In-Network Trajectory Privacy Preservation

MINGMING GUO, XINYU JIN, NIKI PISSINOU, SEBASTIAN ZANLONGO, BOGDAN CARBUNAR, and 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 applications. In this article, we survey existing trajectory privacy work in the context of wireless sensor networks, location-based services, and geosocial 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.2.4 [**Computer-Communication Networks**]: Distributed Systems; H.3.5 [**Online Information Services**]: Data Sharing

General Terms: Design, Algorithms, Security

Additional Key Words and Phrases: Trajectory privacy, wireless sensor networks, location-based services, geosocial networks

ACM Reference Format:
Mingming Guo, Xinyu Jin, Niki Pissinou, Sebastian Zanlongo, Bogdan Carbunar, and S. S. Iyengar. 2015. In-network trajectory privacy preservation. ACM Comput. Surv. 48, 2, Article 23 (October 2015), 29 pages.
DOI: http://dx.doi.org/10.1145/2818183

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, and wireless 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 of location-aware applications. The more

This material is based upon work partially supported by AFOSR under grant FA9550-14-1-0299, NSF under grants CNS-1263124 and CNS-1407067. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the above agencies.
Authors' addresses: 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; emails: mguo001@cis.fiu.edu, pissinou@fiu.edu, {szanl001, carbunar}@cs.fiu.edu, iyengar@cis.fiu.edu; X. Jin, Department of Electrical and Computer Engineering, Florida International University, 10555 W. Flagler Street, Miami, FL 33174; email: xjin001@fiu.edu.

DOI: http://dx.doi.org/10.1145/2818183

confidently a system hides the trajectory information of a location-aware device, the wider the range of the services it provided. 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 Services (LBS), and Geosocial Networks (GeoSNs). We focus on the concept named in-network computing, which is a key and common characteristic among the three contexts. "In-network computing" here is defined as operations and algorithms 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. New algorithms need to be designed to operate in networks without offline trajectory data support—in an online or nearly online manner. Under this premise, complex, centralized and time-consuming trajectory data manipulation and computing operations are not well fitted. The three mentioned contexts are facing similar TPP problems for in-network computing. It is also possible that TPP problems exist in other unknown contexts that are not surveyed here.

To study TPP mechanisms in WSNs, we divide our survey into two parts: stationary and mobile sensor networks. In stationary WSNs, both the sensor node and base station are static; their location information is confidential and should be protected from malicious access. 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 developments in these two areas are investigated and organized with specific criteria. LBS offers 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. As a popular LBS, GeoSNs are becoming increasingly attractive. GeoSNs such as Yelp and Foursquare provide convenient interfaces for users to share their trajectory information with other users, and even the public. Nevertheless, such sharing experiences may lead to trajectory privacy leakage and even serious safety vulnerabilities. There is very limited effort that has been made in this area which needs more research participation.

This survey is organized as follows: In Section 2, we overview the fundamentals of TPP in stationary WSNs. In Section 3, we focus on trajectory privacy protection in mobile WSNs. Section 4 surveys trajectory privacy in LBS. We cover trajectory privacy in GeoSNs in Section 5, and finally present the conclusions in Section 6.

2. TPP 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 article, context-oriented privacy is named as trajectory privacy in WSNs. 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.

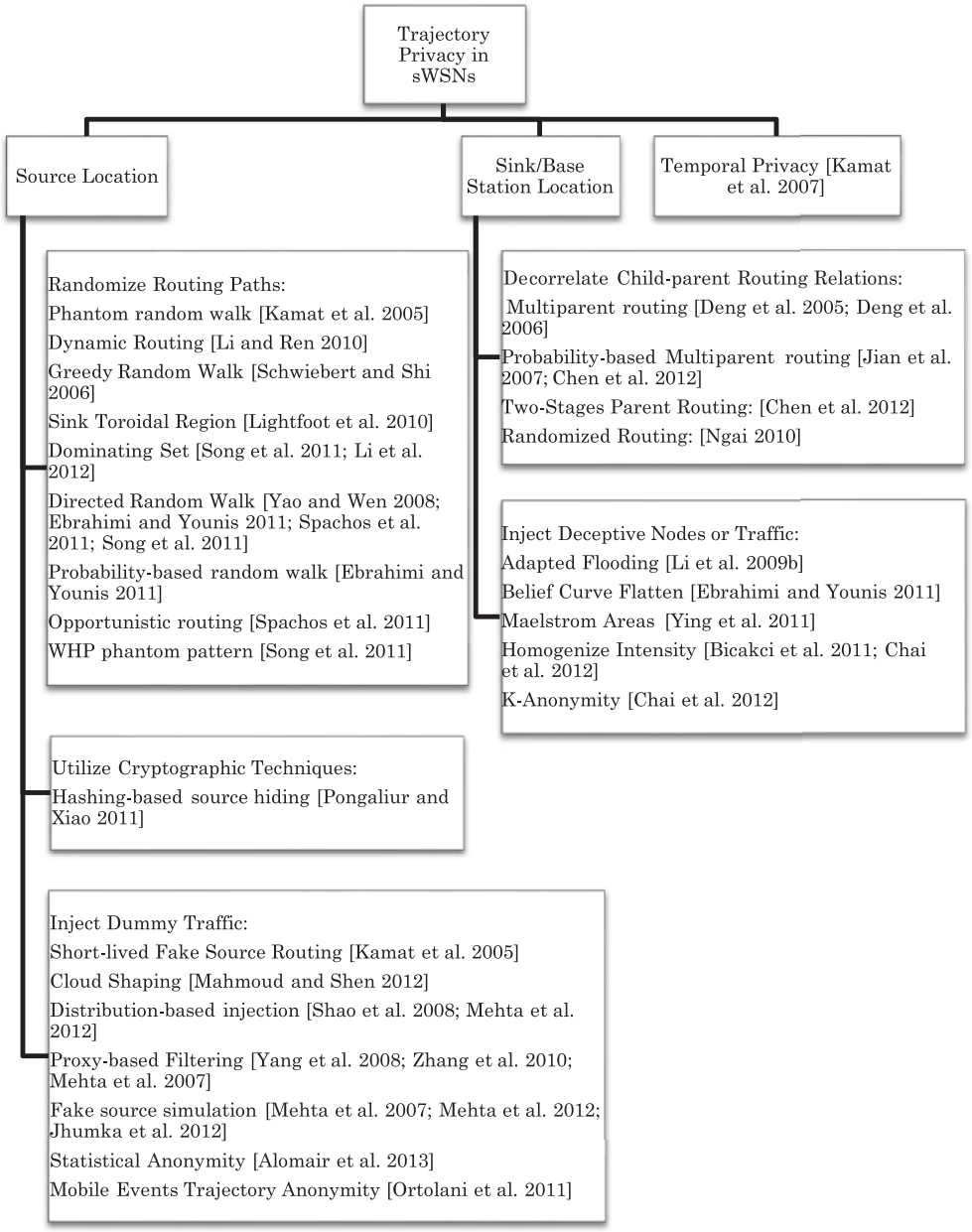

Fig. 1. Trajectory privacy preservation in sWSNs.

2.1. 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 is monitored by the sWSNs, such as protected animals, soldiers, etc. Researchers described the Panda-Hunter Game to study location privacy of the data source node [Kamat et al. 2005]. In a Panda-Hunter Game, a set of sensors is deployed to monitor the habitat for pandas. A source node who has observed a panda will report data periodically to the sink via multihop routing protocols. On the other hand, a

hunter tries to capture the panda by observing the routing path and backtracking the path until it discovers the source location. Thus, privacy-aware routing techniques need to be developed for protecting the source node, while ensuring the data is delivered to the sink. In addition, for dealing with sensor failure and reliable routing, we recommend the work in [Kannan et al. 2004]. The existing privacy-aware routing techniques fall into three categories: routing path randomization, cryptographic technique, and dummy traffic injection. We review these techniques as follows.

2.1.1. 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. In order to hide the location of the panda from adversaries who try to capture the panda by retrieving the routing path of the event message, Phantom random walk routing is proposed [Kamat et al. 2005]. This routing protocol works in a way such that when the source sends an event message, the message is first 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 that 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. Lightfoot et al. design a Sink Toroidal Region (STaR) 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 predefined area that is not far from the sink. The second step is the packet transmission from the selected node to the sink using shortest-path routing. This protocol is simple to implement and also achieves good privacy preservation results. 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 STaR 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 (CDS). 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 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 problem. In this scheme, the sensor nodes are assumed to know their 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. 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 a node that 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 drawbacks are 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.

2.1.2. 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. Due to the relatively long duty cycles for operation intervals, the software implementation of PKC leads to a significant energy consumption. On the other hand, power efficient hardware accelerators might be a better way for the PKC operation for reducing the computation cost. Then, the corresponding transmission power becomes much more efficient with the dedicated hardware [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 packet 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 work and home addresses. Researchers have already shown how the adversary can crack users' encrypted/anonymized identities [Machanavajjhala et al. 2007; Chow and Mokbel 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 base station in implementations. In addition, when the packets fail to reach the base station, it becomes very difficult for the source node to receive the error message from certain routes like "the message cannot be sent to the base station."

2.1.3. 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 packet 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 still possible for global adversaries who have the information of the entire network transmission rate and traffic pattern to identify the fake packets. The cloud-based privacy-preserving scheme proposed by Mahmoud and Shen introduced the method that 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 packets with intervals following a certain distribution, but also the real events. In this way, the global adversary cannot distinguish the real events from fake packets. A similar algorithm was proposed in Mehta et al. [2012], where sensor nodes send packets periodically and independently, including real or dummy packets.

