Indian Journal of Science and Technology

Supplementary Article

QOS Aware Privacy Preserving Location Monitoring in Wireless Sensor Network

K. P. Kaliyamurthie[1]*, D. Parameswari[2] and R. Udayakumar[3]

[1]Professor and Head, Dept. of IT, Bharath University, Chennai-600 073; kpkaliyamurthie@gmail.com
[2]Asst. Prof. (SG), Dept. of Computer Applications, Jerusalem College of Engg., Chennai-600 100; p_kaliyamoorthy@yahoo.com
[3]Associate Professor, Department of Information Technology, Bharath University, Chennai-600073; udayakumar@bharathuniv.ac.in

Abstract

Sensor networks have been widely employed in many real-time applications. One of the most obvious challenges appearing to threaten the successful deployment of sensor networks is privacy issues including source-location privacy which cannot be adequately addressed by general security mechanisms. Focusing on this important kind of privacy, among many approaches proposed in literatures, self-adjusting phantom routing is a very successful one. But it still has some weaknesses. In this paper, we propose an improved version of it to enhance its performance. This method can decrease energy consumption and communication cost while increase the accuracy of the aggregate locations by minimizing their monitored areas.

Keywords: Sensor Network, Privacy, Context Privacy, Source-Location.

1. Introduction

As a cost-efficient approach for collecting real time data, sensor networks have been widely employed in many monitoring-based applications such as gathering data regarding highway traffic, battle field reconnaissance, and habit monitoring of endangered animal species. One of most obvious challenges appearing to threaten the successful deployment of sensor networks is the concern of privacy issues [2]. In general, achieving privacy in sensor networks is a complicated problem by the fact that sensor networks normally consist of a set of low-cost radio devices that operate on readily-available, standardized wireless communication technologies [4-6]. Therefore, the open-architecture of underlying sensor technology results in a privacy breach where an attack, simply by employing a sensor node running at monitoring mode, can easily get into the communication between sensor nodes [5].

Generally, privacy threats in sensor networks can be categorized into two classes, content-oriented privacy threat and contextual privacy threat respectively [7]. Content-oriented privacy concerns an adversary's capability to observe and manipulate data, whether real sensed data or lower-layer control information, transmitted over sensor networks. Fortunately, content-oriented privacy has been addressed adequately in literature and can be preserved by network security mechanisms such as encryption [8]. Contextual privacy, on the other hand, cares the context associated with the measurement and transmission of sensed data [9-11]. For instance, the physical location of a message originator is sensitive and need to be protected in many sensor network applications, especially for those being used in monitoring valuable assets such as the Panda-Hunter game described in [2]. However, contextual privacy protection techniques available for general networks cannot be applied to sensor networks due to their

*Corresponding author:
K. P. Kaliyamurthie (kpkaliyamurthie@gmail.com)

own underlying characteristics. In many sensor networks, the radio-enabled sensor nodes have limited transmission range because of the limited energy supply. Hence, in order to report sensed data to the base station, a multi-hop routing path has to be established between the source and the sink (also called base station) [13]. Consequently, an adversary with a RF localization device can start from the sink. Once he receives a message, by analyzing the direction and signal strength, the adversary knows where this message originates and moves towards that node. Repeating this process makes it easily trace back to the message originator through the multi-hop routing path.

Instead of introducing a new layer for privacy control, a number of current researches spend efforts in designing methods to augment existing routing protocols so that the source-location privacy in sensor networks can be enhanced [15]. Currently, among various routing protocols employed in sensor networks, flooding and single-path routing protocols are the two most popular scenarios. In flooding routing, every sensor node forwards a new message once [13, 14]. The source broadcasts a message to all of its neighbors. When a message arrives at an intermediate sensor node, that node first checks whether it has been forwarded. For a forwarded message, the receiving node simply discards it; otherwise, it broadcasts this message again to all of its neighbors. This kind of paradigm is iterated until the message reaches the sink. With flooding routing, a message is delivered to the sink multiple times through different routing paths. Single path routing, as its name suggests, establishes only one persistent source-sink path for message delivery based on some objectives such as the path with the shortest length. In the current literature, a number of augmenting methods, known as fake source messaging in [1], phantom routing in [2], and self-adjusting phantom routing in [3], have been proposed to be combined with the existing popular routing protocols to achieve source-location privacy in sensor network.

