Location Privacy in Sensor Networks: An Approach for Prevention From Adversaries

[1]Pediredla Srilatha, [2]B.Dinesh Reddy
[1,2]Vignan's Institute of Information Technology, Duvvada, Visakhapatnam, India

Abstract
A good number protocols provide security for wireless sensor networks and provide confidentiality to the messages. Even then the contextual information is exposed. The location information has paramount importance in sensor networks. Certain adversaries may derive this information and about the data sinks in the network. This may reduce the application of any network. One stronger adversary like Eavesdropper override all the existing techniques of prevention. This paper discusses various techniques to provide location privacy for source node and also for sink node. We have discussed two techniques for the prevention of the leakage of location information. They are Source Location Privacy and destination Location Privacy Techniques. It is observed that the proposed techniques are efficient and effective in protecting location information from the attacker.

Keywords
Location Privacy, Eavesdropper

I. Introduction

A Wireless Sensor Network is a network of a large number of small and less expensive devices capable of computing, communication and sensing. WSNs provide bridge between real physical and virtual worlds and they have a wide range of potential applications to industry, science, transportation, civil infrastructure, and security. Habitat and ecosystem monitoring seismic monitoring, civil structural health monitoring, monitoring groundwater contamination, rapid emergency response , industrial process monitoring, perimeter security and surveillance, automated building climate control are some applications of WSNs. Wireless Sensor Networks are found suitable for applications such as surveillance, precision agriculture, smart homes, automation, vehicular traffic management, habitat monitoring, and disaster detection. The key constraints in the development of WSNs are limited battery power, cost, memory limitation, limited computational capability, and the physical size of the sensor nodes. The common problem in the wireless sensor network technology is localization problem. Most of the applications, the network collects the data without location information which is not very useful. Location information plays a vital role in both networking and in other domains of wireless sensor network. In this paper, review has been done on the localization algorithms and different taxonomy based on basic features. As wireless sensor networks are becoming an emerging technology, it is being used in many applications. Location information necessary and useful for many functions, including measurement stamps, coherent signal processing, cluster formation, efficient querying and routing. Privacy is one of the most important problems in wireless sensor networks due to the open nature of wireless communication, which makes it very easy for adversaries to eavesdrop. When deployed in critical applications, mechanisms must be in place to secure a WSN. Security issues associated with WSNs can be categorized into two broad classes: content-related security, and contextual security. Content-related security deals with security issues related to the content of data traversing the sensor network such as data secrecy, integrity, and key exchange. Numerous efforts have recently been dedicated to content-related security issues, such as secure routing, key management and establishment, access control, and data aggregation. In many cases, it does not suffice to just address the content-related security issues. Suppose a sensitive event triggers a packet being sent over the network; while the content of the packet is encrypted, knowing which node sends the packet reveals the location where the event occurs. Contextual security is thus concerned with protecting such contextual information associated with data collection and transmission.

II. Source Location Privacy Techniques

A. Flooding Technique

In flooding, a message originator transmits its message to each of its neighbours, who in turn retransmit the message to each of their neighbours. Although flooding is known to have performance drawbacks, it nonetheless remains a popular technique for relaying information due to its ease of implementation, and the fact that minor modifications allow it to perform relatively well.

B. Fake Packet Generation

Fake packet generation creates fake sources whenever a sender notifies the sink that it has real data to send. The fake senders are away from the real source and approximately at the same distance from the sink as the real sender.

C. Phantom single-path Routing

Phantom single-path routing achieves location privacy by making every packet walk along a random path before being delivered to the sink.