Although this baseline scheme provides event source unobservability, it is also prohibitively expensive for sensor networks. The huge number of dummy packets 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 packets. To address this issue, researchers proposed a Proxy-based Filtering Scheme (PFS) and a Tree-based Filtering Scheme (TFS) furthermore in which some sensors are selected as proxies to filter dummy packets before they reach the base station [Yang et al. 2008]. Zhang et al. propose an all proxy scheme that makes every sensor node have both sensing function and proxy-based filtering [Zhang et al. 2010]. The purpose is to ensure that fake packets 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 a higher packet delivery rate can be achieved.

Another method to protect data source location privacy is fake source simulation proposed in Mehta et al. [2007, 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 trade-off 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 these 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.

In Alomair et al. [2013], Alomair et al. designed a statistical framework for anonymity of source location. 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 itself. 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 the real event discovered 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. However, 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]. The idea is to 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. Although 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, which minimizes the delivery latency.

2.2. 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 so far, we studied the previous work in the categories shown in Figure 1.

2.2.1. Decorrelate Child-Parent Routing Relations. Deng et al. used hop-by-hop reencryption to hide the destination address. The idea is to make sure that the external appearance of a packet changes as it moves forward through a multihop 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, decorrelating child-parent relationship is introduced in this work. 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], 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, named Parent-based Attack Scheme (PAS) and Two-Phase PAS, which are based on sensor nodes' parent-child relations [Chen et al. 2014]. The authors proposed a child-based routing protocol, where each node has the information about its child set but not its 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 hides the identity and location of the sink from the sensor nodes. 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 delivery rate may decrease to some extent due to the fixed hop count.

2.2.2. Inject Deceptive Nodes or Traffic. Li et al. applied anonymous topology discovery and intelligent fake packet injection for protecting location privacy of the base station [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 also 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 introduced a belief-based technique for protecting the privacy of the base station by using Deceptive Packets (DPs) to make the belief curve flatten for different network cells [Ebrahimi and Younis 2011]. The 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 resource consumption, such as storage, etc. The adversary pursues the location of the base station within the cell with the highest belief value after computing each cell's belief value. This algorithm selects some nodes in the cells with low belief values, which are less than the threshold as the potential destinations for DPs 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. gave a maelstrom method to prevent packet tracing and traffic analysis attacks [Chang et al. 2011]. 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. The authors also introduced approximately 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. tried to conceal the sink location by artificially balancing traffic intensity [Ying et al. 2011]. This technique consists of two steps. The first step is topology discovery. 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 sensor 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. adopted a linear programming framework for the sink's location privacy against a global eavesdropper with the consideration of the lifetime of sensor nodes [Bicakci et al. 2011]. The 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 also shows that the network lifetime can be reduced halfway for preserving perfect privacy for the sink.

In Chai et al. [2012], Chai et al. proposed a K-anonymity approach to hide the sink by producing at least k nodes around the sink, which are indistinguishable from it. A quasioptimal method is designed to find the positions of the k entities. This transfers the location problem to be an optimization problem for finding the Euclidean minimum spanning tree. The authors also consider 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 the sink by monitoring the traffic statistics decreases.

2.3. 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 this work, under the assumption that the attacker stays at the base station and collects all the packets that are sent by a source node, the temporal privacy can be defined as the mutual information between the creating time sequences and the received time sequences when the attacker tries to infer the creating times of the packets from their receiving times. 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 a buffer preemption mechanism to preemptively transmit the victim packets under buffer saturation. It serves as a good trade-off between temporal privacy and the buffer utilization. This method is very effective to prevent attackers from inferring message's generation time.

2.4. Research Challenges and Directions in Stationary WSNs

The location privacy problem for source nodes and base stations has been intensively investigated. However, most of the previous research focuses on preserving location privacy of source nodes or base stations independently. How to address the privacy issue for both of them remains an open problem. More efficient end-to-end privacy solutions should be explored in this area.

In addition, most of the solutions proposed by existing works consume large amounts of energy for data transmission for protecting source nodes/base stations. An interesting direction is how to use data compression techniques to reduce the data traffic in the network to save energy for sources/base stations.

Furthermore, the practical deployment of sWSNs with a certain node density also has a great impact on the underlying mechanism design. More specific solutions should be developed based on the particular conditions and applications of sWSNs.

3. TPP IN MOBILE WSNs

There are only a few works that 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. To reduce the communication cost, we propose a lightweight eavesdropping scheme.

3.1. Location Privacy of Mobile Sinks

Ngai and Rodhe proposed a random data collection scheme to preserve the mobile sink location privacy in sensor networks [Ngai and Rodhe 2009]. The scheme is composed of two stages. The first stage is the data forwarding and storage process, where the source node forwards data randomly to its neighbors and continues the forwarding process for several hops until the 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 nonrandom methods, and message loss rate could be high. To improve these drawbacks, Yao adopted an improved random walk scheme [Yao 2010]. The first step is called local flooding where the source node broadcasts packets to all its neighbors. Then, the mobile sink takes a GROW in the sensor region from the start point to the unreached area, and continues to 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, three types of messages need to be created to update the cloaking boxes for all the nodes in the corresponding partitions upon nodes' moving. If a node M moves out of its partition P, it broadcasts a leaving message to notify the nodes inside of P for them to compute the new safety level of P. This message contains the status of the node M who sends out the message. When M tries to join a new partition P', it broadcasts a joining message to the nodes inside of P' to compute the new safety level. If the safety level is lower than a certain value, each node inside of P' will take the parent partition P'' of P' and broadcast a merging message to the nodes inside P''. Other nodes who are receiving these messages can take certain actions toward improving the safety level of current partition.

Another technique is recently proposed in Jin et al. [2012]. The authors consider that the infrastructure of mobile sensor networks is under the passive attack. To hide the trajectory of the target node in an online manner, Basic Trajectory Privacy (BTPriv) and Secondary Trajectory Privacy (STPriv) preservation algorithms were developed. Both BTPriv and STPriv employ the unique privacy-aware routing process, where each node selects the next-hop node according to the dynamic trajectory distance for hiding its trajectory. The privacy-aware routing phase requests that each node should route its data packet through a privacy-aware path instead of the shortest path. In order to select the proper next-hop node that helps the target node to hide its location at the time of data transmission, the next-hop 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 is used to exchange messages. Using the trajectory information from 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 that has the highest probability to mislead invaders as the next hop.

Although both of the techniques have strong limitations, such as frequent message exchanges for updating trajectory information for privacy preservation, which consume extra nodes' power and create a traffic burden for the network, they are good beginnings as early works to address trajectory privacy issues for mWSNs in an online 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 TPP works in Peer-to-Peer (P2P) networks and Mobile Ad hoc Networks (MANETs) in the hope to motivate new techniques in mWSNs.

In P2P networks, Chow et al. designed a peer-to-peer spatial cloaking scheme that can preserve the users' location privacy while using LBS [Chow et al. 2011]. The idea is to let the mobile user cooperate with other users to map his/her location into a cloaked region in order to increase the difficulty for adversaries to find the exact location of the user. The scheme lets mobile users share their location information with each other in the local areas, and also cache the historical location of other peers that can be used for K-anonymity privacy computation. It also avoids the situation that the target user might always be the center of the cloaked areas, and thus supplies a strong location protection against the adversary. Freudiger et al. provided a framework to evaluate the privacy gains from the mix zones [Freudiger et al. 2010]. In Mix Zone, mobile nodes can change their pseudonyms at the same time. The mix zone is a region that can be used by mobile nodes in proximity of each other to protect their locations in a coordinated manner. The adversary only knows the location of the zone but not the targeted user's exact location. By utilizing multiple pseudonyms and proper age for each pseudonym, strong privacy protection for mobile nodes can be achieved.

Liang et al. proposed a message authentication scheme for protecting user privacy in MANETs [Liang et al. 2010]. There are two important aspects. First, the service provider can trace the users' identities while keeping them invisible from each other in the group of users. Second, the message receiver should not deliver the authenticity to other parties when a node delivers authenticity of the message to him/her. In this way, 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 one is true when they receive messages. In Doomun and Soyjaudah [2010], a protocol has been invented for protecting the source and destination privacy against a powerful global adversary in MANETs. The first stage of the protocol is the initialization process where all nodes will be initialized in a broadcast mode at a certain rate. The second stage is the route extrapolation process using a Dijkstra algorithm. Both the sender and receiver use the algorithm to select nodes until the two selected nodes face each other. The third stage is to generate dummy traffic at a rate that should be the same as the source node to hide the real packet transmission pattern. This protocol can provide privacy for both the source and receiver in a flexible level. However, there will be high delivery latency for finding a pair of nodes facing each other.

Hao et al. defined a uniform framework for privacy protection that combines perturbation-based privacy preservation and malicious node revocation [Hao et al. 2010]. In this framework, a node protects its location privacy by controlling the

distribution of its location information. The location servers cannot link a node's position to its real identity. The second mechanism is to defend the inner malicious node that may reveal the location of the sender. It defends the malicious node by verifying the group signature for data transmission. A malicious node will be revoked according to the bad reputation level accumulated by its malicious behaviors. This framework can handle inner malicious nodes and achieve node-controlled privacy. However, the heavy traffic load generated by excessive controlling activities reduces the node's lifetime dramatically.