To preserve personal location privacy, we propose two in-network aggregate location anonymization algorithms, namely, resource- and quality-aware algorithms. Both algorithms require the sensor nodes to collaborate with each other to blur their sensing areas into cloaked areas, such that each cloaked area contains at least k persons to constitute a k-anonymous cloaked area. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to minimize the size of the cloaked areas, in order to maximize the accuracy of the aggregate locations reported to the server. In the resource-aware algorithm, each sensor node finds an adequate number of persons, and then it uses a greedy approach to find a cloaked area. On the other hand, the quality-aware algorithm starts from a cloaked area A, which is computed by the resource-aware algorithm. Then A will be iteratively refined based on extra communication among the sensor nodes until its area reaches the minimal possible size. For both algorithms, the sensor node reports its cloaked area with the number of monitored persons in the area as an aggregate location to the server.

Although our system only knows the aggregate location information about the monitored persons, it can still provide monitoring services through answering aggregate queries, for example. What is the number of persons in a certain area?. To support these monitoring services, we propose a spatial histogram that analyzes the gathered aggregate locations to estimate the distribution of the monitored persons in the system. The estimated distribution is used to answer aggregate queries.

2. Literature Survey

2.1 MobiHide: A Mobile a Peer-to-peer System for Anonymous Location-based Queries

Author: Gabriel Ghinita, Panos Kalnis, and Spiros Skiadopoulos

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.

2.1.1 MobiHide

MobiHide a P2P system which employs a randomized K-ASR construction technique to order query source anonymity, and is scalable to a large number of mobile users.

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. MobiHide outperforms existing solutions: our system

provides strong anonymity, it is fault-tolerant, and scales to large numbers of mobile users.

In future work, we plan to address the issue of anonymizing user trajectories, as opposed to user locations. Furthermore, we plan to investigate efficient methods to anonymize queries for infrastructure-less environments, such as ad-hoc wireless networks (Wi-Fi, Bluetooth), where point-to-point communication channels do not exist between any pair of users, and only users within a limited physical range can be contacted.

2.2 Preventing Location-based Identity Inference in Anonymous Spatial Queries

Author: Panos Kalnis, Gabriel Ghinita, Kyriakos Mouratidis, and Dimitris Papadias

In this paper, we present a framework for preventing location based identity inference of users who issue spatial queries to Location Based Services. We propose transformations based on the well-established K-anonymity concept to compute exact answers for range and nearest neighbor search, without revealing the query source. Our methods optimize the entire process of anonymizing the requests and processing the transformed spatial queries.

2.2.1 K-anonymity

A dataset is said to be K-anonymized, if each record is indistinguishable from at least K-1 other records with respect to certain identifying attributes. In the context of location bas ed services, the Kanonymity concept translates as follows: given a query, guarantee that an attack based on the query location cannot identify the query source with probability larger than 1/K, among other K-1 users.

To provide a formal guarantee for the anonymization strength. Continuous queries involve several complex issues, and constitute a promising topic for further work.

2.3 Casper: Query Processing for Location Services without Compromising Privacy

Author: Chi-Yin Chow Mohamed F. Mokbel Walid G. Aref

This paper presents a new privacy-aware query processing framework Capser in which mobile and stationary users can obtain snapshot and/or continuous location-based services without revealing their private location information. In particular, we propose a privacy-aware query processor embedded inside a location-based database server to deal with snapshot and continuous queries based on the knowledge of the user's cloaked location rather than the exact location.

