Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Location Anonymity Problem Techniques in Wireless Sensor Networks: A Survey

S. A. Pawar, V. N. Nayakwadi, S. M. Kokate
BSCOER Narhe, Pune, M.S.,
India

Abstract— Wireless Sensor Networks (WSNs) are nothing but the collection of mobile sensor nodes those are communicated to each other for information sharing based on requests. Information sharing in such network is having source and destination sensor nodes. And every node is having own position. Recently there are many security threats done using such location information of either source sensor node or receiver sensor node. In this paper we are focusing on source location privacy preservation in WSNs. The privacy preservation of source sensor node in WSN is currently interesting research challenge for researchers. In different real time applications, location of source sensor node needs to keep anonymous due to reason of security. This source sensor node which is having vital information to share with intended recipient. But with the help of information of network topology, the attackers are succeeded in getting the location information of source node. Previously there are many methods presented to keep the source location anonymous, but every method having its own advantages and disadvantages. In this paper our main goal is to take review of different source location privacy preservation methods presented so far for WSNs.

Keywords— sensor networks, information sharing, source node, receiver node, location privacy, packets dropping

I. INTRODUCTION

The WSN is consisting of varying number of tiny sensor devices those are resource constrained. These devices are also called as motes. In addition to this, WSN consisting of one or few general purpose computing devices referred to as base stations (or sinks). The basic use of WSN is to perform the monitoring of physical phenomenon for example light monitoring, temperature monitoring, barometric monitoring etc. over the geographical area of WSN deployment. Each sensor node in WSN is having the functionalities such as battery, processing unit and sensors. Each sensor node is having limitations of battery power which is means WSN is resource constrained. On the other hand, the base stations in WSN are nothing but laptops capabilities therefore those are not power constrained. The role of base station is bridge the communication gap between the other networks and WSN. The real time applications of WSNs are military applications, health applications, commercial applications, temperature monitoring etc. [1].

The classification of WSNs is based on different aspects with main focus of designing the secure routing protocol. The mobility of sensor nodes as well as base station is one aspect based on which the WSNs are classified. In WSNs, the sensor nodes are either stationary or mobile based on application requirements. Another reason of WSNs classification is topology used for nodes position. The placements of nodes are either done manually or randomly by using existing methods of topology. The total number of mobile nodes in WSN is also key based on which the WSNs are classified [13].

Now days, privacy is main challenge of WSNs. This privacy is divided into two classes such as contextual privacy and content oriented privacy. The contextual privacy is basically concerning with the concerns the ability of adversaries to infer information from observations of sensors and communications without access to the content of messages. Content-oriented privacy is concerned with the ability of adversaries to learn the content of transmissions in the sensor network. In contrast to content-oriented security, the issue of contextual privacy is concerned with protecting the context associated with the dimensions and transmission of sensed data. For many scenarios, general contextual information surrounding the sensor application, specially the location of the message originator and the base station called as sink. Among the different security threats in wireless sensor networks one is eavesdropping which involves attack against the confidentiality of data that is being transmitted across the network. Various privacy-preserving routing techniques have been developed for sensor networks. Most of them are designed to protect against the local eavesdropper and some of them are capable of protecting against global eavesdropper [3] [7].

In this paper we are taking the review of location privacy preservation details and their different methods. In section II, we are discussing the classification of different types of privacy preservation problems. In section III, different methods are discussed those are presented by various researchers to provide the security for location information.

II. TAXONOMY OF PRIVACY PROTECTION METHODS

WSNs privacy security classification is the classification and further refining the last privacy offers security are classified in the first data-oriented (content-oriented) and context-oriented data aggregation and personal data security-oriented. Then query the data during the privacy protection techniques are classified. Context-oriented spaces privacy protection privacy protection technology, data sync location source location safety and protective cover, and can be divided into the proverbial privacy protection techniques. An overview of the classification is shown in Figure 1.

A. Data Privacy

Data privacy protections target privacy of data collected by a network and queries posted to a network. There are two types of adversaries threatening the data privacy-external adversary and internal adversary. The external adversary only eaves drop communication in a network. This kind of adversary can be easily defeated by encryption techniques such as SPINS or pDCS. On the other hand, the internal adversary controls one or more nodes and usually has an access to encryption keys of these nodes. In such a case, the easiest way to protect privacy of data sent from nodes to the base station is to use end-to-end encryption based on keys shared between the sending node and the base station. However, such encryption makes data aggregation within the network impossible. Therefore, one of the challenges is to provide secure and privacy preserving data aggregation in the presence of an internal adversary. Multiple schemes were proposed to solve this problem.

