ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2015**

# Review on Privacy Preserving Location Monitoring Services in WSNs

[1] **A. Deepika,** [2] **R. Nirmalan**

[1]PG Student (CSE), Dept. of CSE, Sri Vidya College of Engineering and Technology, Virudhunagar, Tamil Nadu, India

[2] Assistant professor, Dept. of IT, Sri Vidya College of Engineering and Technology, Virudhunagar, Tamil Nadu, India

**ABSTRACT:** Wireless sensor technologies gave rise to many new applications widely used by general citizens as well as military operations. Numerous cases of these applications are based on the information of personal locations. Observations of these locations with untrusted server cause privacy threats to the individuals being monitored. To deal with such a privacy break, the concept of aggregate location information has been proposed using counting sensors, which would also pretence retreat breaches. To overcome this problem k-anonymity privacy approaches are employed, wherein every person is indiscernible among k-persons. The objective this review is to study various location preserving protocols which can provide high quality location monitoring services for system user, while preserving personal location privacy. This paper formalizes the summary of different location privacy preserving schemes for wireless sensor networks.

**KEYWORDS:** Wireless Sensor networks, location privacy, k-anonymity privacy, eavesdropper.

## I.INTRODUCTION

Wireless sensor networks (WSNs) are innovative large-scale wireless networks that consist of distributed, autonomous, low-power, low-cost, small-size devices using sensors to cooperatively collect information through infrastructure less ad-hoc wireless network. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. Security plays a fundamental role in many wireless sensor network applications. Because sensor networks pose unique challenges, security techniques used in conventional networks cannot be directly applied to WSNs because of its unique characteristics. The sensor nodes such networks are deployed over a geographic area by aerial scattering or other means. Each sensor node can only detect events within a very limited distance, called the sensing range. In addition, sensor nodes normally have fairly limited transmission and reception capabilities so that sensing data have to be relayed via a multi-hop path to a distant base station (BS), which is a data collection center with sufficiently powerful processing capabilities and resources. Monitoring personal locations with a potentially untrusted system poses privacy threats to the monitored individuals. This paper proposes a privacy preserving location monitoring system for wireless sensor networks to provide monitoring services. The privacy preserving techniques are discussed in the following section.

## II.PRIVACY PRESERVING TECHNIQUES

Based on system architecture, current spatial cloaking techniques for k-anonymity can be classified into

1. Centralized Techniques
2. Distributed Techniques
3. Peer-to-peer Techniques

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2015**

**2.1. Centralized Techniques**

B. Bamba et al [1] presented Privacy Grid − a framework for sup- porting anonymous location-based queries in mobile information delivery systems. The Privacy Grid framework offers three unique capabilities. First, it provides a location privacy protection preference profile model, called location P3P, which allows mobile users to explicitly define their preferred location privacy requirements in terms of both location hiding measures (e.g., location k-anonymity and location l-diversity) and location service quality measures (e.g., maximum spatial resolution and maximum temporal resolution). Second, it provides fast and effective location cloaking algorithms for location k-anonymity and location l-diversity in a mobile environment. Dynamic bottom- up and top-down grid cloaking algorithms are developed with the goal of achieving high anonymization success rate and efficiency in terms of both time complexity and maintenance cost. A hybrid approach that carefully combines the strengths of both bottom-up and top-down cloaking approaches to further reduce the average anonymization time is also developed. Last but not the least, Privacy Grid incorporates temporal cloaking into the location cloaking process to further increase the success rate of location anonymization. Also the Privacy Grid mechanisms for supporting anonymous location queries are discussed. Experimental evaluation shows that the Privacy Grid approach can provide close to optimal location k-anonymity as defined by per user location P3P without introducing significant performance penalties.