2.3.1 Privacy-aware Query Processor

The snapshot/continuous privacy-aware query processor is embedded inside the location-based database server to anonymously deal with cloaked areas from the location anonymizer rather than exact point locations. Instead of returning an exact answer, the privacy-aware query processor returns a candidate list of answers in which the exact query answer to the user issuing the query through the location anonymizer must be included.

Our query processor achieves high quality snapshot and continuous location-based services while supporting queries and/or data with cloaked locations. Scalability and efficiency with a large number of mobile users, continuous queries, and data, various privacy requirements, and various performance tuning settings.

In addition, the performance of the query processor can be tuned through several parameters to achieve a trade-off between system scalability, i.e., query processing time, and query answer optimality, i.e., candidate list size.

2.4 PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks

Author: Wenbo He, Xue Liu, Hoang Nguyen, Klara Nahrstedt, Tarek Abdelzaher

In this paper, we present two privacy-preserving data aggregation schemes for additive aggregation functions. The first scheme – Cluster-based Private Data Aggregation (CPDA)– leverages clustering protocol and algebraic properties of polynomials. The second scheme – Slice-Mix-AggRegaTe (SMART)–builds on slicing techniques and the associative property of addition.

2.4.1 Cluster-based Private Data Aggregation

In the CPDA scheme, sensor nodes are formed randomly into clusters. Within each cluster, our design leverages algebraic properties of polynomials to calculate the desired aggregate value. At the same time, it guarantees that no individual node knows the data values of other nodes. The intermediate aggregate values in each cluster will be further aggregated (along an aggregation tree) on their way to the data sink.

2.4.2 Slice-Mix-AggRegaTe

In the SMART scheme, each node hides its private data by slicing it into pieces. It sends encrypted data slices to different intermediate aggregation nodes. After the pieces are received, intermediate nodes calculate intermediate aggregate values and further aggregate them to the sink. In both schemes, data privacy is preserved while aggregation is carrying out. The goal of our work is to bridge the gap between collaborative data collection by wireless sensor networks and data privacy.

It has the advantage of incurring less communication overhead It has the advantage of incurring less computation overhead.

No data privacy protection is provided. Our future work includes designing private-preserving data aggregation schemes for general aggregation functions. We are also investigating robust private-preserving data aggregation schemes under malicious attacks.

2.5 pDCS: Security and Privacy Support for Data-centric Sensor Networks

Author: Min Sha, Sencun Zhu, Wensheng Zhang, and Guohong Cao

We present pDCS, a privacy-enhanced DCS network which offers different levels of data privacy based on different cryptographic keys. In addition, we propose several query optimization techniques based on Euclidean Steiner Tree and Keyed Bloom Filter to minimize the query overhead while providing certain query privacy. Finally, detailed analysis and simulations show that the Keyed Bloom Filter scheme can significantly reduce the message overhead with the same level of query delay and maintain a very high level of query privacy.

The proposed techniques can significantly reduce the message overhead without losing any query privacy. In the future, we will address other issues such as source anonymity, key management, and look into other query techniques to balance the tradeoff between query delay and message overhead.

2.5.1 Achieving Guaranteed Anonymity in GPS

2.6 Traces via Uncertainty-aware Path Cloaking

Author: Baik Hoh, Marco Gruteser, Hui Xiong,

This paper considers the problem of achieving guaranteed anonymity in a locational data set that includes location traces from many users, while maintaining high data accuracy. We consider two methods to re-identify anonymous location traces, target tracking, and home identification, and observe that known privacy algorithms cannot achieve high application accuracy requirements or fail to provide privacy guarantees for drivers in low-density areas. To overcome these challenges, we derive a novel time-to-confusion criterion to characterize privacy in a locational data set and propose a disclosure control algorithm (called uncertainty-aware path cloaking algorithm) that selectively reveals GPS samples to limit the maximum time-to confusion for all vehicles.