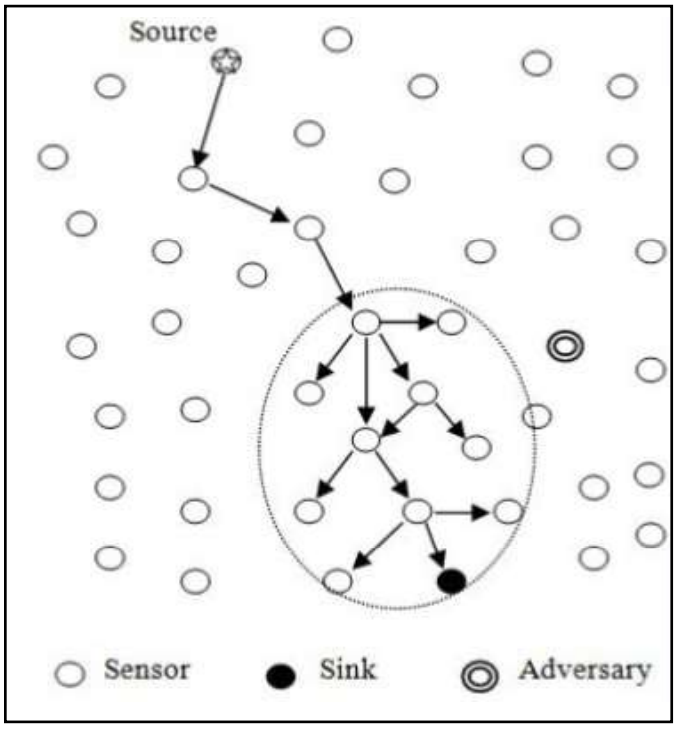

Fig. 1: Phantom Routing

E. Cyclic Entrapment

Cyclic entrapment creates looping paths at various places in the network to fool the adversary into following these loops repeatedly and thereby increase the safety period.

III. Sink Location Privacy Techniques

A. Location Privacy Routing (LPR)

A technique called Location Privacy Routing (LPR) is used along with the fake packet injection which uses randomized routing to confuse the packet tracer along with fake packets that makes the transmission completely random. Careful monitoring of packet sending time may allow adversary to get information about the data traffic flows.

B. Randomized Routing with Hidden Address (RRHA)

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 obtain 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 strong protection for the sink privacy against both active and passive attackers.

C. Bidirectional Tree Scheme (BT)

This is used to protect the end-to-end location privacy in sensor network. The real messages travel along the shortest route from the source to the sink node. Branches are designed along the shortest route in source side to travel dummy messages from leaf nodes to nodes which makes the adversary deviate from the real route, and help to protect the source location privacy.

D. Secure Location Verification Using Randomly Selected Base Stations

This method selects a random set of base stations and assumes that they are known instead of hiding them. But, it hides the details of which particular base stations are being used in a specific execution of the location determination protocol. Even if the positions of base stations are known, invader has at most a 50% chance of succeeding in one trial.

E. Base Station Location Anonymity and Security Technique (BLAST)

BLAST aims to secure the base station from both packet tracing and traffic analysis attacks and provides good privacy against the global attacker. Network is divided into blast nodes and ordinary nodes. Receiver is present somewhere nearby blast nodes.
Source node sends packet to one of the blast nodes which is then retransmitted inside blast region. The adversary is unaware of the communication between blast node and actual receiver. Hence, location privacy of the receiver is maintained.

F. BLAST with Clustering

The whole sensor network is divided into small groups called clusters using some efficient clustering algorithm. A cluster contains many members and a cluster head. An efficient shortest path algorithm is used to send data from source node to the blast node. Now, packet is retransmitted within the blast security ring using varying transmission power depending upon location of the sink node. In this approach Always the sink node is present within the security ring of blast nodes an adversary who has the global knowledge of the network traffic can easily defeat this scheme. In this case the adversary only needs to identify the region of high activity to locate the destination.

IV. Conclusion

Providing privacy for contextual information such as location of the source or sink node is very important in sensor network. An adversary can use location information and perform some attacks on either source node or destination node. In this paper, we have studied different approaches for providing location privacy for source node and sink node against adversaries in sensor network.

References

[1] V. Rini, K. Janani,"Securing the Location Privacy in wireless Sensor Networks", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 1, January-2013.

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

[3] M. Penrose,"On K-Connectivity for a Geometric Random Graph", Random Structures and Algorithms, 1999.

[4] Chinnu Mary George and Teslin Jacob,"Privacy Towards Base Station In Wireless Sensor Networks Against a Global Eavesdropper – A Survey", International Journal of Computer Science and Management Research, Vol. 2, Issue, February 2013. pp. 1493-1497.

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

[6] Amitangshu Pal,"Localization algorithms in wireless sensor networks: current approaches and future challenges", Network Protocols and algorithms, Vol. 2, No. 1.2010.

[7] Adel Youssef, Ashok Agrawala, Mohamed Younis, "Accurate anchor-free node localization in wireless sensor networks", 24th IEEE international performance, computing, and communications conference, 2005. IPCCC, pp. 465 – 470, 7-9 April 2005.

[8] E. Ngai,"On providing sink anonymity for sensor networks", In Proceedings of 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly. ACM, 2009, pp. 269–273.

[9] A. Savvides, C. Han, M. Srivastava,"Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors", Proc. ACM MobiCom, July 2001.

Pediredla Srilatha M.Tech student Vignan's Institute of Information Technology, Duvvada, Visakhapatnam, India.

B.Dinesh Reddy Asst. Professor Vignan's Institute of Information Technology, Duvvada, Visakhapatnam, India.