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

Location Privacy in Wireless Sensor Networks

Pavitha N, Santosh N. Shelke
Department of Computer Engineering
Sinhgad Academy of Engineering
Pune, Maharashtra, India

Abstract— The insecure atmospheres makes easy for an adversary to eavesdrop the network in a wireless sensor network. An eclectic collection of protocols are available for providing content privacy but the contextual information remains unprotected. So an adversary can use this contextual information to carry out attack on source node or the sink node in sensor network. The current approaches for location privacy protect the sensor network only against a local adversary. In this locale to provide location privacy for source node intervallic gathering and source imitation methods are proposed. Also for preventing sink node from adversary sink imitation and backbone flooding methods are proposed. These proposed approaches provide location privacy against global adversaries.

Keywords— sensor network, location privacy

I. INTRODUCTION

The link between encroachments in wireless communication technologies and low-cost hardware has instigated a transformation in the tenacity for which networks are used. Progressively reasonable sensors are being settled that can operate for elongated periods of time without needing exterior power, and can collect an extensive scale of data such as temperature dimensions in office buildings, pollution evaluations in ecologically sensitive surroundings, or cardiologic data for at-risk heart patients. Concurrently, there have been noteworthy advances in communication technologies, such as low-power systems capable of consistently communicating information between radio devices, and new networking prototypes that will permit radio nodes to form ad hoc connections with each other that can adjust to changing radio surroundings. Together, these improvements will provision the disposition of networks skilled for delivering massive amounts of strategic and timely data, which will expedite new classes of remote-sensing and monitoring applications.

Even if there is a massive demand for sensor applications, there are numerous troublesome challenges prowling in the future that portend the fruitful disposition of sensor networks and how efficiently they will be combined into our day-to-day lives. Conceivably fundamental between these challenges are problems connected with security and privacy.

Maintaining location privacy of a wireless sensor network is tremendously inspiring. In other words, an adversary can effortlessly capture the network movement due to the use of a broadcast medium for routing packets. They can then make traffic examination and recognize the source node. This can disclose the locations of serious and high value entities being supervised by the sensor network. On the other hand, the resource limitations of sensor nodes make it very costly to put on traditional communication methods for hiding the communication from a sensor node to the base station.

Many location privacy protective routing methods have been developed recently for wireless sensor networks. But many of these techniques work well with adversaries who have limited knowledge about the network traffic. The adversaries who have the extensive knowledge about the network can easily beat these schemes. To protect the sensor network against global adversaries we are proposing intervallic gathering, source imitation, sink imitation and backbone flooding methods.

II. LITERATURE SURVEY

This section gives a brief discussion about source location privacy procedures and sink node location privacy procedures in wireless sensor network.

A. Flooding Technique [1]

In baseline flooding [1] mechanism a sensor node notices the existence of the panda and broadcasts it to its neighbours. Neighbour nodes then broadcast to their neighbour and lastly being received by the base station. To discourse the consequence of the baseline flooding, probabilistic flooding is proposed in [1], in this approach each node broadcasts with a Pre-set probability. This pattern decreases the energy consumption but there is no assurance of the reception of data by the base station. To increase the level of privacy random walk mechanism [1] was proposed, where in phantom routing is used. In this a random walk is performed from the data source, and then a probabilistic flooding arrangement is used.

B. Phantom Routing [2]

In baseline routing method the sources offer a static route for each message so that the adversary can effortlessly back trace the route. Based on this thought, phantom routing techniques were proposed. The goal behind phantom methods is to tempt the hunter away from the source near a phantom source. [2]

C. Cyclic Entrapment [3]

Cyclic entrapment generates circling paths at several places in the network to fool the adversary into following these loops continually and thereby rise the safety period.

D. Routing through a Random Intermediate Node (RRIN) [4]

Phantom routing has no control over the phantom source without leaking significant side evidence. To solve this problem, in this protocol [4], the message source first randomly selects an intermediate node at the sensor domain based on the relative location of the sensor node defined in the grid.