2.6.1 Uncertainty-aware Path Cloaking Algorithm

That guarantees a maximum time-to-confusion and provides high data accuracy. Time-To-Confusion effectively captures how long an adversary can follow an anonymous user at a specified level of confidence and depends on parameters such as sampling frequency and user density. The uncertainty-aware path cloaking algorithm then determines which location samples from a set of users can be revealed anonymously given a maximum allowable time-to-confusion parameter.

We show that our uncertainty-aware path cloaking effectively guarantees worst-case tracking bounds (i.e., outliers), while achieving significant data accuracy improvements. Since the algorithm considers both density and driving behaviors (i.e., speed and direction), it effectively detects and removes traces that are sampled in low-density areas or could be easily tracked due to differences in driving direction from surrounding vehicles. It achieves better privacy than a random sampling technique at the same level of data quality. We also show that our solution is effective against clustering-based place identification techniques.

3. Summarization and Conclusion

In this paper, we propose a privacy-preserving location monitoring system for wireless sensor networks. We design two in-network location anonymization algorithms, namely, resource- and quality-aware algorithms that preserve personal location privacy, while enabling the system to provide location monitoring services. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to minimize the size of cloaked areas in order to generate more accurate aggregate locations. To provide location monitoring services based on the aggregate location information, we propose a spatial histogram approach that analyzes the aggregate

locations reported from the sensor nodes to estimate the distribution of the monitored objects. The estimated distribution is used to provide location monitoring services through answering range queries.

4. References

1. Ozturk C, Zhang Y et al. (2004). Source-location privacy in energy-constrained sensor network routing, Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks SASN '04, 88–93.
2. Kamat P, Zhang Y et al. (2005). Enhancing source-location privacy in sensor network routing, Distributed Computing Systems, ICDCS 2005, Proceeding 25th IEEE International Conference, 599–608.
3. Zhang L (2006). A self-adjusting directed random walk approach for enhancing source-location privacy in sensor network routing, Proceedings of the 2006 International Conference on Wireless communications and mobile computing IWCMC '06, 33–38.
4. Son B, Shin S et al. (2007). Implementation of the realtime people counting system using wireless sensor networks, International Journal of Multimedia and Ubiquitous Engineering (IJMUE), vol 2, No. 3, 63–80.
5. Culler D, and Estrin M S D (2004). Overview of sensor networks, IEEE Computer, vol 37, No. 8, 41–49.
6. Gedik B, and Liu L (2008). Protecting location privacy with personalized k-anonymity: Architecture and algorithms, IEEE TMC, vol 7, No. 1, 1–18.
7. Kalnis P, Ghinita G et al. (2007). Preventing location-based identity inference in anonymous spatial queries, IEEE TKDE, vol 19, No. 12, 1719–1733.
8. Samarati P (2001). Protecting respondent's privacy in microdata release, IEEE Transactions on Knowledge and Data Engineering, vol 13, No. 6, 1010–1027.
9. Sweeney L (2002). k-Anonymity: A model for protecting privacy, International Journal of Uncertainty, Fuzziness, and Knowledge-Based Systems, vol 10, No. 5, 557–570.
10. Gedik B, and Liu L (2005). A customizable k-anonymity model for protecting location privacy, Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS '05), 620–629.
11. Meyerson A, and Williams R (2004). On the complexity of optimal k-anonymity, Proceedings of ACM Symposium, Principles of Database Systems (PODS '04), 223–228.
12. Aggarwal G, Feder T et al. (2005). Anonymizing Tables, Proceedings of International Conference on Database Theory (ICDT '05), 246–258.
13. Gedik B, and Liu L (2005). Location privacy in mobile systems: a personalized anonymization model, Proceedings of 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05), 620–629.
14. Hoh B, Gruteser M et al. (2006). Enhancing Security and Privacy in Traffic-Monitoring Systems, IEEE Pervasive Computing, vol 5, No. 4, 38–46.
15. Terrovitis M, and Mamoulis N (2008). Privacy preservation in the publication of trajectories, Proceedings of Ninth International Conference on Mobile Data Management (MDM '08), 65–72.