sensor nodes. When a node sends messages to the sink, fake packets will be generated from those nodes along the path. Those fake packets will be forwarded to the maelstrom areas in order to distract the adversary from the real receiver. Also, the author introduced approximate the shortest routing algorithm to increase the randomness on the routing path. This technique is effective for both traffic analysis and packet tracing attacks.

[Ying et al. 2011] tried to conceal the sink location by artificially balancing traffic intensity. This technique consists of two steps. The first step is topology discovery in order to select some nodes to send fake messages. In this step, the sink learns the network topology for all sensors, and randomly selects some nodes to send fake messages. The second step is data transmission. In the spanning tree structure where the sink is the root, the nodes that are far from the sink are required to send the same number of messages as the closer ones. By using fake message injection to homogenize the intensity of the traffic in the network, the location privacy of the sink is well preserved. [Bicakci et al. 2011] adopted a linear programming framework for the sink's location preservation against a global eavesdropper considering the lifetime of sensor nodes. This framework formalized two techniques for concealing the sink: balanced flows and fake sinks. For the balanced flows, the method is to make the outgoing flows equal to the total incoming flows for each node except the base station. Each node acts as the sink, and drops messages that are routed to it. This framework shows that the network lifetime can be reduced halfway when preserving perfect privacy for the sink.

[Chai et al. 2012] proposed a k-anonymity approach to hide the sink by producing at least k nodes around the sink, which are indistinguishable from it. A quasi-optimal method is designed to find the positions of the k entities. This transfers the location question to be an optimization problem for finding the Euclidean minimum spanning tree. The author also considers the routing energy cost and privacy requirements when deriving the K designated nodes' locations. Through the k-anonymity method, the probability for the global adversary to locate to sink by monitoring the traffic statistics becomes low.

2.1.3 Temporal Privacy in SWSNs

Temporal information is the other element of trajectory information, besides location information. As reviewed, location privacy in sWSNs has drawn much attention from researchers. On the contrary, temporal privacy has not been formally defined. Kamat et al. made temporal privacy the main focus for their work [Kamat et al. 2007]. As informally defined in [Kamat et al. 2007], "If we assume that the adversary stays at the sink, collects all the packets that are generated by a source, and tries to infer the creation times of these packets from the times when they are received, then the temporal privacy can be defined as the mutual information between the received time sequences and the creation time sequences." Given the hop count and average delay on each hop, by observing the message's arrival time, attackers are able to infer the message's generation time. It is possible to locate the event to a specific region, given speed estimate. By monitoring multiple messages, the attacker may be able to predict the next spot of the event. Kamat et al. developed the Rate-Controlled Adaptive Delaying (RCAD) algorithm to protect temporal privacy. RCAD uses intermediate nodes to buffer received packets. The processing delay distribution is determined by the incoming traffic rate and available buffer space at each node.

RCAD employs buffer preemption mechanism to preemptively transmit the victim packets under buffer saturation. It serves a good tradeoff between temporal privacy and the buffer utilization. This method is very effective to prevent attackers from inferring message's generation time.

3. TRAJECTORY PRIVACY PRESERVATION IN MOBILE WSNS

There are only a few works studied trajectory privacy issues specifically focusing on mWSNs. We categorize the existing works based on the main techniques developed in the algorithms and their studied objects.

3.1 Location Privacy of Mobile Sinks

Researchers proposed a random data collection scheme to preserve the mobile sink location privacy in sensor networks [Ngai and Rodhe 2009]. The technique is composed of two stages. The first stage is the data forwarding and storage by sensor nodes where the source node forwards data randomly to its neighbors and continues the forwarding for several hops until data are stored. The second stage is that the mobile sink moves randomly in the area, requests the data from its neighbors occasionally and filters out the data that have been received. Due to the randomness of the data storage and the movement of the mobile sink, it is very difficult for the adversaries to track and attack the mobile sink. The drawbacks are that the delivery latency is bigger than non-random methods, and message loss rate could be high. To improve these drawbacks, [Yao 2010] adopted an improved random walk scheme. The first stage is local flooding where sensor nodes broadcast data to all the neighbors. Then the mobile sink takes a greedy random walk in the sensor region from the start point to the unreached area, and it continues move to the areas that have nodes with less pass-time counters.

3.2 Mobile Nodes' Trajectory Privacy

One proposed technique to preserve mobile nodes' trajectory privacy is to reduce the location resolution to achieve a desired level of safety protection [Xu and Cai 2009]. The authors consider an ad hoc network formed by a set of sensor nodes deployed in a hostile environment, where communications among the nodes may be open to an adversary. This location cloaking technique allows nodes to reveal their location information, yet make it practically infeasible for the adversary to locate them based on such information. To be more specific, each node will recursively compute a cloaking box by broadcasting its current locating region partition P and counting the number of neighbors within P. P is divided into equal halves until the number of nodes within P meets the desired safety level where P is set to be the cloaking box. This cloaking box is used as location information for reporting to service providers. To compute the cloaking box in the presence of node mobility, LEAVE, JOIN and MERGE messages need to be created to update the cloaking boxes for all the nodes in the corresponding partitions upon nodes' moving.

Another technique is recently proposed in [Jin et al. 2012]. Authors consider the infrastructure mobile sensor networks under the passive attack. To hide the trajectory of the target node in an on-line manner, Basic Trajectory Privacy (BTPriv) and Secondary Trajectory Privacy (STPriv) preservation algorithms were developed. Both BTPriv and STPriv employ the unique privacy-aware routing phase, where each node selects the next-hop node according to dynamic trajectory distance in order to hide its trajectory. The privacy-aware routing phase requests each node to route its data packet through privacy-aware path instead of shortest path. In order to select the proper next-hop node which helps the target node to hide the location at the time of data transmission from eavesdroppers, the target node needs to collect limited trajectory information from its neighboring nodes. To avoid privacy invasion of the neighbors' trajectory privacy, the one-time pad virtual name are used to exchange

messages. Using the trajectory privacy information of the neighbors, the target node computes the dynamic trajectory distance to each neighbor. The dynamic trajectory distance indicates the irrelevance between two trajectories at a specific time. Finally, the target node selects the neighbor which has the highest probability to mislead invaders as the next hop.

Although both above techniques have considerable limitations such as frequent messages exchanges to update trajectory information for privacy preservation, which consumes extra nodes' power and create traffic burden for the network, they are good beginnings as early works addressing trajectory privacy issues for mWSNs in on-line manner.

3.3 Trajectory Privacy in P2P and MANET Environments

Given the highly restricted network resources and special mobile network topology, the trajectory privacy issue in mWSNs has been a challenge and only a few works have been developed. In this subsection, we briefly review some trajectory privacy preservation works in Peer-to-Peer networks and Mobile Ad hoc Networks (MANETs) in the hope to motivate new techniques in mWSNs.

In peer-to-peer networks, [Chow et al. 2011] designed a peer-to-peer spatial cloaking scheme that can preserve the users' location privacy while obtaining the location-based services. The method is to let the mobile user cooperate with other users to map their location into a cloaked region to increase the difficulty for adversaries to find the exact location of the user. The scheme lets mobile users share location information in the local areas, and also cache the historical location of other peers which will be used for K-anonymity privacy computation. It also avoids the target mobile user always be the center of the cloaked areas and thus supplies a strong location protection against the adversary. [Freudiger et al. 2010] provided a framework to evaluate the privacy gains from the mix zones. The idea is that the mobile nodes can coordinated together to change their pseudonyms to get a better privacy for themselves. The mix zone is a region that can be used by mobile nodes in proximity of each other to protect their location in a coordinated manner. The adversary can only know the location of the zone but cannot know the targeted user's exact location. Through using multiple pseudonyms and the proper age for each pseudonym, the strong privacy of mobile nodes can be achieved.

[Liang et al. 2010] introduced a message authentication scheme for protecting users' privacy in MANETs which includes two important aspects. The first one is that the service provider can trace the users' identities while keeping them invisible from each other in the group of users. The second one is that the message receiver cannot deliver the authenticity to other parties when a node gives the authenticity of the message to that receiver. Through this method, the users' location privacy can be improved significantly due to the fact that the total number of authenticated messages is reduced and the adversaries cannot easily justify which information is true or not when they receive messages. A protocol in the work [Doomun and Soyjaudah 2010] has been invented for protecting the source and destination privacy against a powerful global adversary in MANETs. The first stage is initialization which means all nodes will be initialized in a broadcast mode at certain rate. The second stage is the route extrapolation using a Dijkstra algorithm. Both of sender and receiver will using the algorithm to select node until the two selected nodes face each other. The third stage is to generate dummy traffic at a rate same to the source node to hide the real packet transmission pattern. This protocol can provide the privacy for both of source and receiver in a flexible level. The drawback is the high delivery latency for finding the pair of nodes facing each other.

Hao et al. defined a uniform framework for the privacy protection which combines perturbation-based privacy preservation and malicious node revocation [Hao et al. 2010]. The node protects its location privacy by controlling the distribution of its location information. The position servers cannot link the node's position to its real identity. The second mechanism is to defend the inner malicious node which may reveal the location of the sender. It defends the malicious node by verifying the group signature for transmission. The malicious node will be revoked according to its bad reputation level accumulated by its malicious behavior. This framework can handle inner malicious nodes and achieve node-control privacy. However, the heavy traffic load generated by excessive controlling activities reduces the node's lifetime dramatically.

