International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 9, November- 2012

Survey On Location Privacy Preserving Schemes In Wireless Sensor Network

Revati A. Parate
ABHA GAIKWAD – PATIL
College of Engg., Nagpur.

Pragati Patil
ABHA GAIKWAD – PATIL
College of Engg., Nagpur.

Girish Agarwal
ABHA GAIKWAD – PATIL
College of Engg., Nagpur.

Abstract

Sensor networks are used in variety of application areas to monitor the objects. Privacy is one of the major issues of wireless sensor network as wireless transmissions are susceptible to illicit interception and detection. There are many protocols that provide content-oriented security in wireless sensor network but context-oriented information generally remains insecure. Such context-oriented information can be utilized by an adversary to deduce sensitive information such as the locations of monitored objects and data sinks in the network field. No. of techniques exist that are capable of defeating the limited adversary called local eavesdropper who can only observe network traffic in a small region but very few techniques has been proposed to achieve protection against the stronger adversary called global eavesdropper. This paper formalizes the summary of different location privacy preserving schemes for wireless sensor networks.

Keywords: Wireless Sensor networks, source node, sink node, location privacy, eavesdropper, context oriented security.

1. Introduction

Wireless sensor network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. The main characteristics of wireless sensor network include:

- Power consumption constrains for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use

Sensor networks can be used for wide range of applications where it is difficult or infeasible to set up wired networks. Some of the areas include forest fire detection, air pollution monitoring, health, wildlife habitat monitoring etc. A sensor network can be deployed in a forest to detect the occurrence of fire. The sensors measure the temperature, humidity and gases due to the fire in the trees or vegetation. Wireless sensor networks have been deployed in various cities to detect foreign chemical agents in the air. Sensors are used by the doctors to monitor the physiological condition of patient.

Privacy is one of the major issues in wireless sensor network. Privacy may be categorized into two sub-classes: content-oriented privacy and contextual privacy. Content-oriented privacy is concerned with the ability of adversaries to learn the content of transmissions in the sensor network. Contextual privacy concerns the ability of adversaries to infer information from observations of sensors and communications without access to the content of messages. 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, are sensitive and must be protected. 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.

In this paper we are summarising the survey made on various location privacy preserving schemes for wireless sensor networks.

2. Baseline Flooding

In [2, 3] author has explored 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.

3. Single Path Routing

In [3] 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.

4. Routing With Fake Messages

The next technique that author proposes in [2, 3] 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 senders start generating packets at the same time. This scheme provides decent privacy against a local eavesdropper. While implementing this technique author has made certain observations as follows:

a. 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.

b. If the rate of fake message is less than that of real message then the adversary will be drawn towards real source.

c. If the rate of fake message is greater than that of real message then the adversary will be kept at the real source.

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

5. Phantom Flooding/ Routing

In [2, 3] 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.

6. Cyclic Entrapment Method

In [4] 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 analyze 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. Energy consumption and privacy provided by this method will increase as the length of the loops increase.

7. Location Privacy Routing Protocol (LPR)

The author in [5] focuses on packet tracing attack and proposes location privacy routing protocol (LPR). In this technique each sensor divides its neighbours into closer list and further list. After the construction of lists sensors select the neighbour as the next hop randomly from either of the two list as a result routing paths from source to destination is not fixed. If sensor selects the next hop from closer list then energy efficiency will be greater and if it selects next hop from the further list, privacy protection will be stronger. The LPR is augmented with fake packet injection so as to minimize the retrieval of traffic direction information by the adversary.

8. Random Data Collection Scheme

In [6] 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. The location or ID of the destination is not included in the message so that attackers fail to obtain the destination of the message. 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.

9. Greedy Random Walk (GROW)

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. Forwarding a packet by sensor to one of its previous hop's neighbour is not beneficial. Bloom filter is used to prevent this case. In the forwarding packet bloom filter stores all the current neighbours. When sensor selects any of its neighbours for packet forwarding, it checks if that neighbour is already in the filter.

10. Source Location Privacy through Routing to a Random Intermediate Node (RRIN)

The author proposes the technique RRIN to achieve source location privacy in wireless sensor network by using the concept of dynamic routing in [8]. In this approach each packet is routed through the node which is selected randomly according to the relative location of the sensor node. The intermediate node should be at least some minimum distance away from the source node in order to avoid the exposure of the source location to the adversary. This scheme is suitable for small scale sensor network.

11. Source Location Privacy through Angle - Based Multi – Intermediate Nodes

In this approach the intermediate node is selected prior to the message is sent out from source node. The information of the intermediate node is stored in the header of the messages, but before forwarding the message from the intermediate node, the information of the former intermediate node(s) will be deleted from the header of the message. The intermediate nodes are selected according to the angle - based intermediate node scheme. In this scheme source node initially determines the maximum angle between last intermediate node and itself according to the sink node, and then the actual angle between the same. After this source node needs to determine no. of intermediate nodes and calculate the angle generated by one intermediate node. After determining all the angles, the source node generates the distances between the intermediate node and itself. This scheme is suitable for large scale sensor networks [8].

12. Sink Toroidal Region (STaR) Routing

The author proposes the two–phase routing scheme called as Star Routing in [9]. In the first phase source node selects intermediate node randomly. This random intermediate node is located in the pre-determined region called Sink Torodial Region (STaR) around the sink node. In the second phase the message is forwarded form intermediate node to the sink by single path routing. This scheme is proposed to provide both local and global source location privacy.

13. A Navie Algorithm

In [10] author proposes a navie 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.

14. A Globally Optimal Algorithm

This is the next technique that author proposes in[10]. 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. The computation and storage cost of this techniques is high.

15. A Heuristic Greedy Algorithm

This is the approach that author put forwards in [10] 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.

16. Periodic Collection

In Periodic collection [11] sensor nodes independently and periodically transmits packets at rational frequency without concerning whether there is real data to send or not. This is because the traffic pattern where the object resides is changed due to the presence of real objects and this change can be easily identified by global eavesdropper. This method provides optimal location privacy but consumes substantial amount of energy and is not suited for real time application.

17. Source Simulation

In source simulation [11] 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.

18. Sink Simulation

In Sink Simulation approach explored in [11] fake sink are simulated receiving the same traffic as that of real sink. Each real sink will have fake sink simulated within its communication range. After detection of every event report

will be sent to the entire fake sink. After receiving the packet fake sink broadcasts it locally. Here the author has assumed the static fake sink, if real sink are mobile then attacker can distinguish between them. To meet high degree of location privacy large numbers of sinks are to be simulated as a result the communication cost increases.

19. Backbone Flooding

In Backbone Flooding [11] the 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.

20. 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.

21. References

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

[2] 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.

[3] 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.

[4] 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.

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

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

[7] Yong Xi, Loren Schwiebert and Weisong Shi, "Preserving Source Location Privacy in Monitoring Based Wireless Sensor Networks".

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

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

[10] 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.

[11] 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.

[12] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz," Security Issues in Wireless Sensor Networks" International Journal of Communications, Issue 1, Volume 2, 2008, pp.106-115.

.