3.4. Research Challenges and Directions in Mobile WSNs

The trajectory privacy in mobile WSNs is still an active research area. There are many challenges that need to be addressed for privacy preservation of mobile nodes and sinks.

First, similar to the problem in stationary WSNs, the existing solutions in mobile WSNs focus on either mobile nodes or sinks but lack a comprehensive framework for protecting both of them.

Secondly, current research works make the assumption that if the sensor nodes are mobile, then the sink should be static, and vice versa. This assumption may not always be the case and more investigation needs to be conducted on it. The problem becomes more challenging if both the source and sink are mobile.

Thirdly, multiple mobile nodes in mWSNs may form a MANET. From the MANET's point of view, how to efficiently deliver the source data among a set of mobile nodes remains a question. Additional areas of inquiry include how to detect the inner malicious nodes that are compromised by an adversary, and how to defend the attacks from such malicious nodes.

Last but not least, it is also important to explore how to evaluate the efficiency of the proposed schemes in mobile WSNs; and which privacy metric is better to use (i.e., entropy-based metric, or trajectory k-anonymity).

4. TRAJECTORY PRIVACY IN LBS

LBS provide users with convenient functions and services with respect to their locations. In LBS, mobile users need to report their coordinates, obtained from GPS, Cell-ID, or Wi-Fi connections, to the LBS server for accessing the data services. However, in this way, a user's real-time location and/or trajectory is revealed to the service provider, which may compromise user privacy. Trajectory privacy protection in LBS should consider user mobility inherently, because LBS frameworks rely heavily on applications running on cellular phones, PDA's, or other smart mobile devices. According to the LBS system architecture, we first give the categories of the techniques in the literature. Then, we list some research challenges and possible directions for TPP in LBS.

4.1. Trusted Third-Party-Based Techniques

4.1.1. Anonymity-Based Techniques. Anonymity-based techniques are also called cloaking-based techniques. The general idea is to combine a user's query together with a query set of other users sent to the service provider. Many of the previous works are based on K-anonymity. K-anonymity is a simple yet significant concept in the publication ofmicrodata. 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 by Gruteser and Grunwald, and is applied as each user submits queries along with other $k-1$ users or the query refers to k POIs [Gruteser and Grunwald 2003]. Some research also focuses on setting

up the personal profile for each user to predefine the privacy requirement [Poolsappasit and Ray 2008, 2009].

Based on the concept of K-anonymity, Ghinita 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 Mokbel et al. [2006], Mokbel et al. deployed a grid-based complete pyramid data structure that hierarchically decomposes the space into H levels to create cloaking regions. In Damiani et al. [2008] and Ghinita et al. [2007], researchers generated cloaking regions by implementing a Hilbert space filling curve as well. In Yiu et al. [2008], Yiu et al. built the cloaking regions by computing the exact k Nearest Neighbors (kNN) in an incremental fashion. In Gedik and Liu [2008], the authors 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 Wang et al. [2012], Wang et al. proposed several location-aware algorithms for protecting location privacy of mobile users. In this work, a user can adjust the privacy level according to his/her preference along with the movement. Based on the surrounding conditions and users' density, the user's location privacy can be protected by modifying certain parameters in several ways. Masoumzadeh and Joshi proposed an alternative anonymity concept named LBS (k, T)-anonymity to defend against location attacks in a time window [Masoumzadeh and Joshi 2011]. The main idea is to make sure that the user population should achieve k in time period T, which is not always available in other main methods based on K-anonymity. In this work, the problem is formed as an optimization problem related to spatiotemporal dimensions. A greedy algorithm is proposed to ensure that all queries have K, which is the coverage value.

Gong et al. designed a framework called KAWCR (K-Anonymity Without Cloaked Region) [Gong et al. 2010]. This method only needs the server to handle the incremental nearest-neighbor queries, and then it guarantees that a user cannot be distinguished from other $k-1$ users. Instead of sending all the points to the server, this method only sends the center of a k-anonymizing spatial region. The authors also proposed an anonymizer-side kNN algorithm to process the INN query for the LBS server. Then, the LBS 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. introduced an r-anonymity concept to blur the user's trajectory by preprocessing some similar trajectories R [Hwang et al. 2012]. This approach gave a time-obfuscation method that can break the list of time issuances of users' queries. It can prevent the attacker from learning the user's trajectory information including the direction. Moreover, this work considers the s segment together with k-anonymity to enhance the privacy level when a user sends out a query request. The key for this work is that when users are traveling, the anonymity server uses the time-obfuscated method to break the normal sequence of queries and sends them to the service provider randomly. The related information can be cached in the anonymity server and the query results can be sent back to the users. In Shin et al. [2010], Shin et al. tried to divide the whole request trajectory into many shorter trajectories in an optimal way. This work introduced the concept of trajectory K-anonymity, which means that a user's trajectory should be anonymized by at least $k-1$ other trajectories.

Regardless of effectiveness, efficiency, and the practicality of the previously mentioned solutions, K-anonymity is vulnerable to query sampling attacks, background

obtained attacks, and query tracking attacks. To eliminate the query sampling attack, the concept of reciprocity in Kalnis et al. [2007], which means a cloaking area not only contains at least k users but is also shared by at least k of these users, is restricted to create cloaking regions. To defend against background knowledge attack, Machanavajjhala et al. proposed the L-diversity principle, which requires that the sensitive attribute needs to have at least one well-represented value [Machanavajjhala et al. 2007]. To address query tracking attack, Chow and Mokbel introduced the memorization property for the cloaked query [Chow and Mokbel 2007].

4.1.2. Pseudonym-Based Techniques. Mix zone is one of the famous methods in this category. Liu et al. proposed a traffic-aware mix-zone scheme to set multiple mix zones along with the movement of mobile users [Liu et al. 2012]. By utilizing the graph theory, the problem becomes an optimization problem with certain constraints. The placement of mix zone is also affected by the traffic conditions. By computing the entropy, the best mix-zone locations are selected. In Palanisamy and Liu [2011], the authors also proposed a mix-zone approach for protecting users' location privacy with consideration of multiple factors. These factors include the zone's geometric shape, the user population's statistical behavior, and the spatiotemporal resolution of the location's exposure. By devising a suite of construction methods to build a mix zone, this work provides a lower bound on the anonymity level and a higher level on the attack resilience.

4.2. Trusted Third-Party-Free Techniques

4.2.1. Obfuscation-Based Techniques. Suzuki et al. tried to generate scatter locations closing to a user based on the former fake locations and the user's actual location [Suzuki et al. 2010]. According to the real road conditions, this work can adjust the process to get a better effect. Ma et al. explored an effective tool named Gaussian Process Regression (GPR) to preserve the trajectory privacy [Ma et al. 2011]. The idea is to reconstruct the trajectory information of mobile users by exposing selected locations. The GPR is used for inference of the possible direction for the trajectory, and then gives the estimated information by feeding the GPR tool the location samples. By carefully selecting the locations to be exposed, the exposure rate can be controlled within a certain level. This allows mobile users to send necessary information to the LBS server while controlling the trajectory privacy level. The drawback is that the service quality depends on the selected exposing locations.

Zhu and Cao designed a system to allow mobile users to report fake positions to the LBS server to get results [Zhu and Cao 2011]. In this system, mobile devices generate location proofs, and then the location proof server can be used by them to verifying the trust level. A mobile device can also be protected by changing the pseudonyms statistically. The location privacy model with user concentration evaluates the user privacy level time by time, and makes the decision to accept the request of a location proof. This approach focuses on the combination of location proof and location privacy to improve users' privacy level. In Ardagna et al. [2011], the authors devised some basic obfuscation operators to transform a location measurement by changing the center or radius. In addition, the basic operators can be used together to execute in a sequence for effectively protecting users' location. Feng et al. argued to generate fake paths along with users' true trajectories [Feng et al. 2012]. A noisy location is considered as a real location and will be reachable at the generated time with map information. A message containing the true position and noise data of a user should be sent to the server with two scheduling strategies. The first one is normal scheduling strategy, and the other is disordered scheduling strategy. Both are used to confuse adversaries.

4.2.2. Anonymity-Based Techniques. In Chow et al. [2011], Chow et al. proposed a spatial cloaking algorithm for LBS based on the peer-to-peer environment we mentioned in

the previous section. This algorithm has several functions including an information sharing scheme, a historical location scheme, and a cloaked adjustment scheme. For the first two schemes, 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 an area adjustment step. This algorithm satisfies K-anonymity as well as the privacy requirement of the least area specified by users. Jia and Zhang proposed two anonymity algorithms for LBS users in a mobile peer-to-peer environment to preserve location privacy [Jia and Zhang 2013]. The first algorithm generates grid areas, allows users to judge the areas, and then sends the grid area IDs instead of the real coordinates to the LBS server. The second algorithm allows a proxy peer to generate an anonymized spatial region for the query user. However, this work cannot resist the attack with respect to continuous queries.

Pingley et al. proposed a Context-Aware Privacy (CAP) scheme that has two components, named location perturbing and anonymous routing components, to eliminate the disclosure of private information [Pingley et al. 2009]. The perturbing component utilizes the Hilbert curve mapping to produce the perturbed location. The anonymous routing component tries to reduce users' network identities by relaying the LBS query to other nodes in an anonymous network. Nussbaum et al. introduced an (i, j)-privacy method, which uses the information of the travel time to distribute probabilities and to assign less likely traveled locations to users [Nussbaum et al. 2012]. Each user's location in one area should be 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. In this way, the anonymized degree of a user becomes higher along with an increase of the values i and j.