B. Hoh et al [2] introduced virtual trip lines which are geographic markers that indicate where vehicles should provide speed updates. These markers are placed to avoid specific privacy sensitive locations. They also allow aggregating and cloaking several location updates based on trip line identifiers, without knowing the actual geographic locations of these trip lines. Thus, they facilitate the design of a distributed architecture, in which no single entity has a complete knowledge of probe identities and fine-grained location information. The system is implemented with GPS smart phone clients and conducted a controlled experiment with 100 phone-equipped drivers circling a highway segment, which was later extended into a year-long public deployment.

P. Kalnis et al [3] presented a framework for preventing location based identity inference of users who issue spatial queries to Location Based Services. Transformations based on the well-established K-anonymity concept is proposed to compute exact answers for range and nearest neighbor search, without revealing the query source. The methods optimize the entire process of anonymizing the requests and processing the transformed spatial queries. Extensive experimental studies suggest that the proposed techniques are applicable to real-life scenarios with numerous mobile users.

T. Wang and L. Liu et al [4] presented a general model for privacy-aware mobile services. A series of key features distinguish the solution from existing ones: a) it adopts the network-constrained mobility model (instead of the conventional random-waypoint model) to capture the privacy vulnerability of mobile users; b) it regards the attack resilience (for mobile users) and the query-processing cost (for service providers) as two critical measures for designing location privatization solutions, and provides corresponding analytical models; c) it proposes a robust and scalable location anonymization model, XStar, which best leverages the two measures; d) it introduces multi-folded optimizations in implementing XStar, which lead to further performance improvement. A comprehensive experimental evaluation is conducted to validate the analytical models and the efficacy of XStar.

B. Gedik and L. Liu [5] describe a scalable architecture for protecting the location privacy from various privacy threats resulting from uncontrolled usage of LBSs. This architecture includes the development of a personalized location anonymization model and a suite of location perturbation algorithms. A unique characteristic of the location privacy architecture is the use of a flexible privacy personalization framework to support location k-anonymity for a wide range of mobile clients with context-sensitive privacy requirements. This framework enables each mobile client to specify the minimum level of anonymity that it desires and the maximum temporal and spatial tolerances that it is willing to accept when requesting k-anonymity-preserving LBSs. An efficient message perturbation engine is devised to implement the proposed location privacy framework. The prototype that developed is designed to be run by the anonymity server on a trusted platform and performs location anonymization on LBS request messages of mobile clients such as identity removal and spatio-temporal cloaking of the location information. The effectiveness of the location cloaking algorithms is studied under various conditions by using realistic location data that is synthetically generated from real road maps and traffic volume data. The experiments show that the personalized location k-anonymity model, together with the location

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2015**

perturbation engine, can achieve high resilience to location privacy threats without introducing any significant performance penalty.

B. Hoh et al [25] describe a system based on virtual trip lines and an associated cloaking technique, followed by another system design in which the privacy requirements are relaxed to maximize the accuracy of real-time traffic estimation. Virtual trip lines are introduced which are geographic markers that indicate where vehicles should provide speed updates. These markers are placed to avoid specific privacy sensitive locations. They also allow aggregating and cloaking several location updates based on trip line identifiers, without knowing the actual geographic locations of these trip lines. Thus, they facilitate the design of a distributed architecture, in which no single entity has a complete knowledge of probe identities and fine-grained location information. The system is implemented with GPS smart phone clients and conducted a controlled experiment with 100 phone-equipped drivers circling a highway segment, which was later extended into a year-long public deployment.

### 2.2. Distributed Techniques

P. Belsis and G. Pantziou [6] presented a clustering-based anonymity scheme for effective network management and data aggregation, which also protects user's privacy by making an entity indistinguishable from other k similar entities. The presented algorithm is resource aware, as it minimizes energy consumption with respect to other more costly, cryptography-based approaches. The system is evaluated from an energy-consuming and network performance perspective, under different simulation scenarios.

