INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

PRIVACY PRESERVING SYSTEM FOR WSN BY USING LOCATION MONITORING

PROF. P. B. SAMBHARE, PRAJAKTA S. GUPTA

P.R.Pote (Patil) College of Engg. &management, Amravati

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* Monitoring personal locations with a implicitly not trusted server creates privacy threats to the monitored individuals. To this end, we suggest a privacy-preserving location monitoring system for wireless sensor network (WSN). For our system, we design two in network location anonymization algorithms, that is, resource- and quality-aware algorithms that aim to enable the system to provide good quality location monitoring services for system users, by preserving personal location privacy. Both algorithms depends on the well-established n-anonymity privacy concept, that is, a person is indistinguishable among n persons, to enable trusted sensor nodes to provide the aggregate location facts of monitored persons for the system.

Keywords: Wireless sensor network, location monitoring, privacy preservation anonymity network resource aware algorithm, quality aware algorithm

Corresponding Author: PROF. P. B. SAMBHARE

Access Online On:

www.ijpret.com

How to Cite This Article:

P. B. Sambhare, IJPRET, 2016; Volume 4 (9): 531-538

PAPER-QR CODE

INTRODUCTION

Wireless sensor networks have gained worldwide attention in recent sensor network, which promise for various futuristic application for both mass public and military. It provide an overview of ongoing research activities, various design effect involved and possible solutions incorporating these effects. We are primarily concerned with monitoring personal locations with potentially not trusted system that poses privacy threats to the monitored individuals, because an unsympathetic person could misuse the location information gathered by the system to infer personal sensitive information.[9][10][11]For the location monitoring system that uses identity sensors, this sensor nodes will give the exact location information of the monitored persons to the server thus we can understand that using identity sensors immediately creates a major privacy violations. To handle such privacy violations, the conception of aggregate location information can be used, that says that, it is collection of persons from which individual identities have been taken away has been suggested as an effective approach to protect location privacy of location data relating to a group or category of persons from whom individual identities have been removed and suggested as an effective approach to preserve location privacy. [10][12]

1.1 PROBLEM DEFINITION:

We suggest a privacy preserving system for wireless sensor network using location monitoring system. Here, we design two in-network anonymization algorithms that aims to enable the system to provide good quality location monitoring services, by preserving personal location privacy and algorithms that depends upon the well-established n-anonymity privacy generalization. For the location monitoring system that makes use of identity sensors, the sensor nodes gives the exact location data of the monitored persons to the server; thus use of identity sensors immediately creates the major problems. To handle such a privacy issues; the concept of aggregate location information, that is, a collection of location data related to a group or category of persons from whom individual identities have been taken away has been suggested as an effective approach to protect location privacy.

1.2 NEEDS:

Wireless sensor networks depends upon wireless communication, that is by nature a broadcast medium which is more susceptible to security attacks than its wired counterpart due to absence of a physical boundary. In the wireless sensor domain, location privacy is an important security result to be considered. Absence of location privacy can uncover significant data about

the information carried over the network and the physical world entities. Various protocols are suggested for routing and data gathering but hardly few protocols are designed with security as a goal. The resource limitation of sensor networks creates great challenges for security.

1.3 OBJECTIVES:

Provides a summary of ongoing research activities, various design consequences involved and possible solutions incorporating these issues.WSN is an emerging technology that shows great promise for various futuristic applications both for vast public and military applications and studies the security aspects of these networks. Increasing requisition for security and automated monitoring of things and places makes WSNs promising technology. Monitoring personal locations with a potentially not trusted server creates privacy threats to the monitored individuals. It suggests an anonymous communication technique to preserve the location privacy of the users of location-based services. Handles a major privacy risk in current location-based services where users have to describe their exact locations to the database server for systematizing their desired services.

2.0 RELATED WORK:

Straightforward approaches for protecting users' location privacy encompass enforcing privacy policies to hold down the use of collected location data and anonymizing the stored data before any exposure. But, these approaches fail to stop internal data stealing or inadvertent disclosure. Presently, location anonymization techniques have been widely used to anonymise personal location data before any server gathers the location data, in order to protect personal location privacy in location-based services.