4. TRAJECTORY PRIVACY IN LOCATION-BASED SERVICES

Recently Location-Based Services (LBSs) are becoming popular among users of mobile devices. In LBS, mobile users need to report their location information obtained from GPS, Cell-ID or Wi-Fi connections to the application service provider to access the desired service. However, in this way, the user's real-time location and/or trajectory is revealed to the server which can compromise user's privacy. Trajectory privacy preservation for Location-Based Service considers user's mobility inherently since LBS frameworks rely on applications

running on cellular phones, PDA's or other smart mobile devices. The challenge is how to balance the trade-off between data accuracy and privacy level. We give the category of the techniques in the literature according to the system architecture that if there is a trusted third-party involved or not.

4.1 Trusted Third-Party-Based Techniques

4.1.1 Pseudonym-Based Techniques

Pseudonym-based techniques are used to remove the link between the user's identity and its location information by changing user's identities periodically. Mix Zone is the most famous method in the category. [Liu et al. 2012c] propose the traffic-aware multiple mix zone technique which puts multiple mix zones along the movement of mobile users. By using the graph theory, the problem becomes an optimization issue with certain constraints. The mix zone is also affected by the traffic conditions, which is taken into consideration. By computing the entropy, the best mix zone locations are selected. [Palisnamy and Liu 2011] also deploy the mix-zone approach for protecting the user's location privacy by considering multiple factors. For example, they consider the zones' geometry, the user population's statistical behavior, and the spatiotemporal resolution of the location's exposure. By giving a suite of construction methods for building the mix zone, it provides a lower bound on the anonymity level and a high level for the attack resilience.

4.1.1.1 Anonymity-based techniques

Anonymity-based Techniques are also called Cloaking-based Techniques. The general idea is to combine the user's query together with other users' to send to the service provider. Many of the previous works are based on k-anonymity [Sweeney 2002]. K-anonymity is a simple concept yet significant in the publication of microdata1. It states that a table is said to be k-anonymous "if and only if each sequence of quasi-identifier values appears with at least k occurrences" [Sweeney 2002]. In the LBS domain, k-anonymity is first introduced in [Gruteser and Grunwald 2003] is applied as each user submits queries along with other k-1 users or the query refers to k Points Of Interest (POIs). Some research also focuses on setting up the personal profile for each user to predefine the privacy requirement [Poolsappasit and Ray 2008]-[Poolsappasit and Ray 2009].

Based on the concept of k-anonymity, researchers proposed a framework that requires a trusted third party or extra unit, known as an anonymizer/cloaking agent [Ghinita 2009]. Upon receiving the query from a mobile user, the anonymizer produces an "imprecise" service request and forwards it to the server. The imprecise result is produced by removing the user's ID and aggregating the query with k – 1 queries from other users in a certain cloaking region. After the server responds to the queries, the anonymizer translates/filters the response and sends the "precise" results back to the user.

Built upon this framework, the following methods were implemented: In reference [Mokbel et al. 2006], researchers employed a grid-based complete pyramid data structure that hierarchically decomposes the space into H levels to create cloaking regions. In reference [Damiani et al. 2008], [Ghinita et al. 2007], researchers generated cloaking regions by implementing a Hilbert space filling curve as well. In reference [Yiu et al. 2008], researchers generated cloaking regions by computing the exact k Nearest Neighbors (kNN) in an incremental fashion. In reference [Gedik and Liu 2008], researchers proposed a personalized k-anonymity model that allows each mobile user to define and modify the anonymity level in both temporal and spatial dimensions.

In work [Wang et al. 2012], proposed a location-aware method for protecting the mobile users. The user can adjust the privacy level requirement according to the user's preference, which means the k can be changed along the movement of the users. According to the surrounding conditions and user's density, the user's location privacy can be protected in different setups for the parameters. The cloaking area can be changed dynamically and also be sufficient for mobile users. The work in [Masoumzadeh and Joshi 2011] gives an alternative anonymity named LBS(k, T)-anonymity to defend from location attacks in a time window. The main idea is to ensure the assumption that the user population will achieve k in time period T, which is not always available in other main techniques based on k-anonymity. The problem is formed as an optimization issue related to spatiotemporal dimensions. A greedy algorithm is proposed to ensure that all queries have K, which is the coverage value.

[Gong et al. 2010] designed a framework called KAWCR (K-Anonymity Without Cloaked Region). This method only needs the server to handle the incremental nearest-neighbor queries, and then guarantees the user cannot be distinguished from other k-1 users. By sending the center of a K-anonymizing spatial region, the method does

[1] Microdata is original data pertaining to an individual record. In the case of an LBS, it can be the person's name, location, or device information.

not send all the points to the server. It proposes an anonymizer-side kNN algorithm which processes the INN query for the LBS server. Then, the server sends POIs back to the anonymizer. These methods only need INN query processes without more complex computation at the server side. [Hwang et al. 2012] introduced an r-anonymity concept to blur the user's trajectory by preprocessing some similar trajectories R. This approach gave a time-obfuscation method which can break the list of time issuances of user's queries. This can prevent the attacker from learning the user's trajectory info, including the direction. Moreover, when user sends a query, it considers the s-segment to enhance the privacy level together with k-anonymity. The key here is that when a user is travelling, the anonymity server uses the time-obfuscated method to break the normal sequence of queries, and sends them randomly. The related information can be cached in the server and send results back to the users. The work in [Shin et al. 2010] tried to divide the whole request trajectory into many shorter trajectories in an optimal way. It also introduced the trajectory k-anonymity, which means that a user's trajectory should be anonymized by at least k-1 other trajectories.

Regardless of efficiency, effectiveness and the practicality of the above solutions, k-anonymity is vulnerable to background obtained attacks, query sampling attacks and query tracking attacks. To prevent background knowledge attacks, researchers proposed the l-diversity principle, which requires that the sensitive attribute needs to contain at least l well-represented values [Machanavajjhala et al. 2007].To address the query sampling attack, the concept of reciprocity in [Kalnis et al. 2007], [Chow and Mokbel 2007], which means a cloaking region not only contains at least k users, but the region is also shared by at least k of these users, is restricted to create cloaking region. Reference [Chow and Mokbel 2007] also introduced the memorization property for the cloaked query to eliminate query tracking attack.

4.2 Trusted Third-Party Free Techniques

4.2.1 Obfuscation based techniques

[Suzuki et al. 2010] tried to generate scatter locations close to the user which are based on the former fake locations and the user's actual location. According to the real road conditions, they adjust the process to get a better effect. [Ma et al. 2011] explored an effective tool named Gaussian Process Regression to preserve the trajectory privacy. The method is to re-construct the trajectory information of mobile users by exposing selected locations. The Gaussian Process Regression is used for inference of the possible direction for the trajectory, and thus can give the estimated information by feeding the GPR tool the location samples. By careful selection of the locations to be exposed, the exposure rate can be controlled within a certain level. This allows mobile users to give useful information for location based services while controlling the mobile users or nodes' trajectory privacy. The drawback is the service quality is only based on the selected exposing locations.

A system is designed in [Zhu and Cao 2011] to allow user to report a fake location to the LBS server to get the desired service. In this system, the mobile devices can generate location proofs and the location proof server can verify the trust level for them. The mobile device can also be protected by changing the pseudonyms statistically. The location privacy model with user concentration can evaluate the user privacy level time by time, and make the decision to accept the request of location proof. This approach focuses the combination of the location proof and location privacy to protect the user's privacy level. The work in [Ardagna et al. 2011] used the basic obfuscation operators to transform a location measurement by changing the center or radius. Also, the basic operators can be used together to execute in sequence. The operators protect the user's location privacy better than simple privacy enhancement solutions. [Feng et al. 2012] argued to generate fake paths along with the true trajectory. The noisy location will be generated as real location and reachable at that time with map information. The message with the combination of true position and noise data should be sent to the server with two scheduling strategies. The first one is normal scheduling strategy and the other is the disordered scheduling strategy. Both are used to confuse adversaries.

4.2.2 Anonymity based techniques

[Chow et al. 2011] explored a spatial cloaking algorithm for LBS based on the peer-to-peer environment we mentioned in the previous section. It is based on several features including an information sharing scheme, a historical location scheme and a cloaked adjustment scheme. For the first two features the algorithm is divided into a peer search step and a cloaked area building step. For the cloaked area adjustment scheme, the algorithm is divided into a center adjustment step and area adjustment step. The algorithm can satisfy user k-anonymity and the privacy desire of the least area. [Jia and Zhang 2013] gave two anonymity algorithms for LBS users in a mobile peer-to-peer way to protect the location privacy. The first algorithm will generate grid areas and let the mobile users judge the area by themselves, and then send the grid area ID instead of sending the real coordinates.

The second algorithm will let the proxy peer to generate an anonymized spatial region for the query user. However, it cannot resist the attack of continuous queries.

CAP (Context-Aware Privacy) in [Pingley et al. 2009] used two components to eliminate the disclosure of information which is location perturbing and anonymous routing components. The perturbing component introduces the Hilbert Curve Mapping to produce the perturbed location. The anonymous routing components try to reduce the user's network identity by relaying the LBS query to other nodes in the anonymous network. The work in [Nussbaum et al. 2012] introduced a (i, j)-privacy method by using the information of travel time to distribute probabilities and through less likely locations. Each user's location in one area is available with at least I locations in another area, and each user's location in the latter area should have at least j locations with the first area. The anonymized degree are higher along with the value i and j.