G. Ghinita et al [7] address two issues: (i) Existing approaches may fail to provide spatial anonymity for some distributions of user locations and describe a novel technique which solves this problem. (ii) Prive is proposed as a decentralized architecture for preserving the anonymity of users issuing spatial queries to LBS. Mobile users self-organize into an overlay network with good fault tolerance and load balancing properties. Prive avoids the bottleneck caused by centralized techniques both in terms of anonymization and location updates. Moreover, the system state is distributed in numerous users, rendering Prive resilient to attacks. Extensive experimental studies suggest that Prive is applicable to real-life scenarios with large populations of mobile users.

G. Zhong and U. Hengartner [8] proposed a distributed approach that does not have these drawbacks. The approach assumes that there are multiple servers, each deployed by a different organization. A user's location is known to only one of the servers (e.g., to her cell phone provider), so there is no single entity that knows everybody's location. With the help of cryptography, the servers and a user jointly determine whether the k-anonymity property holds for the user's area, without the servers learning any additional information, not even whether the property holds. A user learns whether the k-anonymity property is satisfied and no other information. The evaluation of the sample implementation shows that the distributed k-anonymity protocol is sufficiently fast to be practical. Moreover, the protocol integrates well with existing infrastructures for location-based services, as opposed to the previous research.

### 2.3. Peer-to-peer Techniques

J. Bao et al [9] present the technologies and implementations which protect location privacy by peer-to-peer based cloaking on road networks. The prototype system as named as PROS. With PROS, a mobile user forms a cloaked road segment set by collaborating with her peers when she needs to retrieve information from location-based service providers. Afterward, the cloaked road segment set is sent to the service provider for query processing and an inclusive query result set is returned to the query initiator after the query evaluation.

C.-Y. Chow et al [10] proposed a privacy preserving location monitoring system for wireless sensor networks. Here, two in-network anonymization algorithms are designed which aim to enable the system to provide high quality location monitoring services, while preserving personal location privacy and algorithms rely on the well-established n-anonymity privacy concept. For the location monitoring system using identity sensors, the sensor nodes report the exact location information of the monitored persons to the server; thus using identity sensors immediately poses 3 major privacy breaches. To tackle such a privacy breach, the concept of aggregate location information, that is, a collection of location data relating to a group or category of persons from which individual identities have been removed has been suggested as an effective approach to preserve location privacy.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2015**

B. N. Jagdale and N. S. Gawande [11] developed a system which preserves the location privacy of the concerned individual. This objective is achieved by simulating locally cloak algorithm and globally cloak algorithm for Manhattan mobility model and Waypoint mobility model using NS-2.34 environment. In the experiments, to hide the user's current locations in rectangle [bounding box] according to users privacy need, obfuscation and k-anonymity strategies are used.
J. Chen et al [12] propose a query-aware location privacy model based on p-sensitive & k-anonymity for road networks. By cloaking a user's location into p connected road segments which include at least k users, the model is able to meet privacy requirements, and to minimize the query processing cost. Simulate experiments on the model is conducted, the result manifest its privacy resilience and efficient query processing.
G. Ghinita et al [13] proposed MobiHide, a Peer-to-Peer system for anonymous location-based queries, which addresses these problems. MobiHide employs the Hilbert space-filling curve to map the 2-D locations of mobile users to 1-D space. The transformed locations are indexed by a Chord-based distributed hash table, which is formed by the mobile devices. The resulting Peer-to-Peer system is used to anonymize a query by mapping it to a random group of K users that are consecutive in the 1-D space. Compared to existing state-of-the-art, MobiHide does not provide theoretical anonymity guarantees for skewed query distributions. Nevertheless, it achieves strong anonymity in practice, and it eliminates system hotspots. The experimental evaluation shows that MobiHide has good load balancing and fault tolerance properties, and is applicable to real-life scenarios with numerous mobile users.
T. Hashem and L. Kulik [14] presented a novel algorithm that safeguards the location privacy of users accessing location-based services via mobile devices. The technique exploits the capability of mobile devices to form wireless ad-hoc networks in order to hide a user's identity and position. Local ad-hoc networks enable us to separate an agent's request for location information, the query initiator, from the agent that actually requests this service on its behalf, the query requestor. Since a query initiator can select itself or one of the $k - 1$ agents in its ad-hoc network as a query requestor, the query initiator remains k-anonymous. In addition, the location revealed to the location service provider is a rectangle instead of an exact coordinate. An anonymous selection algorithm is developed that selects a query requestor with near-uniform randomness, which is a key component to ensure anonymity in an ad-hoc network. The experiments show that a system can ensure a high quality of service and maintain a high degree of privacy in terms of anonymity and obfuscation while accessing location-based services.