2.1 A PRIVACY-PRESERVING LOCATION MONITORING SYSTEM FOR WSNs:

The architecture of the system, where it consist of three major entities, sensor nodes, server, and system users. We will trace the problem addressed by the system, and then narrate the detail of each entity and the privacy model of the system. Problem definition. Given a set of sensor nodes S1,S2, ...,Sn having sensing areas A1,A2, ...,An, respectively, a set of moving objects O1,O2,...,Om, and a required anonymity level n, (1) we find an aggregate location for each sensor node si in a form of Ri = (Areai,Ni), where Areai is a rectangular area containing the sensing area of a set of sensor nodes Si and Ni is the number of objects residing in the sensing areas of the sensor nodes in Si, such that Ni ≥ n, Ni = | ∪sj∈SiOj| ≥ n, Oj = {Ol|Ol∈Aj}, 1 ≤ i ≤ m, and 1 ≤ l ≤ p; and (2) we build a spatial histogram to answer an aggregate query ‘Q’ that asks

about the number of objects in a certain area 'Q'. Area based on the aggregate locations described from the sensor nodes[5].

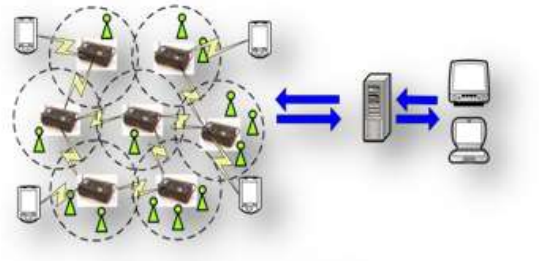

Fig 1 System Architecture

2.2 SECURITY THREATS IN WIRELESS SENSOR NETWORKS:

In a sensor network, an unsympathetic user can easily inject messages, that's why the receiver needs to make sure that the data used in any decision-making procedure originates from the correct source. Data authentication stops unauthorized parties from participating in the network and legal nodes should be able to detect messages from unauthorized nodes and deny them. In the two- party communication case, data authentication could be achieved by a purely symmetric mechanism: The sender and the receiver share a secret key to figure out a message authentication code called as MAC of all communicated data. When a message with a correct MAC arrives, the receiver comes to know that it must have been sent by the sender. But, authentication for broadcast messages requires stronger faith assumptions on the network nodes. The founders of SPINS compete that if one sender wishes to send authentic data to mutually entrusted receivers, using a symmetric MAC is insecure since any one of the receivers know the MAC key, and thus could impersonate the sender and forge messages to other receivers. SPINS forms authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains. LEAP uses a globally shared symmetric key for broadcast messages to the whole group. However, since the group key is shared among all the nodes in the network, an efficient reeking mechanism is defined for updating this key after a compromised node is revoked [2].

2.3 APPROACH TO SECURE SINK NODE'S LOCATION PRIVACY IN WSN:

A technique called Location Privacy Routing is used along with the fake packet injection that uses randomized routing for confusing the packet tracer along with fake packets which makes the transmission completely random. But, this technique involves a number of overhead and it

is not energy efficient as well. Careful monitoring of packet sending time may allow unsympathetic user to get information about the data traffic flows. To avoid this, de-correlation of the packet sending times between a parent node and its child nodes is used. Here, it is implicit that every node sends packets at the same rate. However, sometimes sensor nodes may send packets with different rates. Setting the packet sending rate control between a parent node and its children nodes is the solution to this.

2.4 APPROACH TO SECURE SINK NODE'S LOCATION PRIVACY IN WSN:

One of the famous scheme for location privacy is Randomized Routing with Hidden Address[12]. As the name suggests, the identity and location of the sink is kept private in the network to avoid it to be revealed and to become the target of attacks. The destination addresses of the packets are kept hidden so that the attacker cannot gain the location of the sink even when he reads the header fields of the packets. The packets are forwarded along different random paths. RRHA provides very strong protection for the sink privacy against both active and passive attackers.

3.0 PROPOSED WORK

We present our in-network resource -aware location annonymization algorithms that are frequently executed by the sensor nodes to report their n-anonymous aggregate locations to the server for every reporting period is shown in [16]Fig 2

Fig 2 Sensor Node with System User

That consists of three major entities, sensor nodes, server, and system users.

The node that is communicated with a destination node is to avoiding privacy node are shown in Fig 3. We will see the problem traced by our system, and then describe the detail of each entity and the privacy model of our system.