[Liu et al. 2013] adopted to use game theory to achieve k-anonymity for LBS users. The method is to let mobile users generate fake position according to the privacy level they need, especially when the level is less than k. The work proposed two Bayesian games in both static and time-aware contexts to model the behavior of users, and then help users achieve the optimized payoffs. [Zhu et. al. in 2013] provided a two-tier Adaptive Location Privacy-preserving System (ALPS). The separation tier introduces artificial perturbations into the location. However, an attacker could perform outlier filtering to deduce which determine which points have been modified. The conformation tier smoothens these anomalies to reduce the appearance that the location information has been tampered.

4.2.3 Protocol based techniques

Protocol-based techniques mean that a certain protocol has been developed for all the participators in the mobile system to follow in order to protect the location or trajectory information of users. Without the assistance from the anonymizer, an off-line phase to map POI locations all over the service regions into indexes is required in [Ghinita et al. 2008]. During the query process, the user encrypts the query with redundant information and filters the redundancy in the response. A similar idea proposed in [Riboni and Bettini 2012] is to simply generate dummy queries to confuse attackers. [Khoshgozaran et al. 2011] provided an approach to handle range and k-nearest neighbor queries based on the method of private information retrieval. This approach places trust on a secure coprocessor which is using for initiating PIR requests inside the service server. It devises a sweeping algorithm to handle range queries. The KNN queries are privately evaluated by three algorithms which are Hierarchical, Progressive and Hilbert-based algorithms. By using PIR, the user privacy can be guaranteed better than cloaking and anonymity based techniques. This method can prevent the server from learning the user location information, and also the content of users' queries.

An encryption approach given by [Buchanan et al. 2012] tried to protect the user's location and trajectory based on Private Equality primitive by creating a single encrypted table of identities and users can match the identities of their locations privately by checking this table. The protocol would let the users privately select the interesting records provided by the service server. [Ardagna et al. 2013] designed a protocol that let the local user of Wi-Fi network to form a group to defense the global adversary. It also provides an incentive to stimulate the peers to cooperate in this protocol. The peer who participates in the protection process will be anonymously rewarded by a micropayment scheme. This protocol also tries to minimize the probability of fake reward in hybrid scenarios.

4.2.4 Location sharing techniques

The work in [Shin et al. 2010] explored a share generation algorithm for protecting location privacy in non-trusted systems. It reduces the predictability in order that the adversaries are harder to obtain more accurate locations. By proposing a map-aware position sharing approach, the size of obfuscation areas can be adapted which are defined by map information shares. The idea of position sharing is to divide the original position information into a set of imprecise location shares which are distributed to many different location based servers. So the single LBS service cannot reveal the accurate location of users'.

A sub-trajectory synthesis algorithm is given in [Xue et al. 2012] for predicting the destination of LBS users. This algorithm uses a Markov model to compute the posterior probability for online given query trajectory. Then, the author tries to use a grid graph for abstracting the map and use Bayer's rule to predict the destination. After that, the user can choose to remove some critical locations in the query trajectory in order that the destination of the query trajectory cannot be predicted higher than a given threshold with a probability. [Wernke et al. 2013] gave a position sharing method to manage the user's private location information whose idea is to divide the user's location into location shares, and then distribute the location shares to different location servers which are used by multiple service providers. So the malicious provider can only discover a location with lower degree of

precision. This approach is powerful as it can defense the maximum velocity attack and also map mapping attacks to some degree.

[Shokri et al. 2009] defined a method of storing a user-side profile which is representative of the users' preferences; and a subset of that profile on the server side. Users' contact each other and update their offline profile by introducing a subset of their peers' profiles. The server receives this aggregate profile and reports back with a set of recommendations. The user client can then remove redundant or irrelevant recommendations based on its privileged information. This is further refined in [Shokri et al. 2011], with the use of MobiCrowd. This application establishes a *mobile transparent proxy* between nearby users through an ad-hoc network. LBS queries are first checked against nearby devices through this proxy. Only if no nearby devices have the request cached is the request sent to the LBS provider.

4.2.5 Geometric Based techniques

[Li et al. 2013] proposed a geometric solution to solve the location privacy leakage of mobile users. The idea is to send multiple center and radii queries to the application service provider instead of the users' location and interested scan radii. By using geometric computation, these queries can cover user's interest area. So an adversary only can derive an anonymity zone from those multiple queries. The drawback is the communication overhead is a little high, and it is still weak to trajectory attack for continuous LBS users.

4.3 Research Challenges for TPP in Location-based Service

The challenges for the trust thirty-party based techniques exist in several aspects:

- The biggest challenge is that if there is a trust third-party in the real world. The research community continuously asks this question making TTP-based techniques more questionable.
- Even if a trusted third-party exists, how to implement a system based on the TTP to satisfy personalized privacy requirement is still a challenge.

On the other hand, the TTP based techniques have more advantages and more flexibility because users directly send the request queries to the application service server without an intermediate party to ensure the user's privacy. Here we give several challenges for this type of solution:

- The biggest challenge is how to reduce the energy consumption because user's need to do some extra computation to protect themselves. This will require lighter algorithms and methods to achieve the privacy goal.
- The communication overhead in this type of solution is always high due to the extra information flow.

Game Theory is a good step towards reducing the overhead while also achieving minimal energy consumption by modeling mobile users as rational, self-interested users involved in the game in order to obtain their desired service and preferred privacy level.

5. TRAJECTORY PRIVACY IN GEO SOCIAL NETWORKS

With the incredible fast spreading of online social networks and the evolution of real-time geocoding and geotagging technology, GeoSN applications are becoming increasingly popular. As formally defined in Gambs et al.'s work, a GeoSN is "a web-based or mobile-based service that allow users to (1) construct a profile containing some of their geolocated data (along with additional information), (2) connect with other users of the system to share their geolocated data and (3) interact with the content provided by other users" [Gambs et al. 2011]. Popular GeoSNs, such as Foursquare, Twitter, Facebook Places, provide convenient interfaces for users to share their trajectory data with families, friends, and even the public. However, the trajectory privacy leakage during such sharing experience may lead to severe safety threaten [Borsboom et al. 2010].

To readers interested in the related topic of privacy vulnerabilities in GeoSN like Sybil Attacks, Fraudulent Check-Ins and Fake Reviews, etc. and related defense techniques we recommend the survey of [Carbunar et al. 2013]. In this section, we focus on trajectory privacy concerns in the field of GeoSNs and highlight related literatures. We will first briefly introduce the findings in analyzing privacy risk of the representative GeoSN applications. Then we study the TPP mechanisms proposed in existing works. Finally, we summarize TPP challenges and open issues in GeoSNs.

5.1 Trajectory Privacy Risk Analysis in GeoSNs

Most of GeoSN providers did not pay much attention on trajectory privacy issues in the first place. Gambs et al. provide a comparative privacy risk analysis of several existing GeoSNs, including Foursquare, Qype, La Ruche

and Twitter [Gambs et al. 2011]. The authors compare these GeoSNs in terms of privacy issues in the criteria of registration information, real identities versus pseudonyms, information available to others and privacy settings. They conclude that most of the current GeoSN do not integrated directly many privacy features.

Trajectory privacy risk in GeoSNs could be caused by three different resources, including 1) social network profiles, 2) location check-ins and queries, and 3) event posts and multimedia tagging.

Pontes et al. analyze the datasets collected from Foursquare, Google+ and Twitter. Without location inferring mechanisms, they found that the vast majority of Foursquare users provided valid home city locations in the corresponding venue attributes [Pontes et al. 2012a].

Similar findings are presented in [Pontes et al. 2012b], where a large number of users are found to exposure full addresses in their residential venue profiles. By analyzing the frequency and statistics of check-ins and geolocated data posts, these two groups of researchers also provide the location inferring mechanisms to infer possible residential addresses of GeoSN users. The results indicate that 78% of the analyzed users' home cities can be easily and correctly inferred within 50 kilometers of distance. Jin et al. focused on modeling and comparing the access control mechanisms for users' check-ins in the popular GeoSNs [Jin et al. 2012]. They conclude that there is no fine-grained access control mechanism for users' check-in information components. Co-location tagging also creates vulnerabilities to trajectory privacy. In [Cheng et al. 2013], Cheng et al. propose a probabilistic framework overcoming the absence of granular location information in the posts to estimate a microblog (such as Twitter) user's location purely relying on her publicly available posts. Besides utilizing the geolocated data posts, the authors also develop a classifier to identify words in status updates with a local geographic scope to discover the association of certain words or phrases with certain locations. As a result, this framework provides k estimated cities for each user with a descending order of possibility. On average, 51% of randomly selected microblog users are located within 100 miles of their actual location. These aforementioned findings indicate that trajectory privacy leakage and risk associated with GeoSN applications cannot be ignored and it is one of the critical issues which hinder the development of GeoSNs.

5.2 TPP Techniques in GeoSNs

5.2.1 Trajectory Obfuscation:

TPP issue in GeoSNs is more complex comparing with TPP in other LBS applications (we will analyze the challenges in the following section). There are only a few works have been proposed to address this issue. One of the major approaches is to apply trajectory obfuscation technique, such as spatio-temporal cloaking and space transformation.