E. Privacy-aware Routing [5]

This paper proposes two privacy-aware routing [5] schemes. The first routing scheme is called Random Parallel (RP) routing and the second routing scheme, Weighted Random Stride (WRS) routing was proposed.

F. Statistically Strong Source [6]

This paper [6] first proposes Policy for Dummy Traffic Generation and then proposes Policy for Embedding Real Traffic.

G. Tree-Based Diversionary Routing [7]

The implementation of the scheme [7] is divided into two phases to meet the design principles: (1) Establish the backbone route path (2) Establish redundancy diversionary routes.

H. Location Privacy Routing (LPR) [8]

A method called Location Privacy Routing (LPR) [8] 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.

I. Intrusion Tolerance and Anti-traffic Analysis Strategies [9]

To avoid the problems of LPR, de-correlation of the packet sending times [9] between a parent node and its child nodes is used. Here, it is implicit that every node sends packets at the same rate.

J. Randomized Routing with Hidden Address (RRHA) [10]

Another scheme for location privacy is Randomized Routing with Hidden Address (RRHA) [10]. 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.

K. Bidirectional Tree Scheme (BT) [11]

A Bidirectional Tree Scheme (BT) [11] scheme 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.

L. Secure Location Verification with Randomly-Selected Base Stations [12]

Secure location verification using randomly selected base stations [12] selects a random set of base stations and assumes that they are known instead of hiding them.

M. Base Station Location Anonymity and Security Technique [13]

Base station Location Anonymity and Security Technique (BLAST) [13] aims to secure the base station from both packet tracing and traffic analysis attacks and provides good privacy against the global attacker.

N. Effect of Mobility, Count of Base-stations on the Anonymity [14]

The paper [14] shows that having more than one base-station can help to improve both the average and maximum anonymity of the base station.

O. BLAST with Clustering [15]

In this case 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.

III. DESIGN GOALS

This paper has the following goals to attain:

- To prevent the adversaries from identifying the ‘source location information’ through analysing the traffic pattern.

- To avoid the adversaries from recognizing the 'sink location information' by analysing the traffic pattern.
- To stop the adversaries from getting the 'source location information' even if they are able to monitor certain area of the sensor network.
- To block the adversaries from getting the 'sink location information' even if they are able to monitor certain area of the sensor network.
- Only the SINK node is able to identify the source location through the messages received.
- Only the SOURCE node is able to identify the sink location through the messages received.

IV. ARCHITECTURAL DESIGN

System architecture is the abstract design that states the assembly and activities of a system. An architecture explanation is a recognised explanation of a system, structured in a way that chains reasoning about the structural possessions of the system. It defines the system constituents or building blocks and delivers a plan from which products can be procured, and systems developed, that will work together to implement the overall system. The System architecture is shown in figure 1.

The system has following components.

CONFIG module: The users configure the number of nodes and sink using this module.

Communication Engine module: Nodes and sink communicate using this module. This module implements multihop routing.

Node module: This module implements the wireless sensor node functionality. They sense and generate data.

Sink module: This module implements the base station functionality in the sensor network.

Eavesdropper module: This module captures the message communicated in the communication engine and tries to identify the source location and sink location.

Location Privacy Engine module: This is the important module which implements all the 4 algorithms mentioned for source and sinks location privacy.