## III.CONCLUSION

Location privacy is of the essence to the successive deployment of wireless sensor network. This paper addresses the survey on various techniques of securing a wireless sensor network against a variety of security threats that can lead to the failure of sources and sinks. The results of the survey shows that there is a broad room for research on preserving location privacy considering various parameters like energy efficiency, latency, security, communication cost.

## REFERENCES

[1] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacy grid," in Proc. 17th Int. Conf. World Wide Web, 2008, pp. 237–246.
[2] B. Hoh, T. Iwuchukwu, Q. Jacobson, D. Work, A. M. Bayen, R. Herring, J.-C. Herrera, M. Gruteser, M. Annavaram, and J. Ban, "Enhancing privacy and accuracy in probe vehicle-based traffic monitoring via virtual trip lines," IEEE Trans. Mobile Comput., vol. 11, no. 5, pp. 849–864, May 2012.
[3] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733, Dec. 2007.
[4] T. Wang and L. Liu, "Privacy-aware mobile services over road networks," Proc. VLDB Endowment, vol. 2, no. 1, pp. 1042–1053, Aug. 2009.
[5] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," IEEE Trans. Mobile Comput., vol. 7, no. 1, pp. 1–18, Jan. 2008.
[6] P. Belsis and G. Pantziou, "A k-anonymity privacy-preserving approach in wireless medical monitoring environments," Pers. Ubiquitous Comput., vol. 18, no. 1, pp. 61–74, 2014.
[7] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous location-based queries in distributed mobile systems," in Proc. 16th Int. Conf. World Wide Web, 2007, pp. 371–380.
[8] G. Zhong and U. Hengartner, "A distributed k-anonymity protocol for location privacy," in Proc. IEEE Int. Conf. Pervasive Comput. Commun., 2009, pp. 1–10.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 11, November 2015**

[9] J. Bao, H. Chen, and W.-S. Ku, "PROS: A peer-to-peer system for location privacy protection on road networks (Demo)," in Proc. 17th ACM SIGSPATIAL Int. Conf. Adv. Geographic Inf. Syst., 2009, pp. 552–553.
[10] C.-Y. Chow, M. F. Mokbel, and T. He, "A privacy-preserving location monitoring system for wireless sensor networks," IEEE Trans. Moblie Comput., vol. 10, no. 1, pp. 94–107, Jan. 2011.
[11] B. N. Jagdale and N. S. Gawande, "Hybrid model for location privacy in wireless ad-hoc networks for mobile applications," Int. J. Comput. Appl., vol. 57, no. 21, pp. 1–10, 2012.
[12] J. Chen, H. Xu, and L. Zhu, "Query-aware location privacy model based on p-sensitive and k-anonymity for road networks," in Internet of Things. New York, NY, USA: Springer, 2012.
[13] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "MOBIHIDE: A mobile peer-to-peer system for anonymous location-based queries," in Proc. Int. Symp. Spatial Temporal Databases, 2007, pp. 221–238.
[14] T. Hashem and L. Kulik, "Safeguarding location privacy in wireless ad-hoc networks," in Proc. 9th Int. Conf. Ubiquitous Comput., 2007, pp. 372–390.