Cuellar et al. first formally defined a number of notions for evaluating a location obfuscation function [Cuellar et al. 2012]. The authors define formalized the concept of indistinguishability of obfuscation functions, which requires that the user's actual location should be indistinguishable from a set a possible positions, e. g. an obfuscation region which includes the real location and noise. Indistinguishability needs to be satisfied under different scenarios: 1) when the attacker query a user's position at regular intervals, the attacker should not be able to increase the precision of his knowledge on the real location up to the predefined threshold chosen by the user; 2) an adversary should not be able to determine the destination from the user's original position and location updates in route; 3) an adversary cannot deduce that the user revisits a certain location. Additionally, with such indistinguishable properties, the obfuscation region needs to be constant for all points contained within it. For more restrict trajectory privacy protection, the obfuscation function needs to prevent attackers from determining users' current and past routes as well. Although this work defined an explicit concept of indistinguishability, it did not consider the impact of social relations and interactions among users on the privacy leakage, which is highly possible to be utilized by the adversary to infer users' location.

On the contrary, Freni et al. attempted to deploy a centralized trusted entity to process a user's original resource which may involve multiple users before publishing it to the GeoSN to insure it comply involved users' privacy preferences [Freni et al. 2010]. The authors introduce the notion of Minimal Uncertainty Region (MUR) as a spatio-temporal region for which an adversary cannot infer any internal point as the users' actual location. The location cloaking system architecture is presented in Figure 2. The pre-processing module is designed to retrieve the privacy preferences of all the involved users and the corresponding MUR. The cloaking module applies spatial generalization and/or temporal generalization (depending on the service attribute whether it is time sensitive) algorithms to generalize the pre-processed *srg* if the disclosure of *srg* introduces privacy violations. Then the result is processed by the publisher module where the users' absence privacy preferences will be complied by postponed the publication of the resources if necessary. This step is to enforce users' trajectory privacy under the scenario that an attacker may infer a user's absence by utilizing the current MUR and

maximum velocity. This system has great potential to be adapted on top of the current GeoSN architectures. However, the centralized trusted clocking entity could be an issue to be designated.

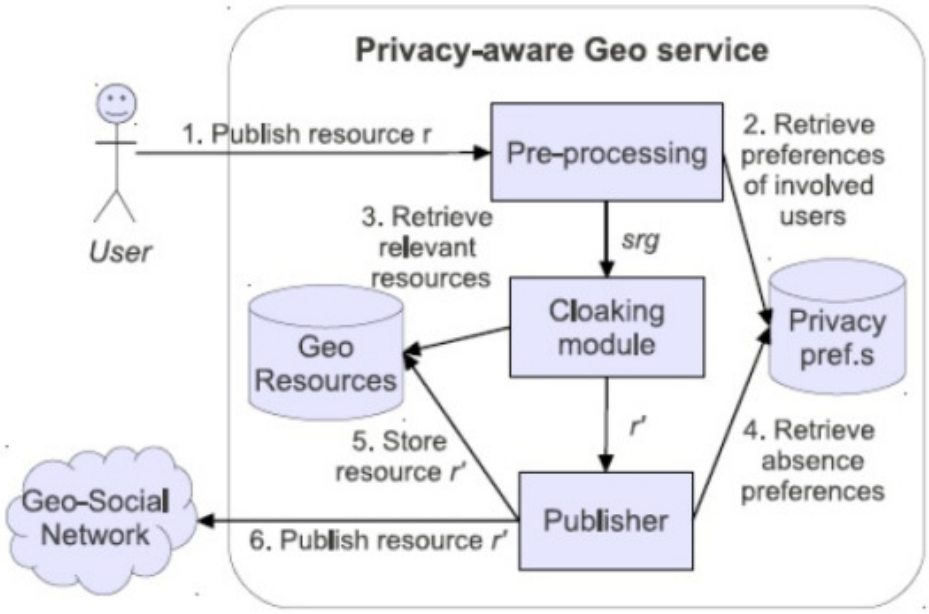


Figure 2 System architecture in [Freni et al. 2010]

Puttaswamy et al. applied a user-specific, distance preserving space transformation algorithm, named *LocX*, under the assumption that the GeoSN servers or other intermediaries are untrusted. This algorithm is intended to deal with point queries and nearest-neighbor (kNN) queries [Puttaswamy et al. 2012]. The main idea is that users share secret keys with their friends and use these keys to encrypt location data and store them in the proxy to process location queries. The encryption mapping is split into two pairs: a mapping from the transformed location to an encrypted index, named L2I, and a mapping from the index to the encrypted location data, named I2D. These two pairs are stored in two modules/servers in the proxy. When a user submits a query referencing to the certain POI, she submits the query in the form of transformed location data encrypted by symmetric keys to the proxy. The proxy returns the all the pairs of L2I that in the user's query. Then the user decrypts the index and queries the I2D pair. The proxy then returns the encrypted location data pair with the corresponding index. Although the authors claimed that *LocX* can run on mobile devices with low computation and communication cost, it is not presented that how the computation power consumption is evaluated, which is an important concern of mobile users. Moreover, the symmetric key distribution and rekeying management could be difficult to realize in practical GeoSNs.

There is another k-anonymity-based location cloaking algorithm proposed by Masoumzadeh et al. focusing on Anonymizing GeoSN Datasets [Masoumzadeh and Joshi 2011]. In this work, the authors tackle the issue that the location information revealed by social connections may assist an attacker in re-identifying a user.

In order to guarantee location privacy and users' identifies, the GeoSN datasets should satisfy $L_{2\,k}$-anonymity, meaning that there are at least k - 1 other users assigned the same location information for each user, and the user's adjacent users in the social network are assigned the same location information as other users' adjacent users too. The algorithm starts with each user as a separate cluster, centering at her location. In the iteration, the distance between every pair of cluster is computed in order to select the minimum pair to form a new cluster. The iteration stops until the cloaking region satisfies L_{2k}-anonymity. The possible difficulty to realize this algorithm is that in some cases, the uniqueness of a user may result in impossibility to satisfy L_{2k}-anonymity, such as a user is travelling out of town. Additionally, this work focuses on the datasets anonymization. There are still issues to adopt this algorithm into in-network computing, such as how to retrieve the location of other users to compute the distance. Nevertheless, the concept of L_{2k}-anonymity has great potential to resolve TPP in GeoSNs where social relation is playing an important role.

5.2.2 Context Analysis:

In GeoSN applications, context analysis is particularly an important tool for security and privacy protection due to the rich semantic contents during social interactions. Riboni et al. proposed an initial investigation to prevent users' POI preferences are learned by other users, which leads to privacy leakage [Riboni and Bettini 2012]. The main idea is to apply PINQ [McSherry 2009] query engine to enforce ϵ-differential privacy by adding random noise to extract statistics about personal preferences for POIs. To protect trajectory privacy, users submit their queries with a spatial granule in which they are currently located instead of the accurate location. Unfortunately, as an initial investigation, there is no detail of how to define the granularity level of the granule to guarantee both trajectory privacy and service accuracy.

Jagtap et al. proposed a context aware access control mechanism [Jagtap et al. 2011]. They adopt Web Ontology Language to capture users' characteristics, including location and surroundings, the presence of other people and devices, feeds from social networking systems they use and the inferred activities in which they are engaged. The reasoning engine is used to handle queries and performs reasoning for access control decisions. These two components support the privacy control module to enforce access control of the query to protected information. The privacy control module is embedded at both client and server sides to check the privilege to access protected resources for peer-to-peer queries and peer-to-server queries. There are several concerns to apply this mechanism: 1) the server might not be trustworthy; 2) the energy consumption of at the client side is not neglectful; and 3) since the privacy control module collects all the user's social profiles and preferences, it may need extra protection for security reasons.

5.2.3 Identity and Location Encryption:

Cryptography technique is a fundamental and direct solution for security and privacy protection. In GeoSNs, symmetric key encryption and hashing methods are commonly used in TPP in proximity services. Since proximity service is a particular application which mainly involves location coordinates manipulation and distance computation, the existing methods lack of generality to be applied in other GeoSN applications. Hence, we limit the number of related literatures here. More explicit materials are surveyed in [Mascetti et al. 2010], [Amir et al. 2007].

[Mascetti et al. 2010] proposed two protocols, named C-Hide&Seek and C-Hide&Hash, to protect a user's location privacy from untrusted Service Providers (SPs) and other users when she submit a proximity service request. In the C-Hide&Seek protocol, the SP replies with a message containing the latest encrypted location updates of each friend of the requester.

Since the encryption uses symmetric key, the requester can decrypt the message using the keys that shared with her friends. To prevent attackers from inferring that the target is crossing the boundary between two granules by monitoring the time stamp of the location updates, the location is only updated after a certain interval and identified by an interval index. The major difference of C-Hide&Hash with respect to C-Hide&Seek is that the requester provides a set of granules to check if any of her friend's location falls in this set. In this case, other users' locating granules are protected from the requester. This work has considered untrusted SPs and curious users, and provided the complete privacy preservation protocols in proximity service. The guaranteed location privacy has been theoretically approved. However, how to properly define the update interval still remains a question. Additionally, these protocols might not be applicable in time sensitive services due to the improper update interval. Moreover, as most of other methods using symmetric keys, the key distribution issue needs to be addressed before practical implementations. Li et al. also applied symmetric key hashing to transform location information during proximity service querying under similar system assumptions [Li et al. 2012]. Their work is focusing on increasing the proximity detection accuracy by using optimal grid overlay and multi-level grids.