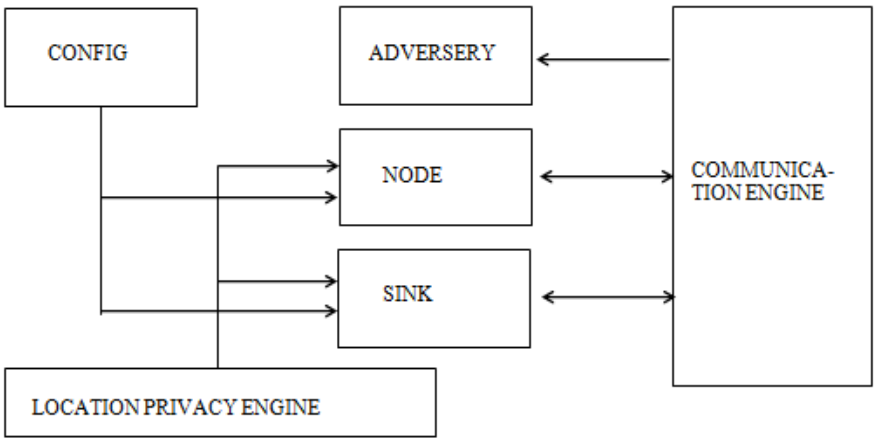

Figure 1: System Architecture

V. RESULTS

The results obtained for the developed routing algorithms are as follows.