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

4.2.3. Protocol/Encryption-Based Techniques. Protocol means that all the participators in a system should follow the same set of rules. In protocol-based techniques for LBS, all the participators in a mobile system should collaborate and follow a protocol in order to protect the location and/or trajectory information of mobile users. Without the assistance from an anonymizer, an offline phase to map POI locations in the service regions into indexes is required in Ghinita et al. [2008]. During the query process, users encrypt the queries with redundant information, and then filter the redundancy in the response. A similar idea proposed in Riboni and Bettini [2012] is to simply generate dummy queries to confuse attackers. In Khoshgozaran et al. [2011], Khoshgozaran et al. introduced an approach to handle range and kNN queries based on the principle of Private Information Retrieval (PIR). This approach places trust on a secure coprocessor that is used for initiating PIR requests inside the LBS server. The range queries are handled by a sweeping algorithm. The kNN queries are privately evaluated by three algorithms, which are Hierarchical-, Progressive-, and Hilbert-based algorithms. This approach prevents the server from learning the user location information, and even the content of users' queries. By applying PIR, the user privacy can be guaranteed better than cloaking and anonymity-based techniques.

Buchanan et al. proposed an encryption approach to protect users' location and trajectory privacy based on private equality primitive. By creating a single encrypted table of identities, users can match their identities with their location privately by checking this table [Buchanan et al. 2013]. This protocol also allows users to privately select the interesting records provided by the server. Ardagna et al. proposed a protocol that allows the local users of a Wi-Fi network to form a group to defend a global adversary [Ardagna et al. 2013]. They also provide an incentive to stimulate the peers to cooperate in the process. The peers who participate in the protection process will be anonymously rewarded by a micropayment scheme. In addition, this protocol tries to minimize the probability of fake reward in hybrid scenarios.

4.2.4. Multiple Shares Techniques. The idea of location sharing is to divide the original position information into a set of imprecise location shares, which are distributed to many different LBS servers. As the result, a single LBS server cannot reveal the accurate location of a user. In Shin et al. [2010], Shin et al. proposed a share generation algorithm for protecting user location privacy in nontrusted systems. This algorithm reduces the location predictability so that it is harder for adversaries to obtain more accurate locations of users. With a map-aware position sharing approach, the size of obfuscation area that is defined by map information shares, can be adapted accordingly.

Xue et al. proposed a subtrajectory synthesis algorithm for predicting the destination of a LBS user [Xue et al. 2013]. This algorithm uses a Markov model to compute the posterior probability for an online given query trajectory. Then, the author tried to use a grid graph for abstracting the map and to use Bayer's rule to predict the destination. A user can remove some critical locations in the query trajectory so that the destination of the query trajectory cannot be predicted in a higher level than a given threshold with a probability. Wernke et al. devised a location sharing method to manage users' private location information. This method divides users' location data into location shares, and then distributes the location shares to different location servers that are used by multiple LBS providers [Wernke et al. 2013]. As a result, the malicious LBS providers can only discover some locations with lower degree of precision. This approach is powerful as it can defend against the maximum velocity attack as well as the mapping attack to some degree.

Shokri et al. introduced a method to store a user-side profile that is representative of the user's preference; and a subset of that profile on the server side [Shokri et al. 2009]. The users can contact each other and update their offline profiles by introducing a subset of their peers' profiles. The server receiving the aggregate profiles can report back to the users with a set of recommendations. Then, the user client removes redundant or irrelevant recommendations based on its privileged information. This work is further refined in Shokri et al. [2011] with the use of MobiCrowd. MobiCrowd establishes a mobile transparent proxy among nearby users through an ad hoc network. LBS queries are first checked against nearby devices by this proxy. Only if no nearby devices have the request cached, should the request be sent to the LBS provider.

4.2.5. Geometric-Based Techniques. In Li et al. [2013], Li et al. proposed a geometric approach to solve the location privacy problem for mobile users. The main idea is to send queries with multiple center and radii pairs to the application service provider instead of sending a user' real location and his/her real interested scanning radii. By devising a geometric computation algorithm, the query set can cover the user's original interested area. As a consequence, an adversary can only derive an anonymity zone from these multiple queries. The adversary knows that users are located in the anonymity zones without learning their exact positions. The drawbacks for this method are that it is still vulnerable to trajectory attack for continuous LBS users and it mainly focuses on POI applications. Guo et al. extended this method by proposing a pseudonym changing

process as well as a dummy generation mechanism to defend against trajectory privacy attacks [Guo et al. 2015]. By generating distributed anonymity zones and breaking the linkages among query updates on the fly, users' location and trajectory privacy leakage can be reduced dramatically.

4.3. Research Challenges and Directions in LBS

Although trusted thirty-party-based techniques guarantee strong privacy preservation for mobile users, third party itself forms a bottleneck of the system and becomes an ideal target for attackers. In addition, in the current LBS system architecture, there is no real deployment of such a third party. Researchers are paying less attention to this direction. On the other hand, third-party-free techniques have more advantages and flexibility, because users can directly interact with the LBS server without an intermediate party involved to handle user privacy. More research effort should be made in this direction. We list several challenges and directions in LBS as follows:

—The challenge is how to achieve the balance among service quality, energy consumption and privacy preservation for mobile devices in an optimal way. This requirement calls for more lightweight algorithms and protocols to achieve the privacy protection goal.
—Game Theory is a promising tool toward reducing overhead while achieving minimal energy consumption. Game Theory models mobile users as rational, self-interested entities that are willing to engage in the game in order to obtain their interested services and preferred privacy level.
—Geometric-based solution should also attract more attention from the community. This methodology has no effect on the existing system architecture, and does not need any collaboration with other users. Thus, the main advantage is its simplicity to be implemented in the system.
—Caching is another promising technique that can be used to reduce the number of queries sent to the LBS server, which leads to the reduction of energy consumption and communication overhead. The challenge is how to design an effective LBS system with caching capability to better preserve user privacy.
—K-anonymity, L-diversity, and T-closeness, concepts borrowed from database areas, should be paid special attention. These criteria are also very important in LBS that can be used to evaluate the performance of the proposed schemes.
—More complex privacy issues may arise along with the development of some mobile context-acquiring platforms like MobiCon in [Lee et al. 2012].

5. TRAJECTORY PRIVACY IN GeoSNs

GeoSN applications are becoming incredibly popular, due to the fast spread of online social networks, and the invention of real-time geocoding and geotagging technologies. The concept of a GeoSN is formally defined in the work of Gambs et al, as "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]. Famous GeoSNs, such as Facebook Places, Sina Weibo, Yelp, and Foursquare, developed easy-to-use interfaces for all users to share their location trajectory data with friends and families as well as the public. On the contrary, the privacy leakage during such sharing trajectory data behavior may lead to serious security threats [Borsboom et al. 2010].

In this section, we investigate trajectory privacy issues in the context of GeoSN and highlight related literature. First, we analyze privacy risk of the representative GeoSNs and briefly introduce the findings. Secondly, we study the TPP schemes proposed in the

literature. Finally, we summarize TPP challenges and discuss open research problems in GeoSN. 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].

5.1. Risk Analysis for Trajectory Privacy in GeoSNs

Trajectory privacy issues are not addressed at the beginning by most GeoSN providers. Gambs et al. conducted a comparative privacy leakage analysis of several popular GeoSNs, including Qype, Twitter, La Ruche, and Foursquare [Gambs et al. 2011]. Based on the criteria of user registration profile, pseudonyms versus real identities, and information open to others and privacy settings, the authors compare those GeoSNs in terms of privacy leakage issues. The conclusion is that most of the popular GeoSNs do not have many privacy features integrated in their products.

The privacy risk of trajectory data sharing could come from three different sources, including (1) users' profiles when registering social networks, (2) location queries and check-ins, and (3) multimedia tagging and event posting.

By analyzing the datasets collected from Google+, Foursquare, and Twitter, Pontes et al. conclude that without location inferring techniques, the vast majority of users of Foursquare provided valid home city locations in the corresponding venue attributes [Pontes et al. 2012a]. Similarly, a large number of users are found to provide full addresses in their residential venue profiles [Pontes et al. 2012b]. In order to infer possible residential addresses of GeoSN users, two groups of researchers also provide the location inferring schemes by analyzing the statistics and frequency of geolocated data posts and check-ins. As a result, 78% of the home cities of the analyzed users can be correctly and easily inferred within 50 kilometers of distance. By modeling and comparing the access control schemes for user's check-ins in several famous GeoSNs, Jin et al. conclude that for user's check-in information components, there are no fine-grained access control mechanisms [Jin et al. 2012]. Trajectory privacy of GeoSNs is also affected by colocation tagging, which creates more vulnerabilities. To estimate a microblog (such as Twitter) user's location only depending on his/her publicly available posts, Cheng et al. [2013] proposed a probabilistic framework overcoming the absence of granular location data in the posts. The authors not only utilized the geolocated information posts, but also developed a classifier that can be used to identify words with a local geographic scope in status updates, to discover the association of certain locations with certain words or phrases. For each user, the proposed framework provides k estimated cities with a descending order of possibility. As a result, on average, 51% of randomly selected microblog users are located within 100 miles of their actual location. All the aforementioned insights indicate that trajectory privacy risk and leakage cannot be ignored in GeoSN applications, and it is one of the critical issues that needs to be addressed in the development of GeoSN.

5.2. Trajectory Privacy Techniques in GeoSNs

5.2.1. Trajectory Obfuscation. Trajectory privacy issues in GeoSNs are more complex compared with trajectory privacy in other LBS applications. There are only limited works that have been proposed for solving this issue. One of the major solutions is to apply trajectory obfuscation technique, such as space transformation and spatiotemporal cloaking.