In [Provost et al. 2012], suggest to used one-to-one or many-to-one hashing to hash users' identities and location information. This work focuses on utilizing GeoSN behavior similarity for Ad targeting like-minded individuals. Carbunar et al. designed the mechanisms that construct users' location centric profiles in a private and correct manner [Carbunar et al. 2012]. In this work, the authors prompt the issue of dishonesty in GeoSN applications, such as Yelp, Foursquare, where users may create incorrect check-ins to gain benefits, as well as the privacy violation issue when venues collect users' location centric profiles. The main idea is to install a device at each venue to initiate a challenge and authorize a time-stamped token encrypted by its secret key to check-in users. This step is used to prove a user's physical presence at the venue. Then the venue collects the user's profile by increasing the counter by 1 on a certain dimension and the corresponding range where user's profile value falls in. Then the statistics of the collected profiles is published. Although these two works lack details of TPP mechanisms, they are inspiring works that consider TPP issue in the inherent design of GeoSNs.

5.2.4 Statistical Modeling and Privacy by Design:

Recently statistical modeling technique becomes a new trend for privacy preservation in GeoSN. [Provost et al. 2011] argue that location based targeted advertisement should be provided with privacy by design in GeoSN, minimizing data collection and storage. They show that since statistical modeling techniques have no need for the data to retain its semantic meaning, targeted advertising can be made privacy friendly. Thus, user identifiers and locations can be (consistently) replaced by pseudo-random numbers which also protect the trajectory privacy. The challenge remains for GeoSN providers to adopt such privacy-by-design approach and to prove the fact they are not storing sensitive user information. Furthermore, there is a need to investigate the inability of an adversary to recover user identities from data anonymized as such. Another trend is to design the system with privacy as the primary feature in GeoSN. [Pidcock and Hengartner 2013] propose Zerosquare, a GeoSN architecture that decouples the storing of user identity information and the handling of user locations. They propose a set of goals, including providing privacy friendliness by design while supporting existing GeoSN applications, decoupling the data storage from the social networking functionality, and minimizing client side computations. They propose a set of APIs for the user data and location storage servers and show how applications such as locating friends, interest match and social recommendations can be provided with privacy. It remains to be seen if existing GeoSN providers are willing to switch to an architecture that prevents them from accessing parts of the user data, or, if new GeoSNs embracing these techniques from the start, will emerge.

5.3 Trajectory Privacy Features in GeoSNs

TPP in GeoSNs is particularly important to social network users due to the fact that trajectory information available from GeoSNs is always associated with users' social activities and such activities can be easily identifies from public or semi-public resources, such as urban patterns [Ferrari et al. 2011], open social events and interactions among users. As summarized in [Vicente et al. 2011], GeoSNs have several features which may render existing TPP techniques in LBS and databases to be directly applied. 1) Some applications, such as check-ins, require exact locations with high granularity. 2) Some applications require "real time" response, such as proximity services. 3) Users could be tagged passively, such as in photo posts and co-location check-ins. 4) Users could be re-identified through linking available background knowledge and external information.

In addition, we would like to emphasize the following two aspects. 1) The massive interaction among users could be a resource of trajectory privacy leakage. Regardless of passive tagging by friends or group members, users might reveal her trip plans or daily routines during the interaction with friends. Although the involved friends maybe trustworthy, the access to such interaction is commonly ignored by users. 2) Profiles of the same user from multiple GeoSN applications might lead to a clear "picture" of the user for re-identification. Actively social network users likely join more than one GeoSNs. Although users may be aware of privacy and set privacy preferences carefully, it is very possible for attackers to link information from multiple GeoSN accounts and extract more characteristics of the target.

5.4 Research Challenges in GeoSNs

As indicated in existing literatures [Freni et al. 2010], [Vicente et al. 2011], TPP in GeoSNs need to consider location privacy, absence privacy and collocation privacy. As the conclusion of this part, we summarize the challenges in terms of connections to be considered in GeoSNs as follows:

- The connection among users – It includes the social relations and the interaction among users during online social activities as we discussed above.
- The connection between the social pattern and available traces – As an entity in the society, participating in normal social activities is very common, which forms a certain pattern in corresponding environments. On the other hand, it is possible to infer private trajectory information from available traces and the social pattern.
- The connection among different GeoSNs and other online service sites – This is an issue which has been ignored in existing literatures. However, it is a highly possible and effective method for attackers to obtain private data since most of the online sites require users to register services by a unique identification, and many users use the same identity for registration, such as email accounts and phone numbers. Particularly facilitated by effective searching engines, like Google and Bing, collecting information from multiple sites is cost-efficient in terms of time and energy consumption. Moreover, different access control policies provided by variety GeoSN services hinder effective preservation mechanisms.

- The connection between the geographic map and available traces – This is a consistent issue to be considered along with TPP in different applications. However, in GeoSNs, the geographic map could contain rich social context. Combining background knowledge and social context may distinguish the target from other users who have similar available traces. For example, if there is an art exhibition in the museum, which is located nearby a church, on Sunday morning. It is likely that an art student is going to the museum and a religious person is going to the church, giving that they are both heading to this region. Geographic map associated with social context may further ease the inference of users' private trajectories.

6. REFERENCES

[1] Sébastien Gambs, Olivier Heen, and Christophe Potin. 2011. A comparative privacy analysis of geosocial networks. In Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS (SPRINGL '11). ACM, New York, NY, USA, 33-40. DOI=10.1145/2071880.2071887 http://doi.acm.org/10.1145/2071880.2071887

[2] Barry Borsboom, Boy van Amstel, Frank Groeneveld (2010) Please Rob Me, Available at: http://pleaserobme.com/ (Accessed: 12/09/2013).

[3] Tatiana Pontes, Gabriel Magno, Marisa Vasconcelos, Aditi Gupta, Jussara Almeida, Ponnurangam Kumaraguru, and Virgilio Almeida. 2012. Beware of What You Share: Inferring Home Location in Social Networks. In Proceedings of the 2012 IEEE 12th International Conference on Data Mining Workshops (ICDMW '12). IEEE Computer Society, Washington, DC, USA, 571-578. DOI=10.1109/ICDMW.2012.106 http://dx.doi.org/10.1109/ICDMW.2012.106

[4] Tatiana Pontes, Marisa Vasconcelos, Jussara Almeida, Ponnurangam Kumaraguru, and Virgilio Almeida. 2012. We know where you live: privacy characterization of foursquare behavior. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12). ACM, New York, NY, USA, 898-905. DOI=10.1145/2370216.2370419 http://doi.acm.org/10.1145/2370216.2370419

[5] Lei Jin, Xuelian Long, and James B.D. Joshi. 2012. Towards understanding residential privacy by analyzing users' activities in foursquare. In Proceedings of the 2012 ACM Workshop on Building analysis datasets and gathering experience returns for security (BADGERS '12). ACM, New York, NY, USA, 25-32. DOI=10.1145/2382416.2382428 http://doi.acm.org/10.1145/2382416.2382428

[6] Pongaliur, K. and Xiao, L., 2011. Maintaining source privacy under eavesdropping and node compromise attacks. In INFOCOM, 2011 Proceedings IEEE. pp. 1656–1664.

[7] Yun Li and Jian Ren. 2010. Source-location privacy through dynamic routing in wireless sensor networks. In Proceedings of the 29th conference on Information communications (INFOCOM'10). IEEE Press, Piscataway, NJ, USA, 2660-2668.

[8] Toby Xu and Ying Cai. 2009. Location safety protection in ad hoc networks. Ad Hoc Netw. 7, 8 (November 2009), 1551-1562. DOI=10.1016/j.adhoc.2009.04.001 http://dx.doi.org/10.1016/j.adhoc.2009.04.001

[9] Xinyu Jin, Niki Pissinou, Cody Chesneau, Sitthapon Pumpichet, and Deng Pan. "Hiding Trajectory on the Fly". In Proc. of IEEE International Conference on Communications (ICC 2012).