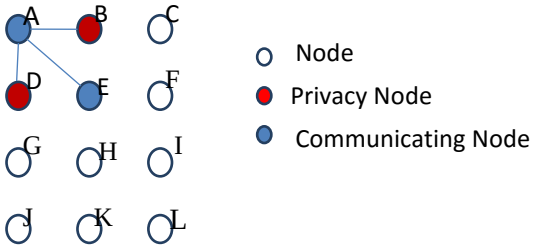

Fig 3. A Path of communicating Node with avoiding privacy

Our proposed work dependant on following basic algorithm

The Resource-Aware Algorithm:

This algorithm target is to minimize communication and calculation cost, while the quality-aware algorithm target is to minimize the size of cloaked areas in order to generate more exact aggregate locations. To provide location monitoring services based on the aggregate location information, we suggest a *spatial histogram* approach that analyzes the aggregate locations reported from the sensor nodes to evaluate the distribution of the monitored objects. The evaluated distribution is used to provide location monitoring services over answering range queries.

Quality Aware Algorithm:

The quality-aware algorithm begins from an area A, which is computed by resource aware algorithm. Then A will be repeatedly updated based on extra communication between the sensor nodes until its area reaches the minimal possible size. For both algorithms, the sensor node narration its masked area with the number of monitored persons in the area as an aggregate location to the server.

CONCLUSION:

We suggest a privacy-preserving system for wireless sensor networks using location monitoring system, We design two in-network location anonymization algorithms, that is, *resource*- and *quality-aware* algorithms, which protects personal location privacy, while enabling the system to provide location monitoring services. We will be evaluating our system through simulated experiments, whose results will be showing that our system provides high quality location monitoring services.

REFERENCES:

1. A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, .The anatomy of a context-aware application,. in*Proc. of MobiCom*, 1999.
2. N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, .The cricket location-support system,.in*Proc. of MobiCom*, 2000.
3. M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, Privacy-aware location sensor networks,. in*Proc. of HotOS*, 2003.
4. K. Bohrer, S. Levy, X. Liu, and E. Schonberg, .Individualized privacy policy based access control,.in*Proc. of ICEC*, 2003.
5. A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, SPINS: Security protocols for sensor netowrks,.in*Proc. of MobiCom*, 2001.
6. L. Sweeney, .Achieving k-anonymity privacy protection using generalization and suppression,.*IJUFKS*, vol. 10, no. 5, pp. 571. 588, 2002.
7. B. Gedik and L. Liu, .Protecting location privacy with personalized k-anonymity: Architecture and algorithms,.*IEEE TMC*, vol. 7, no. 1, pp. 1.18, 2008.
8. M. F. Mokbel, C.-Y. Chow, and W. G. Aref, .The New Casper: Query procesing for location services without compromising privacy, in *Proc. of VLDB*, 2006.
9. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, Private queries in location based services: Anonymizers are not necessary,.in*Proc. of SIGMOD*, 2008.
10. W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, PDA: Privacy-preserving data aggregation in wireless sensor networks,.in*Proc. of Infocom*, 2007.
11. M. Shao, S. Zhu, W. Zhang, and G. Cao, .*pDCS*: Security and privacy support for data-centric sensor networks,.in*Proc. OfInfocom*, 2007.
12. B. Carbunar, Y. Yu, W. Shi, M. Pearce, and V. Vasudevan, .Query privacy in wireless sensor networks,.in*Proc.ofSECON*,2007.
13. A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, “SPINS: Security protocols for sensor netowrks,” in Proc. of Mo- biCom, 2001.
14. P.Kamat,Y.Zhang,W.Trappe,andC.Ozturk,“Enhancingsource- location privacy in sensor network routing,” in Proc. of ICDCS, 2005.
15. S. Guo, T. He, M. F. Mokbel, J. A. Stankovic, and T. F. Abdelzaher, “On accurate and efficient statistical counting in sensor-based surveillance systems,” in Proc. of MASS, 2008.
16. L. Sweeney, “Achieving k-anonymity privacy protection using generalization and suppression,” IJUFKS, vol. 10, no. 5, pp. 571– 588, 2002.

17. B. Son, S. Shin, J. Kim, and Y. Her, “Implementation of the real- time people counting system using wireless sensor networks,” IJMUE, vol. 2, no. 2, pp. 63–80, 2007.