Cuellar et al. first formally defined a number of notions for evaluating a location obfuscation function in Cuellar et al. [2012]. The authors also formalized the concept of indistinguishability of location obfuscation functions, which requires that a user's actual position should be indistinguishable from a set of possible locations, for example, an obfuscation zone that includes noise and the real location. Indistinguishability

of obfuscation functions needs to be satisfied under different scenarios: (1) when an attacker queries a user's location at regular intervals, the attacker should not be able to increase the precision of his/her knowledge on the real position up to the predefined threshold chosen by the user; (2) an adversary cannot deduce that the user revisits a certain position; and (3) from the user's original location and location updates in route, an adversary should not be able to determine the destination. In addition, the obfuscation zone needs to be constant for all points contained within it with such indistinguishable properties. For more restrictive TPP protection, the obfuscation functions need to prevent an adversary from determining the users' current and past routes as well. However, the authors only defined a concept of indistinguishability; they did not consider the privacy leakage in social relations and interactions among users, which is highly possible to be explored by the attackers to infer users' location.

On the other hand, Freni et al. deployed a centralized trusted entity that can be used to process a user's original resource. Before publishing it to the GeoSN, the process may involve other users to ensure that it complies with the privacy preferences of involved users [Freni et al. 2010]. The authors introduce the notion of Minimal Uncertainty Region (MUR) as a spatiotemporal region for which an adversary cannot infer any internal point as the users' actual location. In its location cloaking system, the preprocessing module called Single Resource Generalization (SRG) is designed to retrieve the privacy preferences of all the involved users and the corresponding MUR. The output of SRG is a generalized resource called srg that covers all the users' MURs. The cloaking module applies to spatial generalization and/or temporal generalization (depending on whether the service attribute is time sensitive) algorithms to generalize the preprocessed generalized resource srg if the disclosure of srg introduces privacy violations. Then, the next process is the publisher module. By postponing the publication of the resources if necessary, the publisher module will compile the user's absence privacy preferences. This process is to improve users' privacy level in the situation that the adversary may infer a user's absence by utilizing the maximum velocity and current MUR. It is highly possible for current GeoSN service providers to adopt such a system on top of their system architectures. However, there is an issue with this system, which is the designation of the centralized trusted entity.

Under the assumption that the GeoSN service providers or other intermediaries are untrusted, Puttaswamy et al. proposed LocX, a user-specific and distance preserving space transformation algorithm that focuses on dealing with point queries and Nnearest-Neighbor (NN) queries [Puttaswamy et al. 2014]. The idea is to let users encrypt their location data and store them in the proxy for later location query processes by sharing and using secret keys with their friends. There are two pairs in the encryption mapping: (1) L2I, which is a mapping from the transformed location to an encrypted index, and (2) I2D, which is a mapping from the encrypted index to the encrypted location data. Two modules/servers in the proxy are responsible for storing the two pairs. When a query referencing a certain POI is submitted by a user to the proxy, the query will be in the form of transformed location data encrypted by symmetric keys. The proxy will return all L2I pairs that are in the user's query. The user needs to decrypt the index and queries the pair of I2D. Then, the encrypted location data pair will be returned by the proxy with the corresponding index. The drawback for LocX is that it lacks of evaluation of computation power consumption for running on mobile devices, even if the authors claimed the cost is low. Moreover, it could be difficult to realize the symmetric key distribution and rekeying management in practical GeoSNs.

Masoumzadeh et al. proposed a k-anonymity-based location cloaking algorithm with the focus on anonymizing GeoSN datasets [Masoumzadeh and Joshi 2011]. The authors try to solve the issue that an attacker may reidentify a user by exploring the location information revealed by social connections. In order to guarantee privacy of users'

location and identities, the datasets should satisfy L2 k-anonymity, which means for each user, there is at least $k-1$ other users assigned the same location data, and the user's adjacent users are also assigned the same location information in the social network as other user's adjacent users too. At the beginning, the algorithm considers each user as a separate cluster that centers at his/her location. In order to select the minimum pair to form a new cluster, the distance between every pair of clusters will be computed in the latter iteration. The algorithm stops when the cloaking region satisfies L2k-anonymity. However, in some cases such as when a user is traveling out of town, the conditions of L2k-anonymity will not be satisfied due to the user's uniqueness and the algorithm will fail to work. This work also focuses on the anonymization of the GeoSN datasets. There are still some difficulties in applying this algorithm into in-network computing, such as the problem of retrieving the location of other users to calculate the distance. In sum, L2k-anonymity has great potential to resolve the trajectory privacy issue in GeoSN where social relation is a critical factor.

5.2.2. Context Analysis Technique. Due to the rich semantic contents during social interactions among users, context analysis is a particularly important tool for security and privacy preservation in GeoSN applications. In Riboni and Bettini [2012], Riboni et al. conducted an initial investigation to prevent the learning of the user's POI preferences by other users that may lead to privacy leakage. The authors apply a PINQ [McSherry 2009] query engine to achieve ϵ-differential privacy by injecting random noise to extract statistics about personal preferences for POIs. Instead of submitting the accurate location, users submit the queries with a spatial granule in which they are located to protect trajectory privacy. However, how to define the granularity level of the granule is not addressed in detail to guarantee both service accuracy and trajectory privacy.

In Jagtap et al. [2011], Jagtap et al. proposed a context-aware access control scheme. The authors adopt Web Ontology Language to capture users' characteristics, including feeds from social networks they use, the inferred activities in which they are engaged, the location and surroundings, and the presence of other devices and people. The reasoning engine is responsible for handling queries and performing reasoning for access control decisions. The privacy control module is supported by the two mentioned components to enforce access control of the query process to the protected data. This module is embedded on both server and client sides for checking the privilege to access protected data for peer-to-server queries and peer-to-peer queries. Before applying this scheme, there are several issues that need to be addressed: (1) the energy consumption at the client side is not neglectful; (2) the server might be malicious; and (3) the privacy control module may need more protection for security considerations, because of the fact that it collects the social profiles and preferences of all users.

5.2.3. Cryptography Technique. In the security and privacy area, cryptography is a fundamental technique and direct solution. Hashing methods and symmetric key encryption are commonly used in TPP in proximity services in GeoSNs. However, the existing methods for proximity services lacks of generality to be applied in other GeoSN applications, because of the fact that proximity service is only a particular application of GeoSNs that mainly involves location coordinates manipulation and distance computation. Thus, we survey a limited number of related works here. More explicit literatures are surveyed in Amir et al. [2007] and Mascetti et al. [2011].

In Mascetti et al. [2011], Mascetti et al. proposed two protocols, named C-Hide&Seek and C-Hide&Hash, to protect a user's location privacy from untrusted service providers and other users when the user submits a proximity service request. In the first protocol, the service provider replies with a message that contains the latest encrypted location updates of each friend of the requester. The message can be decrypted by the requester using the symmetric keys that are shared with his/her friends. To prevent

an adversary from learning that the targeted user is crossing the boundary between two granules by observing the time stamp of the location updates, the location of the user is only updated after a certain interval and identified by an interval index. The major difference between C-Hide&Hash and C-Hide&Seek is that the requester will check if any of his/her friend's location falls in a set of granules provided by him/her. In this situation, the locating granules of other users are protected from the requester. The authors provided a complete set of privacy preservation protocols in proximity service with the consideration of untrusted service providers and curious users. The guaranteed location privacy has been theoretically approved. However, there are several open problems for this work: (1) how to properly define the update interval is not addressed; (2) the protocols might not be applicable in time sensitive services because of the improper update interval; and (3) how to solve the key distribution issue before practical implementations remains a question as most other methods using symmetric keys. Under similar system assumptions, Li et al. also applied a symmetric key hashing mechanism to transform location data in the proximity service query process [Li et al. 2013]. The authors utilized optimal grid overlay and multilevel grids to increase the accuracy of proximity detection.

Provost et al. suggests applying many-to-one or one-to-one hashing to hash users' location and identities information [Provost et al. 2012]. Their work focuses on exploring the similarity of GeoSN behaviors for ad targeting like-minded individuals. In Carbunar et al. [2014], Carbunar et al. proposed a scheme that builds users' location-centric profiles in a correct and private manner. This work prompts the dishonesty issue in GeoSNs such as Foursquare and Yelp, where users may cheat their check-ins to gain benefits, as well as the privacy violation issue when venues collect users' location data for building their profiles. To prove a user's physical presence at the venue, this work installs a device at each venue to initiate a challenge, as well as authorizes a time-stamped token encrypted by its secret key to check-in users. The venue only records the statistics of the collected profiles. The way is to increase the counter by one on a certain dimension and the corresponding range, when a user's profile value falls in it. These two works are inspiring for the inherent design of GeoSNs with trajectory privacy features, even if they lack details of TPP mechanisms.

5.2.4. Statistical Modeling and Privacy by Design. Recently, statistical modeling technique has become 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 pseudorandom numbers that 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. Features of Trajectory Privacy in GeoSNs

Trajectory privacy is particularly important to GenSN users because of the fact that trajectory data available from GeoSNs is always associated with users' social behaviors, and such behaviors can be easily identified from public or semipublic resources, such as open social events and interactions among users, urban patterns [Ferrari et al. 2011]. The existing trajectory privacy techniques in LBS and databases may not be applicable to GenSNs due to the unique features that GeoSN applications own [Vicente et al. 2011]: (1) some applications, such as proximity services, require "real-time" response; (2) some applications require exact locations with high granularity, such as check-ins; (3) in some situations, users could be tagged passively, such as in colocation check-ins and photo posts; and (4) users could be reidentified through linking available background knowledge and external resources.