B. Context privacy

Even though data privacy might be sufficiently protected, a sensor network may still leak valuable context-oriented information. Typical context-oriented information is information on source location, sink location and timing of events. This kind of information can be usually obtained by an external adversary using traffic analysis techniques. We summarize state-of-the-art protections in the following subsections.

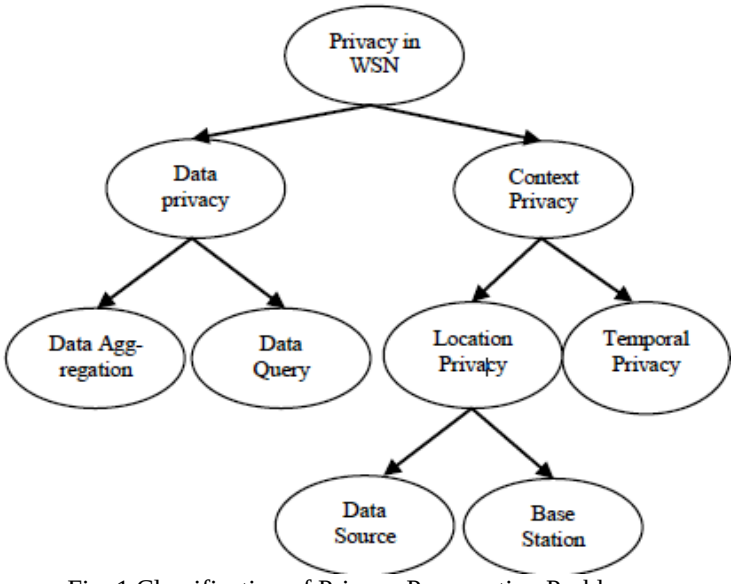

Fig. 1 Classification of Privacy Preservation Problems.

1) Location Privacy: Location privacy is extremely important in WSNs. Information on the location of the incidents or base stations of an anti-virus a primary concern. Panda-Hunter game where a monitor endangered pandas in their Habitat WSN & employed. it is currently creating and Panda successfully to capture local monitoring sensors to detect the location of similar enough to an opponent., Only physical or other DOS attack an opponent's base station on the mount and thus be able to inactivate entire networks to detect the location of the base station needs.

There are two basic types of adversaries considered when evaluating the location privacy-local adversary and global adversary. The local adversary has limited radio range and is able to monitor traffic only in a small part of the network at a time. On the contrary, the global adversary is capable of monitoring the whole network at a time and is able to immediately localize all transmitting nodes.

I. Data Source: Problem of source location privacy was introduced and first studied by Chaum who proposed a mix net to hide information on a data source. Onion routing in computer networks by Reid et al public source location privacy. Gruteser anonymous access to location based services and Grunewald is a proposed approach. This approach can compromise user location privacy fine details that removes spaces on-demand routing path nameless. Anonymity and privacy for mobile ad-hoc and not Etavark that are closely related to WSNs proposed for providing. However, many existing protocols on memory due to the power requirements, energy and computational resources are limited to inappropriate WSNs. WSNs several protocols were designed specifically for and we have them in this section summarize the nature of their main ideas they are based on are divided into four sections.

II. Base station: Base station security is critical for the proper functioning of a WSN. Base station collects data from the entire network and a gateway to other networks usually serves as a single point of failure, so this can be considered as an enemy locates, if base station. Many DOS attacks rendering useless the whole network can mount because of the location of the base station is extremely important. This need emphasized by the first Deng et al. Three basic traffic analysis techniques to discover the location of a base station has identified leading to: attack, attack, attack time correlation and analysis monitoring rate, attack monitoring according to an node messaging rate and the highest rate for a nodeIe., in an attack the time correlation of a node and its neighbours is a correlation in

time between the monitors. Enemy which node forwards the current message and direct path to a base station tries to locate passages. Content analysis in an attack message headers and payload of valuable information (such as a base station) tries to get.

As per the our further research approach which is based on source anonymity problem, in this paper further we are discussing the different methods or techniques presented for privacy preservation in WSN for above categorized problems.)

III. REVIEW OF LOCATION PRIVACY PRESERVATION TECHNIQUES

A. In [2], author presented the Backbone Flooding which is intelligence of the scheme lies in creation of backbone that is created by finding out minimum number of sensors that are needed to flood a packet so that whole network can receive it. The packets are sent only to the backbone and real sink can receive it as long as they are within the communication range of at least one backbone member. In this approach author has assumed static backbone which requires forwarding more packets than other nodes leading to more power consumption.

B. In [3] & [4], authors introduced the technique of Baseline Flooding where the source node transmits message to each of its neighbours. These neighbours in turn retransmit the message to each of its neighbours and so on. Thus packet is routed from source to destination through number of paths to make it difficult for an adversary to trace the source. No node in the network retransmits the packet. Adversary can trace the node using backtracking thus this method does not provide much privacy but consumes significant amount of energy.