A. Intervallic Gathering

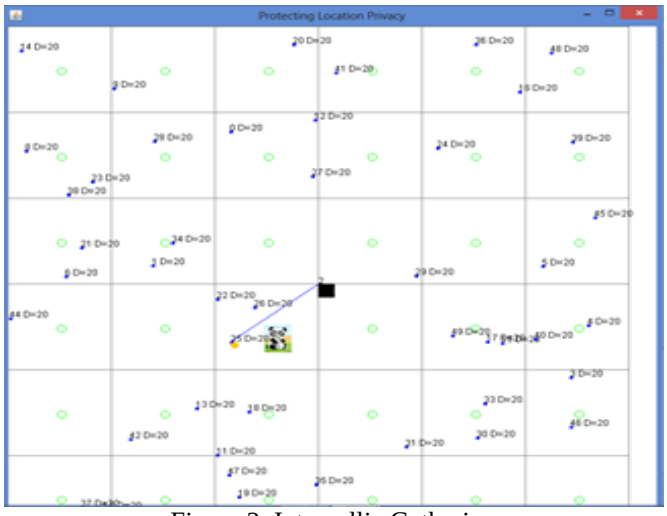

Figure 2: Intervallic Gathering

B. Source Imitation

Figure 3: Source Imitation

C. Sink Imitation

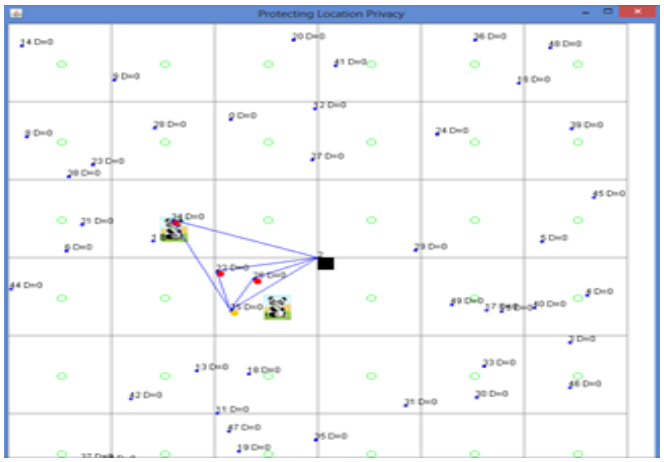

Figure 4: Sink Imitation

D. Backbone Flooding

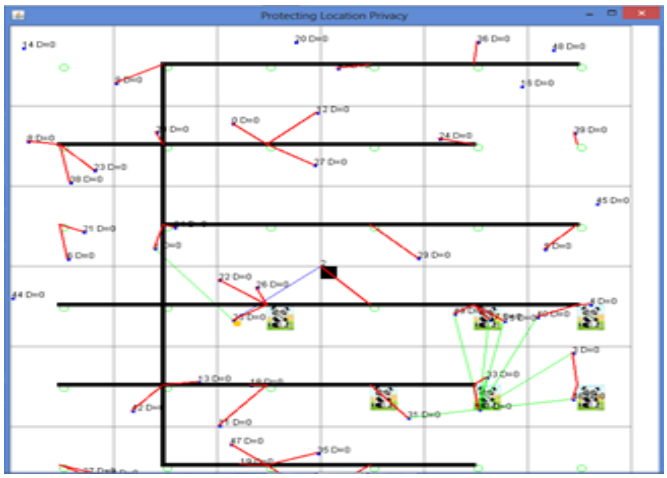

Figure 5: Backbone Flooding

VI. CONCLUSION AND FUTURE ENHANCEMENT

Providing location privacy for the source or sink node is very significant in wireless sensor network. An adversary who has knowledge about the network can use location information and easily attack either source node or destination node. In this paper, intervallic gathering, source imitation, sink imitation, backbone flooding are proposed to safe guard the wireless sensor network against global adversaries.

There are a number of ways that worth studying in the future. In particular, in this paper, we assume that the global adversary will not negotiate any of the sensor nodes; they only perform traffic analysis without observing the content of the packet. However, in practice, the global adversary may be able to negotiate a few sensor nodes in the field and perform traffic analysis with additional information from insiders.

REFERENCES

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

[2] 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.

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

[4] Y. Li and J. Ren, ``Preserving source-location privacy in wireless sensor networks," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sens. Mesh Ad Hoc Commun. Netw.*, Jun. 2009, pp. 1-9.

[5] H.Wang, B. Sheng, and Q. Li, ``Privacy-aware routing in sensor networks," *Comput. Netw.*, vol. 53, no. 9, pp. 1512_1529, 2009.

[6] M. Shao, Y. Yang, S. Zhu, and G. Cao, ``Towards statistically strong source anonymity for sensor networks," in *Proc. 27th Conf. Comput. Commun. IEEE INFOCOM*, Phoenix, AZ, USA, Apr. 2008, pp. 51_55.

[7] Jun Long, Mianxiong Dong, Ota, K., and Anfeng Liu, "Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks," *Access, IEEE* , vol.2, pp. 633-651, 2014.

[8] Y. Jian, L. Zhang , S. Chen, and Z. Zhang, "A novel scheme for protecting receiver's location privacy in wireless sensor networks," Wireless Communications, IEEE Transactions, vol. 7, no. 10, pp. 3769–3779, 2008.

[9] Jing Deng, Han, R., and Mishra S., "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," *Proc. of International Conference on Dependable Systems and Networks*, pp. 637-646, 2004.

[10] 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.

[11] W. Lou, and H. Chen, "From nowhere to somewhere: protecting end-to end location privacy in wireless sensor networks*," IEEE int'l conference on Performance Computing and Communications Conference (IPCCC)* pp. 9-11, 2010.

[12] Matthew Holiday, Subbarayan Venkatesan, and Neeraj Mittal, "Secure Location Verification with Randomly-Selected Base Stations," 2011 31st International Conference on Distributed Computing Systems Workshops. pp. 119-122.

[13] Venkata Praneeth, Dharma P. Agrawal, Varma Gottumukkala, Vaibhav Pandit, and Hailong Li, "Base-station Location Anonymity and Security Technique (BLAST) for Wireless Sensor Networks," First IEEE International Workshop on Security and Forensics in Communication Systems, 2012 IEEE.

[14] Mohamed Younis, and Zhong Ren, "Effect of Mobility and Count of Base-stations on the Anonymity of Wireless Sensor Networks," Department of Computer Science and Electrical Engineering, USA, 2011. pp. 436-441.

[15] Priti C. Shahare, Nekita A. Chavhan "An Approach to Secure Sink node's Location Privacy in Wireless Sensor Networks" Fourth Int'l Conf. on Communication Systems and Network Technologies 2014. pp. 748-751.

[16] K. Mehta, M. Wright, and D. Liu, "Location privacy in sensor networks against a global eavesdropper," IEEE Int'l Conf. 2007, pp. 314–323.

[17] Yun Zhou, Yuguang Fang, Yanchao Zhang "Securing Wireless Sensor Networks: A Survey" IEEE Communications Surveys. 2008.