Additionally, we would like to mention two important aspects: (1) trajectory privacy leakage could result from the massive interactions among users. Users might reveal his/her daily routines or trip schedules during the interaction with friends, regardless of passive tagging by other people. The access to such interactions is always ignored in general by users even if the involved friends or group members are trustworthy; (2) it is highly possible for social network users to join more than one GeoSN. Thus, the collection of the same user's profiles from multiple GeoSN sites might give attackers a clear "picture" for reidentification of the user. In spite of the fact that a user may set privacy preferences carefully for each GeoSN application, it is very likely for an adversary to link multiple GeoSN accounts for the same user and extract more characteristics and knowledge from the linkage.

5.4. Research Challenges and Directions in GeoSNs

Compared with trajectory privacy in LBS, trajectory privacy problems in GeoSNs are much more challenging, due to the involved uncontrolled social elements in the system. In addition to user identity privacy and location privacy that are commonly considered in LBS, we need to consider colocation privacy and absence privacy in GeoSNs for a better TPP solution. Fine-grained access control mechanisms are needed to address the absence and colocation privacy problems, and to defend inference attacks. However, the open connection characteristic of GeoSNs and large volume of social interactions among users make the problem even harder to solve. We list several research challenges and directions in GeoSNs as follows:

—How to carefully control the exposure of the connection graph among GeoSN users to the public or semipublic remains a challenge. The social connection graph combined with the interactions among users contains much more sensitive information that could be captured by adversaries.
—TPP needs to consider the relationship between users' available traces and their social patterns. By participating in normal social activities organized online using GeoSNs, users' certain social patterns in corresponding environments can be formed and later can be discovered by adversaries within a specific time period. At the same time, the location check-ins along with the social activities form users' trace information. Thus, the attacker could infer more private information of the target user from his/her available traces together with the social pattern.
—TPP also needs to consider the privacy leakage when connecting different GeoSN accounts for the same user, as well as connecting other online service site activities for the same user. This is a serious problem that has been ignored in existing literature. Many users may use the same identity for registering GeoSNs and other

online service sites, such as the same phone numbers and email accounts, etc. It is highly possible for the adversary to track the users' activities on these sites with the same registration information, and to infer their private information; particularly facilitated by effective social network providers, like Facebook, who could track a user's online activities even if the user logs out of the sites. Famous search engines like Google and Bing also have the ability to collect user data from multiple sites in a cost-efficient way. It is suggested that users should use different information to register different GeoSNs and other online service sites. In addition, lawful policies should be called for prevention of powerful internet companies from tracking users' online activities.

—Moreover, different GeoSN service providers may have different access control and privacy policies. It is difficult to develop a unified effective TPP mechanism that is suitable for all of them. This can only be possible if the service providers are collaborating with each other, which is not realistic so far.

—TPP needs to take the connections between users' available traces and the public geographic map into consideration. An adversary could learn more information from the public geographic map with available traces, and then launch an attack. This is called a map-mapping attack. This is not a unique issue for TPP in GeoSNs but a consistent problem for many other applications. Nevertheless, the geographic map may contain rich social context in GeoSNs. Combining social context with background knowledge, the adversary may distinguish the targeted user from other users who have similar available trajectories. For instance, on Saturday morning, it is likely that an artist is going to a museum and a religious person is going to the church, if the museum and the church are located close to each other. The inference of a user's private trajectory could be improved by the combination of the social context and public map data. CAP mechanism could be a possible direction for solving this issue.

6. CONCLUSION

Location and trajectory privacy concerns hinder the potential success of location-aware applications. In this article, we surveyed location and TPP techniques in the context of stationary WSNs, mobile WSNs, and LBS as well as GeoSNs. In each of those critical applications, we summarized the main works and developed a clean category. We also pointed out the research challenges based on their own characteristics and structures. Finally, we gave some possible research directions for each application with the purpose to stimulate more researchers and developers to participate in this fascinating area.

REFERENCES

Basel Alomair, Andrew Clark, Jorge Cuellar, and Radha Poovendran. 2013. Toward a statistical framework for source anonymity in sensor networks. *IEEE Transactions on Mobile Computing* 12, 2 (2013), 248–260. DOI: http://dx.doi.org/10.1109/TMC.2011.267

Arnon Amir, Alon Efrat, Jussi Myllymaki, Lingeshwaran Palaniappan, and Kevin Wampler. 2007. Buddy tracking—Efficient proximity detection among mobile friends. *Pervasive and Mobile Computing* 3, 5 (Oct. 2007), 489–511. DOI: http://dx.doi.org/10.1016/j.pmcj.2006.12.002

Claudio A. Ardagna, Marco Cremonini, Sabrina De Capitani di Vimercati, and Pierangela Samarati. 2011. An obfuscation-based approach for protecting location privacy. *IEEE Transactions on Dependable and Secure Computing* 8, 1 (Jan. 2011), 13–27. DOI: http://dx.doi.org/10.1109/TDSC.2009.25

Claudio A. Ardagna, Sushil Jajodia, Pierangela Samarati, and Angelos Stavrou. 2013. Providing users' anonymity in mobile hybrid networks. *ACM Transactions on Internet Technology* 12, 3, Article 7 (May 2013), 33 pages. DOI: http://doi.acm.org/10.1145/2461321.2461322

Kemal Bicakci, Ibrahim Ethem Bagci, and Bulent Tavli. 2011. Lifetime bounds of wireless sensor networks preserving perfect sink unobservability. *IEEE Communications Letters* 15, 2 (Feb. 2011), 205–207. DOI: http://dx.doi.org/10.1109/LCOMM.2011.010311.101885

Barry Borsboom, Boy van Amstel, and Frank Groeneveld. 2010. Please Rob Me. Retrieved December 9, 2013 from http://pleaserobme.com/.

William J. Buchanan, Zbigniew Kwecka, and Elias Ekonomou. 2013. A privacy preserving method using privacy enhancing techniques for location based services. *Mobile Networks and Applications* 18, 5 (Oct. 2013), 728–737.

Bogdan Carbunar, Mahmudur Rahman, Jaime Ballesteros, Naphtali Rishe, and Athanasios V. Vasilakos. 2014. ProfilR: Toward preserving privacy and functionality in geosocial networks. *IEEE Transactions on Information Forensics and Security* 9, 4 (April 2014), 709–718. DOI:http://dx.doi.org/10.1109/TIFS.2014.2307697

Bogdan Carbunar, Mahmudur Rahman, Niki Pissinou, and Athanasios V. Vasilakos. 2013. A survey of privacy vulnerabilities and defenses in geosocial networks. *IEEE Communications Magazine* 51, 11 (Nov. 2013), 114–119. DOI:http://dx.doi.org/10.1109/MCOM.2013.6658662

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* 2012, Article 648058 (2012), 16 pages. DOI:http://dx.doi.org/10.1155/2012/648058

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)*. Springer-Verlag, Berlin, 190–201.

Juan Chen, Hongli Zhang, Xiaojiang Du, Binxing Fang, and Liu Yan. 2014. Designing robust routing protocols to protect base stations in wireless sensor networks. *Wireless Communications and Mobile Computing* 14, 17 (Dec. 2014), 1613–1626. DOI:10.1002/wcm.2300

Zhiyuan Cheng, James Caverlee, and Kyumin Lee. 2013. A content-driven framework for geolocating microblog users. *ACM Transactions on Intelligent Systems and Technology* 4, 1, Article 2 (Jan. 2013), 27 pages. DOI:http://doi.acm.org/10.1145/2414425.2414427

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)*. Springer-Verlag, Berlin, 258–273.

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:http://dx.doi.org/10.1007/s10707-009-0099-y

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, 1463–1469. DOI:http://doi.acm.org/10.1145/2245276.2232010

Maria Damiani, Elisa Bertino, and Claudio Silvestri. 2008. *PROBE: An Obfuscation System for the Protection of Sensitive Location Information in LBS.* Purdue Technical Report TR2001-145, CERIAS.

Jing Deng, Richard Han, and Shivakant Mishra. 2005. Countermeasures against traffic analysis attacks in wireless sensor networks. In *Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*. IEEE Computer Society, 113–126. DOI:http://dx.doi.org/10.1109/SECURECOMM.2005.16

Jing Deng, Richard Han, and Shivakant Mishra. 2006. Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks. *Pervasive and Mobile Computing* 2, 2 (April 2006), 159–186. DOI:http://dx.doi.org/10.1016/j.pmcj.2005.12.003

Mohammad Razvi Doomun and Krishnaraj Madhavjee Sunjiv Soyjaudah. 2010. Route extrapolation for source and destination camouflage in wireless ad hoc networks. *IEEE International Conference on Computer Communications Networks (ICCCN'10)*. IEEE Press, 1–7. DOI:http://dx.doi.org/10.1109/ICCCN.2010.5560088

Yousef Ebrahimi and Mohamed Younis. 2011. Using deceptive packets to increase base-station anonymity in wireless sensor network. In *7th International Wireless Communications and Mobile Computing Conference (IWCMC'11)*. IEEE Press, 842–847. DOI:http://dx.doi.org/10.1109/IWCMC.2011.5982656

Yunxia Feng, Peng Liu, and Jianhui Zhang. 2012. A mobile terminal based trajectory preserving strategy for continuous querying LBS users. In *IEEE 8th International Conference on Distributed Computing in Sensor Systems (DCOSS'12)*. IEEE Press, 92–98. DOI:http://dx.doi.org/10.1109/DCOSS.2012.33

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, 9–16. DOI:http://doi.acm.org/10.1145/2063212.2063226

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, 309–318. DOI:http://doi.acm.org/10.1145/1871437.1871480

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, 1577–1585. DOI:http://dx.doi.org/10.1109/INFCOM.2010.5461975

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, 33–40. DOI:http://doi.acm.org/10.1145/2071880.2071887

Buğra Gedik and Ling Liu. 2008. Protecting location privacy with personalized k-Anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing* 7, 1 (Jan. 2008), 1–18. DOI:http://dx.doi.org/10.1109/TMC.2007.1062

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, 121–132. DOI:http://doi.acm.org/10.1145/1376616.1376631

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)*. Springer-Verlag, Berlin, 221–238.