C. In [4] author has discussed the Single Path Routing technique in which unlike flooding the node forwards message only to one of its neighbours. This technique requires pre-configuration phase where sink initiates the flood setting the hop count to zero. The packets from the neighbours are processed only once. Every time the node receives the message the hop count is incremented by one and stored in its local memory. Then the minimum value of the number of hops is selected, accordingly the neighbours are updated. The head of the neighbour list that has shortest distance to the sink is chosen as a path to forward the message to the sink.

D. In [5] author has put forward the Cyclic Entrapment Method that creates looping paths at various places in the sensor network. When message is routed from source to destination each node on a route will check if it is on a loop. If so, it will activate the loop by sending fake message. If an adversary is trying to analyse the route and trace the path towards source, if it find a node that is common to both loop and the true path then adversary has to make the decision which way to go. This will cause a local adversary to follow these loops repeatedly if wrong decision is taken and thereby increase the safety period.

E. In [3] & [4], another technique that author proposes is the phantom Flooding/ Routing, which achieves location privacy by making every packet generated by a source walk a random path which is either pure random walk or directed walk which let the messages towards the phantom source. Then the single path routing or flooding is employed to route the message toward the destination. As different messages exhibits different path this algorithm increases the safety period against local eavesdropper but the latency increases because of directing every message to a random location first.

F. Again in [3] & [4], author introduced next technique is routing with fake messages. In this technique destination creates fake sources whenever a sender notifies the destination that it has real data to send. These fake senders are away from the real source and approximately at the same distance from the destination as the real sender. Both real and fake sender generating packets at the same time, the plan is to start a local eavesdropper against decent privacy. To implement this technique whereas observations as follows:
   1) If the rate of fake message is same as the real message then adversary toggles between real source and fake source and cannot progress towards either of them.
   2) If the rate of fake message is less than that of real message then the adversary will be drawn towards real source.
   3) If the rate of fake message is greater than that of real message then the adversary will be kept at the real source.

   Thus showing fake messages at faster speed than real message will protect the privacy but will require more energy.

G. In [6], author focuses on packet tracing attack and proposes location privacy routing protocol (LPR). In this technique each sensor divides its neighbour's into closer list and further list. After choosing the creation of neighbours lists sensors next hop randomly either as a result of routing list path from source to destination as not fixed. If the sensor is the next hop from the list of picks will be more energy efficiency and if it chooses the next hop from the list, Privacy protection will be stronger the retrieval of information so that LPR traffic. Direction to minimize duplicate packet injection is augmented by an opponent.

H. In [7] author proposes the GROW algorithm for preserving source location privacy in monitoring based wireless sensor networks. Initially sink sets up the random path to receive packets from the source. The source then forwards the packet through the random path until it reaches the sink. When sensor selects any of its neighbours for packet forwarding, it checks if that neighbour is already in the filter.

I. In [8] random data collection scheme is designed to provide location privacy to mobile sinks. It comprises two steps, random data forwarding storage and random Movement of sink in data collection. In first step whenever sensor has data to forward it encrypts the message with symmetric key and forwards along the random path storing a copy locally. When node forwards the message it selects any node randomly as the next hop and increments the hop count

by one. This message travels the random path until hop cont field equals the pre-define length of the random path. In second step mobile sink moves around the network to gather data from the sensors and store it in its buffer. To evade from getting attacked and tracked, mobile sink changes its moving direction randomly.

J. In [9], the author introduced technique called RRIN to achieve source location privacy in wireless sensor network by using the concept of dynamic routing. In this approach each packet is routed through the node which is selected randomly according to the relative location of the sensor node. Intermediate node from the source node is at least some minimum distance from the source location to avoid the risk of conflicting to. This plan is suitable for small scale sensor networks.

K. In [9], intermediate nodes before the message are sent out from the source node in this approach. Intermediate node information is stored in the header of the message, but before you forward messages from intermediate node, intermediate node (s) will be deleted from the message header information. Intermediate nodes angle-based intermediate nodes are selected according to plan. The plan contains source node initially last intermediate node and According to the maximum angle between the sink nodes itself, and then determines the actual angle between the same.

L. To determine the source of a node needs generated by an intermediate node and node to determine the angle of all angles, distances between the source nodes generates intermediate node and itself. This plan is suitable for large scale sensor networks.

M. In [10], the author called as two-star phase routing plan. First step selects the source node is the intermediate node randomly random intermediate node present sync node around sink Toro dial (Star) is located in the area. The second phase to form intermediate node the message sink single-path routing is forwarded to the plan by both local and global offer to provide the source location privacy.