[10] Latanya Sweeney. 2002. k-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 10, 5 (October 2002), 557-570. DOI=10.1142/S0218488502001648 http://dx.doi.org/10.1142/S0218488502001648

[11] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. 2007. L-diversity: Privacy beyond k-anonymity. ACM Trans. Knowl. Discov. Data 1, 1, Article 3 (March 2007). DOI=10.1145/1217299.1217302 http://doi.acm.org/10.1145/1217299.1217302

[12] Zhiyuan Cheng, James Caverlee, and Kyumin Lee. 2013. A content-driven framework for geolocating microblog users. ACM Trans. Intell. Syst. Technol. 4, 1, Article 2 (February 2013), 27 pages. DOI=10.1145/2414425.2414427 http://doi.acm.org/10.1145/2414425.2414427

[13] Jorge Cuellar, Martín Ochoa, and Ruben Rios. 2012. Indistinguishable regions in geographic privacy. In Proceedings of the 27th Annual ACM Symposium on Applied Computing (SAC '12). ACM, New York, NY, USA, 1463-1469. DOI=10.1145/2245276.2232010 http://doi.acm.org/10.1145/2245276.2232010

[14] Dario Freni, Carmen Ruiz Vicente, Sergio Mascetti, Claudio Bettini, and Christian S. Jensen. 2010. Preserving location and absence privacy in geo-social networks. In Proceedings of the 19th ACM international conference on Information and knowledge management (CIKM '10). ACM, New York, NY, USA, 309-318. DOI=10.1145/1871437.1871480 http://doi.acm.org/10.1145/1871437.1871480

[15] Krishna P. N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel, and Ben Y. Zhao. 2014. Preserving Location Privacy in Geosocial Applications. IEEE Transactions on Mobile Computing 13, 1 (January 2014), 159-173. DOI=10.1109/TMC.2012.247 http://dx.doi.org/10.1109/TMC.2012.247

[16] Chi-Yin Chow and Mohamed F. Mokbel. 2007. Enabling private continuous queries for revealed user locations. In Proceedings of the 10th international conference on Advances in spatial and temporal databases (SSTD'07), Dimitris Papadias, Donghui Zhang, and George Kollios (Eds.). Springer-Verlag, Berlin, Heidelberg, 258-273.

[17] Amirreza Masoumzadeh and James Joshi. 2011. Anonymizing geo-social network datasets. In Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS (SPRINGL '11). ACM, New York, NY, USA, 25-32. DOI=10.1145/2071880.2071886 http://doi.acm.org/10.1145/2071880.2071886

[18] Gabriel Ghinita. 2009. Private Queries and Trajectory Anonymization: a Dual Perspective on Location Privacy. Trans. Data Privacy 2, 1 (April 2009), 3-19.

[19] Riboni, D. and Bettini, C., 2012. Private context-aware recommendation of points of interest: An initial investigation. In 2012 IEEE International Conference on Pervasive Computing and Communications Workshops. IEEE, pp. 584–589.

[20] Frank D. McSherry. 2009. Privacy integrated queries: an extensible platform for privacy-preserving data analysis. In Proceedings of the 2009 ACM SIGMOD International Conference on Management of data (SIGMOD '09), Carsten Binnig and Benoit Dageville (Eds.). ACM, New York, NY, USA, 19-30. DOI=10.1145/1559845.1559850 http://doi.acm.org/10.1145/1559845.1559850

[21] Maria Damiani, Elisa Bertino, Claudio Silvestri. 2008. PROBE: an obfuscation system for the protection of sensitive location information in LBS. TR2001-145, CERIAS.

[22] Gabriel Ghinita, Panos Kalnis, Ali Khoshgozaran, Cyrus Shahabi, and Kian-Lee Tan. 2008. 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). ACM, New York, NY, USA, 121-132. DOI=10.1145/1376616.1376631 http://doi.acm.org/10.1145/1376616.1376631

[23] Man Lung Yiu, Christian S. Jensen, Xuegang Huang, and Hua Lu. 2008. SpaceTwist: Managing the Trade-Offs Among Location Privacy, Query Performance, and Query Accuracy in Mobile Services. In Proceedings of the 2008 IEEE 24th International Conference on Data Engineering (ICDE '08). IEEE Computer Society, Washington, DC, USA, 366-375. DOI=10.1109/ICDE.2008.4497445 http://dx.doi.org/10.1109/ICDE.2008.4497445

[24] Panos Kalnis, Gabriel Ghinita, Kyriakos Mouratidis, and Dimitris Papadias. 2007. Preventing Location-Based Identity Inference in Anonymous Spatial Queries. IEEE Trans. on Knowl. and Data Eng. 19, 12 (December 2007), 1719-1733. DOI=10.1109/TKDE.2007.190662 http://dx.doi.org/10.1109/TKDE.2007.190662

[25] Bugra Gedik and Ling Liu. 2005. Location Privacy in Mobile Systems: A Personalized Anonymization Model. In Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05). IEEE Computer Society, Washington, DC, USA, 620-629. DOI=10.1109/ICDCS.2005.48 http://dx.doi.org/10.1109/ICDCS.2005.48

[26] Mohamed F. Mokbel, Chi-Yin Chow, and Walid G. Aref. 2006. The new Casper: query processing for location services without compromising privacy. In Proceedings of the 32nd international conference on Very large data bases (VLDB '06), Umeshwar Dayal, Khu-Yong Whang, David Lomet, Gustavo Alonso, Guy Lohman, Martin Kersten, Sang K. Cha, and Young-Kuk Kim (Eds.). VLDB Endowment 763-774.

[27] Gabriel Ghinita, Panos Kalnis, and Spiros Skiadopoulos. 2007. MOBIHIDE: a mobilea peer-to-peer system for anonymous location-based queries. In Proceedings of the 10th international conference on Advances in spatial and temporal databases (SSTD'07), Dimitris Papadias, Donghui Zhang, and George Kollios (Eds.). Springer-Verlag, Berlin, Heidelberg, 221-238.

[28] XI, Y., Schwiebert, L. and Shi, W., 2006. Preserving source location privacy in monitoring-based wireless sensor networks. In Proceedings 20th IEEE International Parallel & Distributed Processing Symposium. IEEE, p. 8 pp.

[29] Kamat, P., Zhang, Y., Trappe, W. and Ozturk, C., 2005. Enhancing Source-Location Privacy in Sensor Network Routing. 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), pp.599–608.

[30] Shao, M., Yang, Y., Zhu, S. and Cao, G., 2008. Towards Statistically Strong Source Anonymity for Sensor Networks. In 2008 IEEE INFOCOM - The 27th Conference on Computer Communications. IEEE, pp. 51–55.

[31] Yi Yang, Min Shao, Sencun Zhu, Bhuvan Urgaonkar, and Guohong Cao. 2008. Towards event source unobservability with minimum network traffic in sensor networks. In Proceedings of the first ACM conference on Wireless network security (WiSec '08). ACM, New York, NY, USA, 77-88. DOI=10.1145/1352533.1352547 http://doi.acm.org/10.1145/1352533.1352547

[32] Mehta, K., Liu, D. and Wright, M., 2007. Location Privacy in Sensor Networks Against a Global Eavesdropper. In 2007 IEEE International Conference on Network Protocols. IEEE, pp. 314–323.

[33] Kamat, P., Xu, W., Trappe, W. and Zhang, Y., 2007. Temporal Privacy in Wireless Sensor Networks. In 27th International Conference on Distributed Computing Systems (ICDCS '07). IEEE, pp. 23–23.

[34] Na Li, Nan Zhang, Sajal K. Das, and Bhavani Thuraisingham. 2009. Privacy preservation in wireless sensor networks: A state-of-the-art survey. Ad Hoc Netw. 7, 8 (November 2009), 1501-1514. DOI=10.1016/j.adhoc.2009.04.009 http://dx.doi.org/10.1016/j.adhoc.2009.04.009

[35] Rui Zhang, Yanchao Zhang, Kui Ren, "DP^2AC: distributed privacy-preserving access control in sensor networks". In Proc. of IEEE INFOCOM 2009 - The 28th Conference on Computer Communications, pp.1251–1259.

[36] Jing Deng, Richard Han, and Shivakant Mishra. 2005. Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks. In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM '05). IEEE Computer Society, Washington, DC, USA, 113-126. DOI=10.1109/SECURECOMM.2005.16 http://dx.doi.org/10.1109/SECURECOMM.2005.16

[37] Jian, Y., Chen, S., Zhang, Z. and Zhang, L., 2007. Protecting Receiver-Location Privacy in Wireless Sensor Networks. In IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications. IEEE, pp. 1955–1963.

[38] Jing Deng, Richard Han, and Shivakant Mishra. 2006. Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks. Pervasive Mob. Comput. 2, 2 (April 2006), 159-186. DOI=10.1016/j.pmcj.2005.12.003 http://dx.doi.org/10.1016/j.pmcj.2005.12.003

[39] Nayot Poolsappasit and Indrakshi Ray. 2008. Towards a scalable model for location privacy. In Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS (SPRINGL '08). ACM, New York, NY, USA, 46-51. DOI=10.1145/1503402.1503412 http://doi.acm.org/10.1145/1503402.1503412

[40] Nayot Poolsappasit and Indrakshi Ray. 2009. Towards Achieving Personalized Privacy for Location-Based Services. Trans. Data Privacy 2, 1 (April 2009), 77-99.

[41] Mascetti, S., Freni, D., Bettini, C., Wang, X.S. and Jajodia, S., 2010. Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies.

[42] Arnon Amir, Alon Efrat, Jussi Myllymaki, Lingeshwaran Palaniappan, and Kevin Wampler. 2007. Buddy tracking - efficient proximity detection among mobile friends. Pervasive Mob. Comput. 3, 5 (October 2007), 489-511. DOI=10.1016/j.pmcj.2006.12.002 http://dx.doi.org/10.1016/j.pmcj.2006.12.002

[43] Hong Ping Li, Haibo Hu, Jianliang Xu. 2013. Nearby Friend Alert: Location Anonymity in Mobile Geosocial Networks. IEEE Pervasive Computing, 12(4), pp.62–70.