Gabriel Ghinita. 2009. Private queries and trajectory anonymization: A dual perspective on location privacy. *Transactions on Data Privacy* 2, 1 (April 2009), 3–19.

Zhenqiang Gong, Guang-Zhong Sun, and Xing Xie. 2010. Protecting privacy in location-based services using K-Anonymity without cloaked region. In *2010 11th International Conference on Mobile Data Management (MDM'10)*. IEEE Press, 366–371. DOI:http://dx.doi.org/10.1109/MDM.2010.33

Marco Gruteser and Dirk Grunwald. 2003. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the First International Conference on Mobile Systems, Applications, and Services (MOBISYS'03)*. ACM, New York, NY, 31–42. DOI:http://doi.acm.org/10.1145/1066116.1189037

Mingming Guo, Niki Pissinou, and S. S. Iyengar. 2015. Pseudonym-based anonymity zone generation for mobile service with strong adversary model. In *Proceedings of the 12th Annual IEEE Consumer Communications and Networking Conference (CCNC'15)*, IEEE Press, 335–340. DOI:http://dx.doi.org/10.1109/CCNC.2015.7157998

Jianguo Hao, Weidong Liu, and Yiqi Dai. 2010. A controllable privacy protection framework in position-based routing for suspicious MANETs. *IET International Conference on Wireless Sensor Network (IET-WSN'10)*. 291–296. DOI:http://dx.doi.org/10.1049/cp.2010.1069

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, 208–215. DOI:http://dx.doi.org/10.1109/I-SPAN.2012.35

Pramod Jagtap, Anupam Joshi, Tim Finin, and Laura Zavala. 2011. Preserving privacy in context-aware systems. In *Proceedings of the 5th IEEE International Conference on Semantic Computing (ICSC'11)*. IEEE Press, 149–153. DOI:http://dx.doi.org/10.1109/ICSC.2011.87

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, 760–768. DOI:http://dx.doi.org/10.1109/TrustCom.2012.281

Jinying Jia and Fengli Zhang. 2013. Twice anonymity algorithm for LBS in mobile P2P environment. *Journal of Computational Information Systems* 9, 9 (2013), 3715–3722.

Ying Jian, Shigang Chen, Zhan Zhang and Liang Zhang. 2007. Protecting receiver-location privacy in wireless sensor networks. In *Proceedings of the 26th Conference on Computer Communications (INFOCOM'07)*. IEEE Press, 1955–1963. DOI:http://dx.doi.org/10.1109/INFCOM.2007.227

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, 25–32. DOI:http://doi.acm.org/10.1145/2382416.2382428

Xinyu Jin, Niki Pissinou, Cody Chesneau, Sitthapon Pumpichet, and Deng Pan. 2012. Hiding trajectory on the fly. In *Proceedings of the IEEE International Conference on Communications (ICC'12)*. IEEE Press, 403–407. DOI:http://dx.doi.org/10.1109/ICC.2012.6364508

Panos Kalnis, Gabriel Ghinita, Kyriakos Mouratidis, and Dimitris Papadias. 2007. Preventing location-based identity inference in anonymous spatial queries. *IEEE Transactions on Knowledge and Data Engineering* 19, 12 (Dec. 2007), 1719–1733. DOI:http://dx.doi.org/10.1109/TKDE.2007.190662

Pandurang Kamat, Wenyuan Xu, Wade Trappe, and Yanyong Zhang. 2007. Temporal privacy in wireless sensor networks. In *27th International Conference on Distributed Computing Systems (ICDCS'07)*. IEEE Press, 23–23. DOI:http://dx.doi.org/10.1109/ICDCS.2007.146

Pandurang Kamat, Yanyong Zhang, Wade Trappe, and Celal Ozturk. 2005. Enhancing source-location privacy in sensor network routing. *25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, IEEE Press, 599–608. DOI:http://dx.doi.org/10.1109/ICDCS.2005.31

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, 603–608. DOI:http://dx.doi.org/10.1109/ICC.2009.5199372

Rajgopal Kannan, Sudipta Sarangi, and S. SitharamaIyengar. 2004. Sensor-centric energy-constrained reliable query routing for wireless sensor networks. *Journal of Parallel and Distributed Computing* 64, 7 (July 2004), 839–852. DOI:http://dx.doi.org/10.1016/j.jpdc.2004.03.010

Ali Khoshgozaran, Cyrus Shahabi, and Houtan Shirani-Mehr. 2011. Location privacy: Going beyond K-anonymity, cloaking and anonymizers. *Knowledge and Information Syste*ms 26, 3 (March 2011), 435–465. DOI:http://dx.doi.org/10.1007/s10115-010-0286-z

Youngki Lee, S. S. Iyengar, Chulhong Min, Younghyun Ju, Seungwoo Kang, Taiwoo Park, Jinwon Lee, Yunseok Rhee, and Junehwa Song. 2012. MobiCon: A mobile context-monitoring platform. *Communications of the ACM* 55, 3 (March 2012), 54–65. DOI:http://dx.doi.org/10.1145/2093548.2093567

Hong Ping Li, Haibo Hu, and Jianliang Xu. 2013. Nearby friend alert: Location anonymity in mobile geosocial networks. *IEEE Pervasive Computing* 12, 4 (Oct. 2013), 62–70. DOI:http://dx.doi.org/10.1109/MPRV.2012.82

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 2660–2668. DOI:http://dx.doi.org/10.1109/INFCOM.2010.5462096

Yun Li, Jian Ren, and Jie Wu. 2012. Quantitative measurement and design of source-location privacy schemes for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems* 23, 7 (July 2012), 1302–1311. DOI:http://dx.doi.org/10.1109/TPDS.2011.260

Ming Li, Sergio Salinas, Arun Thapa, and Pan Li. 2013. n-CD: A geometric approach to preserving location privacy in location-based services. In *Proceedings of the 30th Conference on Information Communications (INFOCOM'13)*. IEEE Press, 3012–3020. DOI:http://dx.doi.org/10.1109/INFCOM.2013.6567113

Xinfeng Li, Xiaoyuan Wang, Nan Zheng, Zhiguo Wan, and Ming Gu. 2009. Enhanced location privacy protection of base station in wireless sensor networks. In *Proceedings of the 2009 5th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN'09)*. IEEE Computer Society, 457–464. DOI:http://dx.doi.org/10.1109/MSN.2009.19

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 Networks* 7, 8 (Nov. 2009), 1501–1514. DOI:http://dx.doi.org/10.1016/j.adhoc.2009.04.009

Xiaohui Liang, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. 2010. Message authentication with non-transferability for location privacy in mobile ad hoc networks. In *2010 IEEE Global Telecommunications Conference (GLOBECOM'10)*. IEEE Press, 1–5. DOI:http://dx.doi.org/10.1109/GLOCOM.2010.5683524

Leron Lightfoot, Yun Li, and Jian Ren. 2010. Preserving source-location privacy in wireless sensor network using STaR routing. In *2010 IEEE Global Telecommunications Conference (GLOBECOM'11)*. IEEE Press, 1–5. DOI:http://dx.doi.org/10.1109/WoWMoM.2011.5986491

Xinxin Liu, Kaikai Liu, Linke Guo, Xiaolin Li, and Yuguang Fang. 2013. A game-theoretic approach for achieving K-Anonymity in location based services. In *Proceedings of the 30th Conference on Information Communications (INFOCOM'13)*. IEEE Press, 2985–2993. DOI:http://dx.doi.org/10.1109/INFCOM.2013.6567110

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

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 8th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS'11)*. IEEE Computer Society, 7–12. DOI:http://dx.doi.org/10.1109/MASS.2011.12

Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. 2007. L-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data* 1, 1, Article 3 (March 2007). DOI:http://doi.acm.org/10.1145/1217299.1217302

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 Transactions*

on Parallel and Distributed Systems 23, 10 (Oct. 2012), 1805–1818. DOI:http://dx.doi.org/10.1109/TPDS.2011.302

Sergio Mascetti, Dario Freni, Claudio Bettini, X. Sean Wang, and Sushil Jajodia. 2011. Privacy in geo-social networks: Proximity notification with untrusted service providers and curious buddies. *The International Journal on Very Large Data Bases (VLDB)* 20, 4 (Aug. 2011), 541–566.