N. In [11] author proposes a naive algorithm that hides the real event messages by maintenance messages that are nothing but dummy messages. At the end of every fixed period every sensor node broadcast the maintenance message. The fixed period is called as maintenance period. Whenever source node wants to send an event message, this event message can be replaced with next maintenance message so that the attacker cannot distinguish between them. As the receptor of the event message has to wait till the end of the current maintenance period the delivery time is high.

O. In [11], Globally Optimal Algorithm is the next technique that author proposes. Unlike navie algorithm in this technique the duration of maintenance period is not fixed and is determined by pseudo random number generator (PRNG). By using PRNG it is possible for source node to predict approaching pseudo random for itself as well as for all the nodes in the network. By using this information fastest routing path towards destination can be calculated which leads to shortest delivery time provided global network topology is available and sensor nodes are timely synchronized.

P. In [11], Heuristic Greedy Algorithm is the approach that author put forwards in order to reduce the extra computation and storage cost. This technique does not require the knowledge of global network topology. Sensor nodes require the knowledge of only its neighbour's PRNG and their distances to the destination to select the next node towards the destination. The intelligence of the scheme lies in selecting the next node towards the destination. The neighbouring nodes closer to the end of maintenance periods are preferred.

Q. In [12], author presented the technique called "source simulation" in which fake objects are simulated in the network field that confuses the adversary by generating the traffic similar to the real objects. In this approach set of sensor node is selected called token node as they are preloaded with the token that has unique id. To simulate the behaviour of real objects these tokens will be passed within the nodes. Every token node emits the signal as if real object for event detection and generates the traffic as if the real event was detected thus confusing the adversary. This method is applicable for real time applications but the communication overhear is increased in order to protect location privacy.

IV. CONCLUSIONS

The privacy of source sensor node location is major research challenge in the field of wireless sensor networks under real time environment. Attackers use the source location information for breaking the private important information or leaking the information or dropping the messages without transmitting it to the intended recipient. Hence one must have security strategy which can able to secure the location information of source node in WSN. The transmitter should be designed in such way that privacy of source location is preserved. Source Anonymity is major research problem in WSN, there are many traditional methods were presented to solve the source anonymity problem in WSN. The traditional cryptographic based methods were failed to solve such anonymity problem. Thus to solve this problem recently some more techniques were presented. In this paper we have discussed different methods of securing the source location information in WSN. For the future work we suggest to work over improved new method for source anonymity problem in WSN with aim of improving the rest of routing performances.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," *Elsevier Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002.

[2] K. Mehta, D. Liu, and M. Wright, "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper," *Proc. IEEE Transactions on Mobile Computing*, vol. 11, No. 2, Feb 2012.

[3] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy Constrained Sensor Network Routing," Proc. Workshop Security of Ad Hoc and Sensor Networks (SASN '04), Oct. 2004.

[4] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," *Proc. Int'l Conf. Distributed Computing Systems (ICDCS '05)*, June 2005.

[5] Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping Adversaries for Source Protection in Sensor Networks," *Proc. Int'l Conf. World of Wireless, Mobile, and Multimedia Networking (WoWMoM '06)*, June 2006.

[6] Ying Jian, Shigang Chen and Zhan Zhang, "Protecting Receiver Location Privacy in Wireless Sensor Networks", *Proc. IEEE INFOCOM*, 2007.

[7] Yong Xi, Loren Schwiebert and Weisong Shi, "Preserving Source Location Privacy in Monitoring Based Wireless Sensor Networks," *20th International Parallel and Distributed Processing Symposium,* 2006.

[8] Edith C., H. Ngai and Lona Rodhe, "On Providing Location Privacy for Mobile Sinks in Wireless Sensor Networks," *Proc. ACM MSWiM*, Oct 2009.

[9] Yun Li and Jein Ren, "Source Location Privacy through Dynamic Routing in Wireless sensor Network", *Proc. IEEE INFOCOM*, 2010.

[10] Leron Lightfoot, Yun Li and Jian Rein, "Preserving Source Location Privacy in Wireless sensor Network using Star Routing," *Proc. IEEE Globecom*, 2010.

[11] Yi Ouyang, Zhengyi Le, Donggang Liu, James Ford, Fillia Makedon, "Source Location Privacy against Laptop–Class Attacks in Sensor Networks," *Proc. ACM SecureComm*, Sept. 2008.

[12] K. Mehta, D. Liu, and M. Wright, "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper," *Proc. IEEE Transactions on Mobile Computing*, vol. 11, No. 2, Feb 2012.

[13] Basel Alomair, Andrew Clark, Jorge Cuellar, and Radha Poovendran, "Statistical framework for source anonymity in sensor networks" Technical Report 3, Network Security Lab (NSL), College of Engineering, University of Washington, 2009.