[44] Mohamed M. E. A. Mahmoud and Xuemin (Shermin) Shen. 2012. A Cloud-Based Scheme for Protecting Source-Location Privacy against Hotspot-Locating Attack in Wireless Sensor Networks. IEEE Trans. Parallel Distrib. Syst. 23, 10 (October 2012), 1805-1818. DOI=10.1109/TPDS.2011.302 http://dx.doi.org/10.1109/TPDS.2011.302

[45] Yun Li, Jian Ren, and Jie Wu. 2012. Quantitative Measurement and Design of Source-Location Privacy Schemes for Wireless Sensor Networks. IEEE Trans. Parallel Distrib. Syst. 23, 7 (July 2012), 1302-1311. DOI=10.1109/TPDS.2011.260 http://dx.doi.org/10.1109/TPDS.2011.260

[46] Kiran Mehta, Donggang Liu, and Matthew Wright. 2012. Protecting Location Privacy in Sensor Networks against a Global Eavesdropper. IEEE Transactions on Mobile Computing 11, 2 (February 2012), 320-336. DOI=10.1109/TMC.2011.32 http://dx.doi.org/10.1109/TMC.2011.32

[47] Arshad Jhumka, Matthew Bradbury, and Matthew Leeke. 2012. Towards Understanding Source Location Privacy in Wireless Sensor Networks through Fake Sources. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TRUSTCOM

'12). IEEE Computer Society, Washington, DC, USA, 760-768. DOI=10.1109/TrustCom.2012.281 http://dx.doi.org/10.1109/TrustCom.2012.281

[48] Ren, J. and Tang, D., 2011. Combining Source-Location Privacy and Routing Efficiency in Wireless Sensor Networks. 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, pp.1–5.

[49] P. Spachos, Liang Song, F. M. Bui, and D. Hatzinakos. 2011. Improving source-location privacy through opportunistic routing in wireless sensor networks. In Proceedings of the 2011 IEEE Symposium on Computers and Communications (ISCC '11). IEEE Computer Society, Washington, DC, USA, 815-820. DOI=10.1109/ISCC.2011.5983942 http://dx.doi.org/10.1109/ISCC.2011.5983942

[50] Song, S., Park, H. and Choi, B.-Y., 2011. STEP: Source Traceability Elimination for Privacy against Global Attackers in Sensor Networks. In 2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN). IEEE, pp. 1–6.

[51] Yihua Zhang, Matthew Price, Lukasz Opyrchal, Keith Frikken. 2010. All proxy scheme for event source anonymity in wireless sensor networks. In 2010 Sixth International Conference on Intelligent Sensors, Sensor Networks and Information Processing. IEEE, pp. 263–268.

[52] Jianbo Yao and Guangjun Wen. 2008. Preserving Source-Location Privacy in Energy-Constrained Wireless Sensor Networks. In Proceedings of the 2008 The 28th International Conference on Distributed Computing Systems Workshops (ICDCSW '08). IEEE Computer Society, Washington, DC, USA, 412-416. DOI=10.1109/ICDCS.Workshops.2008.42 http://dx.doi.org/10.1109/ICDCS.Workshops.2008.42

[53] Alomair, B., Clark, A., Cuellar, J. and Poovendran, R., 2013. Toward a Statistical Framework for Source Anonymity in Sensor Networks. IEEE TRANSACTIONS ON …, 12(2), pp.248–260.

[54] Guofei Chai, Miao Xu, Wenyuan Xu, and Zhiyun Lin. 2012. Enhancing Sink-Location Pirvacy in Wireless Sensor Networks through K-Anonymity, International Journal of Distributed Sensor Networks, Volume 2012, pp. 1-16.

[55] Juan Chen, Hongli Zhang, Xiaojiang Du, Binxing Fang and Liu Yan, “Designing robust routing protocols to protect base stations in wireless sensor networks, *IEEE Wireless Communications and Mobile Computing*, 2012, DOI: 10.1002/wcm.2300

[56] Xinfeng Li, Xiaoyuan Wang, Nan Zheng, Zhiguo Wan, and Ming Gu. 2009b. Enhanced Location Privacy Protection of Base Station in Wireless Sensor Networks. In Proceedings of the 2009 Fifth International Conference on Mobile Ad-hoc and Sensor Networks (MSN '09). IEEE Computer Society, Washington, DC, USA, 457-464. DOI=10.1109/MSN.2009.19 http://dx.doi.org/10.1109/MSN.2009.19

[57] Lei Kang. 2009. Protecting location privacy in large-scale wireless sensor networks. In Proceedings of the 2009 IEEE international conference on Communications (ICC'09). IEEE Press, Piscataway, NJ, USA, 603-608 .

[58] Ebrahimi, Y. and Younis, M., 2011. Using deceptive packets to increase base-station anonymity in wireless sensor network. In 2011 7th International Wireless Communications and Mobile Computing Conference. IEEE, pp. 842–847.

[59] Shan Chang, Yong Qi, Hongzi Zhu, Mianxiong Dong, and Kaoru Ota. 2011. Maelstrom: receiver-location preserving in wireless sensor networks. In Proceedings of the 6th international conference on Wireless algorithms, systems, and applications (WASA'11), Yu Cheng, Do Young Eun, Zhiguang Qin, Min Song, and Kai Xing (Eds.). Springer-Verlag, Berlin, Heidelberg, 190-201.

[60] Ying, B., Gallardo, J.R., Makrakis, D. and Mouftah, H.T., 2011. Concealing of the Sink Location in WSNs by artificially homogenizing traffic intensity. In 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, pp. 988–993.

[61] Bicakci, K., Bagci, I. and Tavli, B., 2011. Lifetime bounds of wireless sensor networks preserving perfect sink unobservability. Communications Letters, IEEE, 15(2), pp.205–207.

[62] Ngai, E.C.-H., 2010. On providing sink anonymity for wireless sensor networks. Security and Communication Networks, p.n/a–n/a.

[63] Edith C.-H. Ngai and Ioana Rodhe. 2009. On providing location privacy for mobile sinks in wireless sensor networks. In Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems (MSWiM '09). ACM, New York, NY, USA, 116-123. DOI=10.1145/1641804.1641825 http://doi.acm.org/10.1145/1641804.1641825

[64] Yao, J., 2010. Preserving Mobile-Sink-Location Privacy in Wireless Sensor Networks. In 2010 2nd International Workshop on Database Technology and Applications. IEEE, pp. 1–3.

[65] Ortolani, S., Conti, M., Crispo, B. and Di Pietro, R., 2011. Events privacy in WSNs: A new model and its application. In 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks. IEEE, pp. 1–9.

[66] Lightfoot, L., Li, Y. and Ren, J., 2010. Preserving Source-Location Privacy in Wireless Sensor Network Using STaR Routing. In 2010 IEEE Global Telecommunications Conference GLOBECOM 2010. IEEE, pp. 1–5.

[67] Li Ma, Jiangchuan Liu, Limin Sun, and Ouldooz Baghban Karimi. 2011. The Trajectory Exposure Problem in Location-Aware Mobile Networking. In Proceedings of the 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems (MASS '11). IEEE Computer Society, Washington, DC, USA, 7-12. DOI=10.1109/MASS.2011.12 http://dx.doi.org/10.1109/MASS.2011.12

[68] Chi-Yin Chow, Mohamed F. Mokbel, and Xuan Liu. 2011. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. Geoinformatica 15, 2 (April 2011), 351-380. DOI=10.1007/s10707-009-0099-y http://dx.doi.org/10.1007/s10707-009-0099-y

[69] Julien Freudiger, Mohammad Hossein Manshaei, Jean-Yves Le Boudec, and Jean-Pierre Hubaux. 2010. On the age of pseudonyms in mobile ad hoc networks. In Proceedings of the 29th conference on Information communications (INFOCOM'10). IEEE Press, Piscataway, NJ, USA, 1577-1585.

[70] Liang, X., Lu, R., Lin, X. and Shen, X., 2010. Message Authentication with Non-Transferability for Location Privacy in Mobile Ad hoc Networks. In 2010 IEEE Global Telecommunications Conference GLOBECOM 2010. IEEE, pp. 1–5.

[71] M. Razvi Doomun, K.M. Sunjiv Soyjaudah, “Route Extrapolation for Source and Destination Camouflage in Wireless Ad Hoc Networks”, IEEE International Conference on Computer Communications Networks - ICCCN, Zurich, Switzerland, August 2-5, 2010

[72] Jianguo Hao, Weidong Liu, Yiqi Dai. 2010. A controllable Privacy Protection Framework in Position-based Routing for Suspicious MANETs, IET International Conference on Wireless Sensor Network, IET-WSN, 15-17 Nov. pp. 291-296.

[73] Xinxin Liu, Han Zhao, Miao Pan, Hao Yue, Xiaolin Li and Yuguang Fang, 2012c. Traffic-aware multiple mix zone placement for protecting location privacy. In 2012 Proceedings IEEE INFOCOM. IEEE, pp. 972–980.

[74] Balaji Palanisamy and Ling Liu. 2011. MobiMix: Protecting location privacy with mix-zones over road networks. In Proceedings of the 2011 IEEE 27th International Conference on Data Engineering (ICDE '11). IEEE Computer Society, Washington, DC, USA, 494-505. DOI=10.1109/ICDE.2011.5767898 http://dx.doi.org/10.1109/ICDE.2011.5767898

[75] Akiyoshi Suzuki, Mayu Iwata, Yuki Arase, Takahiro Hara, Xing Xie, and Shojiro Nishio. 2010. A user location anonymization method for location based services in a real environment. In Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems (GIS '10). ACM, New York, NY, USA, 398-401. DOI=10.1145/1869790.1869846 http://doi.acm.org/10.1145/1869790.1869846

[76] Yu Wang, Dingbang Xu, Xiao He, Chao Zhang, Fan Li, Bin Xu , "L2P2: Location-aware Location Privacy Protection for Location-based Services", IEEE INFOCOM, 2012.