Amirreza Masoumzadeh and James B. D. Joshi. 2011. An alternative approach to k-anonymity for location-based services. *Procedia Computer Science* 5 (2011), 522–530. DOI:10.1016/j.procs.2011.07.068

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, 25–32. DOI:http://doi.acm.org/10.1145/2071880.2071886

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, 19–30. DOI:http://doi.acm.org/10.1145/1559845.1559850

Kiran Mehta, Donggang Liu, and Matthew Wright. 2007. Location privacy in sensor networks against a global eavesdropper. In *2007 IEEE International Conference on Network Protocols*. IEEE Press, 314–323. DOI:http://dx.doi.org/10.1109/ICNP.2007.4375862

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 (Feb. 2012), 320–336. DOI:http://dx.doi.org/10.1109/TMC.2011.32

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)*. ACM, New York, NY, 763–774.

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, 116–123. DOI:http://doi.acm.org/10.1145/1641804.1641825

Edith C.-H. Ngai. 2010. On providing sink anonymity for wireless sensor networks. *Security and Communication Networks*. DOI:10.1002/sec. 245.

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 3rd ACM SIGSPATIAL International Workshop on GeoStreaming (IWGS'12)*. ACM, New York, NY, 58–67. DOI:http://doi.acm.org/10.1145/2442968.2442976

Stefano Ortolani, Mauro Conti, Bruno Crispo, and Roberto Di Pietro. 2011. Events privacy in WSNs: A new model and its application. In *2011 IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM'11)*. IEEE Press, 1–9. DOI:http://dx.doi.org/10.1109/WoWMoM.2011.5986491

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, 494–505. DOI:10.1109/ICDE.2011.5767898http://dx.doi.org/10.1109/ICDE.2011.5767898

Steffen Peter, Peter Langendorfer, and Krzysztof Piotrowski. 2008. Public key cryptography empowered smart dust is affordable. *International Journal of Sensor Networks* 4, 1/2 (July 2008), 130–143. DOI:http://dx.doi.org/10.1504/IJSNET.2008.019258

Sarah Pidcock and Urs Hengartner. 2013. Zerosquare: A privacy-friendly location hub for geosocial applications. In *Proceedings of IEEE Mobile Security Technologies Workshop (MoST'13)*. IEEE Press, 1–10.

Aniket Pingley, Wei Yu, Nan Zhang, Xinwen Fu, and Wei Zhao. 2009. CAP: A context-aware privacy protection system for location-based services. In *Proceedings of the 29th IEEE International Conference on Distributed Computing Systems (ICDCS'09)*. IEEE Press, 49–57. DOI:http://dx.doi.org/10.1109/ICDCS.2009.62

Kanthakumar Pongaliur and Li Xiao. 2011. Maintaining source privacy under eavesdropping and node compromise attacks. In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM'11)*. IEEE Press, 1656–1664. DOI:http://dx.doi.org/10.1109/INFCOM.2011.5934959

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, 571–578. DOI:http://dx.doi.org/10.1109/ICDMW.2012.106

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, 898–905. DOI:http://doi.acm.org/10.1145/2370216.2370419

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, 46–51. DOI:http://doi.acm.org/10.1145/1503402.1503412

Nayot Poolsappasit and Indrakshi Ray. 2009. Towards achieving personalized privacy for location-based services. *Transactions on Data Privacy* 2, 1 (April 2009), 77–99.

Foster Provost, David Martens, and Alan Murray. 2011. Geo-social network targeting for privacy-friendly mobile advertising: Position paper. (June 2011). Retrieved July 20, 2013 from http://archive.nyu.edu/bitstream/2451/31279/2/mobile_targeting_position.pdf.

Foster Provost, David Martens, and Alan Murray. 2012. Finding similar users with a privacy-friendly geo-social design. (October 2012). Retrieved October 2, 2013 from http://www.everyscreenmedia.com/everyscreenmedia/wpcontent/uploads/2012/10/Finding_Similar_Users.pdf.

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 (Jan. 2014), 159–173. DOI:http://dx.doi.org/10.1109/TMC.2012.247

Jian Ren and Di Tang. 2011. Combining source-location privacy and routing efficiency in wireless sensor networks. In *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'11)*. IEEE Press, 1–5.

Daniele Riboni and Claudio Bettini. 2012. Private context-aware recommendation of points of interest: An initial investigation. In *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. IEEE Press, 584–589. DOI:http://dx.doi.org/ 10.1109/PerComW.2012.6197582

Min Shao, Yi Yang, Sencun Zhu, and Guohong Cao. 2008. Towards statistically strong source anonymity for sensor networks. In *Proceedings of the 27th Conference on Computer Communications (INFOCOM'08)*. IEEE Press, 51–55. DOI:http://dx.doi.org/ 10.1109/INFOCOM.2008.19

Heechang Shin, Jaideep Vaidya, Vijayalakshmi Atluri, and Sungyong Choi. 2010. Ensuring privacy and security for LBS through trajectory partitioning. In *Proceedings of the 2010 11th International Conference on Mobile Data Management (MDM'10)*. IEEE Computer Society, 224–226. DOI:http://dx.doi.org/10.1109/MDM.2010.29

Reza Shokri, Panos Papadimitratos, George Theodorakopoulos, and Jean-Pierre Hubau. 2011. Collaborative location privacy. In *Proceedings of the IEEE 8th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS'11)*. IEEE Press, 500–509. DOI:http://dx.doi.org/10.1109/MASS.2011.55

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 3rd ACM Conference on Recommender Systems (RecSys'09)*. ACM, New York, NY, 157–164. DOI:http://doi.acm.org/10.1145/1639714.1639741

Sejun Song, Hyungbae Park, and Baek-Young Choi. 2011. STEP: Source traceability elimination for privacy against global attackers in sensor networks. In *Proceedings of the 20th International Conference on Computer Communications and Networks* (*ICCCN'11*). IEEE Press, 1–6. DOI:http://dx.doi.org/10.1109/ICCCN.2011.6005916

Petros Spachos, Liang Song, Francis M. Bui, and Dimitrios 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, 815–820. DOI:http://dx.doi.org/10.1109/ISCC.2011.5983942

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, 398–401. DOI:10.1145/1869790.1869846 http://doi.acm.org/10.1145/1869790.1869846

Latanya Sweeney. 2002. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10, 5 (Oct. 2002), 557–570. DOI:http://dx.doi.org/10.1142/S0218488502001648

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:http://dx.doi.org/10.1109/MIC.2011.29

Yu Wang, Dingbang Xu, Xiao He, Chao Zhang, Fan Li, and Bin Xu. 2012. L2P2: Location-aware location privacy protection for location-based services. In *Proceedings of the 29th Conference on Information Communications (INFOCOM'12)*. IEEE Press, 1996–2004. DOI:http://dx.doi.org/10.1109/INFCOM.2012.6195577

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

Yong Xi, Loren Schwiebert, and Weisong Shi. 2006. Preserving source location privacy in monitoring-based wireless sensor networks. In *Proceedings of the 20th IEEE International Parallel and Distributed Processing Symposium*. IEEE Press, 8. DOI:http://dx.doi.org/10.1109/IPDPS.2006.1639682

Toby Xu and Ying Cai. 2009. Location safety protection in ad hoc networks. *Journal of Ad Hoc Networks* 7, 8 (Nov. 2009), 1551–1562. DOI:http://dx.doi.org/10.1016/j.adhoc.2009.04.001

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'13)*. IEEE Computer Society, 254–265. DOI:http://dx.doi.org/10.1109/ICDE.2013.6544830

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 1st ACM Conference on Wireless Network Security (WiSec'08)*. ACM, New York, NY, 77–88. DOI:http://doi.acm.org/10.1145/1352533.1352547

Jianbo Yao. 2010. Preserving mobile-sink-location privacy in wireless sensor networks. In *2010 2nd International Workshop on Database Technology and Applications*. IEEE Press, 1–3. DOI:http://dx.doi.org/10.1109/DBTA.2010.5659065

Jianbo Yao and Guangjun Wen. 2008. Preserving source-location privacy in energy-constrained wireless sensor networks. In *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops (ICDCSW'08)*. IEEE Computer Society, 412–416. DOI:http://dx.doi.org/10.1109/ICDCS.Workshops.2008.42

Bidi Ying, Jose R. Gallardo, Dimitrios Makrakis, and Hussein T. Mouftah. 2011. Concealing of the sink location in WSNs by artificially homogenizing traffic intensity. In *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'11)*. IEEE Press, 988–993. DOI:http://dx.doi.org/10.1109/INFCOMW.2011.5928957

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:http://dx.doi.org/10.1109/ICDE.2008.4497445

Yihua Zhang, Matthew Price, Lukasz Opyrchal, and Keith Frikken. 2010. All proxy scheme for event source anonymity in wireless sensor networks. In *2010 6th International Conference on Intelligent Sensors, Sensor Networks and Information Processing*. IEEE Press, 263–268. DOI:http://dx.doi.org/10.1109/ISSNIP.2010.5706759

Zhichao Zhu and Guohong Cao. 2011. APPLAUS: A privacy-preserving location proof updating system for location-based services. In *Proceedings of the 29th Conference on Information Communications (INFOCOM'11)*. IEEE Press, 1889–1897. DOI:http://dx.doi.org/10.1109/INFCOM.2011.5934991

Jindan Zhu, Kyu-Han Kim, Prasant Mohapatra, and Paul Congdon. 2013. An adaptive privacy-preserving scheme for location tracking of a mobile user. In *Proceedings of 10th Annual IEEE International Conference on Sensing, Communications and Networking (SECON'13)*. IEEE Press, 140–148. DOI:http://dx.doi.org/10.1109/SAHCN.2013.6644972

Received September 2014; revised April 2015; accepted July 2015