[77] Masoumzadeh, Amirreza and Joshi, James B.D. "An Alternative Approach to k-Anonymity for Location-Based Services". In: The 8th International Conference on Mobile Web Information Systems (MobiWIS 2011), 19-21 September 2011, Niagara Falls, Ontario, Canada.

[78] Ali Khoshgozaran, Cyrus Shahabi, and Houtan Shirani-Mehr. 2011. Location privacy: going beyond K-anonymity, cloaking and anonymizers. Knowl. Inf. Syst. 26, 3 (March 2011), 435-465. DOI=10.1007/s10115-010-0286-z http://dx.doi.org/10.1007/s10115-010-0286-z

[79] Ren-Hung Hwang, Yu-Ling Hsueh, and Hao-Wei Chung. 2012. A Novel Time-Obfuscated Algorithm for Trajectory Privacy. In Proceedings of the 2012 12th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN '12). IEEE Computer Society, Washington, DC, USA, 208-215. DOI=10.1109/I-SPAN.2012.35 http://dx.doi.org/10.1109/I-SPAN.2012.35

[80] Zhichao Zhu, Guohong Cao. "APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services". IEEE INFOCOM 2011. Shanghai, China.

[81] Claudio A. Ardagna, Marco Cremonini, Sabrina De Capitani di Vimercati, and Pierangela Samarati. 2011. An Obfuscation-Based Approach for Protecting Location Privacy. IEEE Trans. Dependable Secur. Comput. 8, 1 (January 2011), 13-27. DOI=10.1109/TDSC.2009.25 http://dx.doi.org/10.1109/TDSC.2009.25

[82] Gong, Z., Sun, G.-Z. and Xie, X., 2010. Protecting Privacy in Location-Based Services Using K-Anonymity without Cloaked Region. In 2010 Eleventh International Conference on Mobile Data Management. IEEE, pp. 366–371.

[83] F. Provost, D. Martens, and A. Murray. 2012. Finding similar users with a privacy-friendly geo-social design. http://www.everyscreenmedia.com/everyscreenmedia/wpcontent/uploads/2012/10/Finding_Similar_Users.pdf, pp.1–26.

[84] A. Pingley, W. Yu, N. Zhang, Xinwen Fu and W. Zhao. "CAP: A Context-Aware Privacy Protection System for Location-Based Services", In Proceedings of the 29th IEEE International Conference on Distributed Computing Systems (ICDCS), June 22-26, 2009 Montreal, Quebec, Canada.

[85] Heechang Shin, Jaideep Vaidya, Vijayalakshmi Atluri, and Sungyong Choi. 2010. Ensuring Privacy and Security for LBS through Trajectory Partitioning. In Proceedings of the 2010 Eleventh International Conference on Mobile Data Management (MDM '10). IEEE Computer Society, Washington, DC, USA, 224-226. DOI=10.1109/MDM.2010.29 http://dx.doi.org/10.1109/MDM.2010.29

[86] Buchanan, W.J., Kwecka, Z. and Ekonomou, E., 2012. A Privacy Preserving Method Using Privacy Enhancing Techniques for Location Based Services. Mobile Networks and Applications, 18(5), pp.728–737.

[87] Doron Nussbaum, Masoud T. Omran, and Jörg-Rüdiger Sack. 2012. Techniques to protect privacy against inference attacks in location based services. In Proceedings of the Third ACM SIGSPATIAL International Workshop on GeoStreaming (IWGS '12). ACM, New York, NY, USA, 58-67. DOI=10.1145/2442968.2442976 http://doi.acm.org/10.1145/2442968.2442976

[88] Feng, Y., Liu, P. and Zhang, J., 2012. A Mobile Terminal Based Trajectory Preserving Strategy for Continuous Querying LBS Users. In 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems. IEEE, pp. 92–98.

[89] Andy Yuan Xue, Rui Zhang, Yu Zheng, Xing Xie, Jin Huang, and Zhenghua Xu. 2013. Destination prediction by sub-trajectory synthesis and privacy protection against such prediction. In Proceedings of the 2013 IEEE International Conference on Data Engineering (ICDE 2013) (ICDE '13). IEEE Computer Society, Washington, DC, USA, 254-265. DOI=10.1109/ICDE.2013.6544830 http://dx.doi.org/10.1109/ICDE.2013.6544830

[90] Liu, X., Liu, K., Guo, L., Li, X. and Fang, Y., 2013. A game-theoretic approach for achieving k-anonymity in Location Based Services, 2013 Proceedings IEEE.

[91] Jia, J. and Zhang, F., 2013. Twice Anonymity Algorithm for LBS in Mobile P2P Environment . Journal of Computational Information Systems, 9, pp.3715–3722.

[92] Claudio A. Ardagna, Sushil Jajodia, Pierangela Samarati, and Angelos Stavrou. 2013. Providing Users' Anonymity in Mobile Hybrid Networks. ACM Trans. Internet Technol. 12, 3, Article 7 (May 2013), 33 pages. DOI=10.1145/2461321.2461322 http://doi.acm.org/10.1145/2461321.2461322

[93] Marius Wernke, Frank DüRr, and Kurt Rothermel. 2013. PShare: Ensuring location privacy in non-trusted systems through multi-secret sharing. Pervasive Mob. Comput. 9, 3 (June 2013), 339-352. DOI=10.1016/j.pmcj.2013.01.001 http://dx.doi.org/10.1016/j.pmcj.2013.01.001

[94] Li, M., Salinas, S., Thapa, A. and Li, P., 2013. n-CD: A geometric approach to preserving location privacy in location-based services. In 2013 Proceedings IEEE INFOCOM. IEEE, pp. 3012–3020.

[95] Zhu, J., Kim, K.-H., Mohapatra, P. and Congdon, P., 2013. An adaptive privacy-preserving scheme for location tracking of a mobile user. 2013 IEEE International Conference on Sensing, Communications and Networking (SECON), pp.140–148.

[96] Reza Shokri, Pedram Pedarsani, George Theodorakopoulos, and Jean-Pierre Hubaux. 2009. Preserving privacy in collaborative filtering through distributed aggregation of offline profiles. In Proceedings of the third ACM conference on Recommender systems (RecSys '09). ACM, New York, NY, USA, 157-164. DOI=10.1145/1639714.1639741 http://doi.acm.org/10.1145/1639714.1639741

[97] Shokri, R., Papadimitratos, P., Theodorakopoulos, G. and Hubaux, J.-P., 2011. Collaborative Location Privacy. In 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems. IEEE, pp. 500–509.

[98] Bogdan Carbunar, Mahmudur Rahman, Naphtali Rishe, and Jaime Ballesteros. 2012. Private location centric profiles for GeoSocial networks. In Proceedings of the 20th International Conference on Advances in Geographic Information Systems (SIGSPATIAL '12). ACM, New York, NY, USA, 458-461. DOI=10.1145/2424321.2424389 http://doi.acm.org/10.1145/2424321.2424389

[99] Laura Ferrari, Alberto Rosi, Marco Mamei, and Franco Zambonelli. 2011. Extracting urban patterns from location-based social networks. In Proceedings of the 3rd ACM SIGSPATIAL International Workshop on

Location-Based Social Networks (LBSN '11). ACM, New York, NY, USA, 9-16. DOI=10.1145/2063212.2063226 http://doi.acm.org/10.1145/2063212.2063226

[100] Carmen Ruiz Vicente, Dario Freni, Claudio Bettini, and Christian S. Jensen. 2011. Location-Related Privacy in Geo-Social Networks. IEEE Internet Computing 15, 3 (May 2011), 20-27. DOI=10.1109/MIC.2011.29 http://dx.doi.org/10.1109/MIC.2011.29

[101] Sarah Pidcock and Urs Hengartner. 2013. Zerosquare: A Privacy-Friendly Location Hub for Geosocial Applications. Mobile Security Technologies (MoST) (May 2013).

[102] Provost, F., Martens, D. and Murray, A. 2011. Geo-Social Network Targeting for Privacy-friendly Mobile Advertising. everyscreenmedia.com, pp.1–26.

[103] Carbunar, B., Rahman, M., Pissinou, N. and Vasilakos, A. V., 2013. A survey of privacy vulnerabilities and defenses in geosocial networks. IEEE Communications Magazine, 51(11), pp.114–119.

[104] Steffen Peter, Peter Langendorfer, and Krzysztof Piotrowski. 2008. Public key cryptography empowered smart dust is affordable. Int. J. Sen. Netw. 4, 1/2 (July 2008), 130-143. DOI=10.1504/IJSNET.2008.019258 http://dx.doi.org/10.1504/IJSNET.2008.019258

[105] Buğra Gedik and Ling Liu. 2008. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms. IEEE Transactions on Mobile Computing 7, 1 (January 2008), 1-18. DOI=10.1109/TMC.2007.1062 http://dx.doi.org/10.1109/TMC.2007.1062