Techniques for Protecting Location Privacy of Source and Sink Node Against Global Adversaries in Sensor Network

Pavitha N[1*] ,S. N. Shelke[2]

1 Department of Computer Engineering, Sinhgad Academy of Engineering, Pune,Maharashtra, India

Email: pavithanrai@gmail.com

2Assistant Professor, Department of Computer Engineering ,Sinhgad Academy of Engineering, Pune, Maharashtra, India

Abstract:

The exposed environment of a sensor network makes relatively easy for an adversary to eavesdrop and trace packet movement in the network in order to capture the source and destination physically. Many security protocols have been developed to provide confidentiality for the content of messages whereas contextual information usually remains exposed. Such contextual information can be exploited by an adversary to derive sensitive information such as the locations of monitored objects and data sinks in the field. The existing techniques safeguard the sensor network only against the local eavesdropper who is having limited knowledge of the network topology. A stronger adversary such as global eavesdropper can still analyse the pattern of traffic and launch advanced attacks. In this paper the focus is on protecting the source and sink node's location by introducing suitable modifications to sensor routing to make it difficult for global adversaries to find the original location of the source and sink nodes. Two techniques to provide location privacy to source node that is intervallic gathering, source imitation and two techniques to ensure location privacy of data sinks that is sink imitation, backbone flooding are proposed. These techniques provide trade-offs between privacy and communication cost.

Keywords:

sensor network, eavesdropper, intervallic gathering, source imitation, sink imitation, location privacy.

I. Introduction.

Wireless sensor network (WSN) 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.

A sensor consists of four basic parts:

(i) Sensing unit

(ii) Processing unit

(iii) Transceiver unit

(iv) Power unit.

It may also have additional application dependent components such as:

(i) Location finding system

(ii) Power generator

(iii) Mobilizer.

Security issues associated with WSNs can be categorized as shown in Fig.1. The main focus of this paper is on base station and data source privacy that is location privacy.

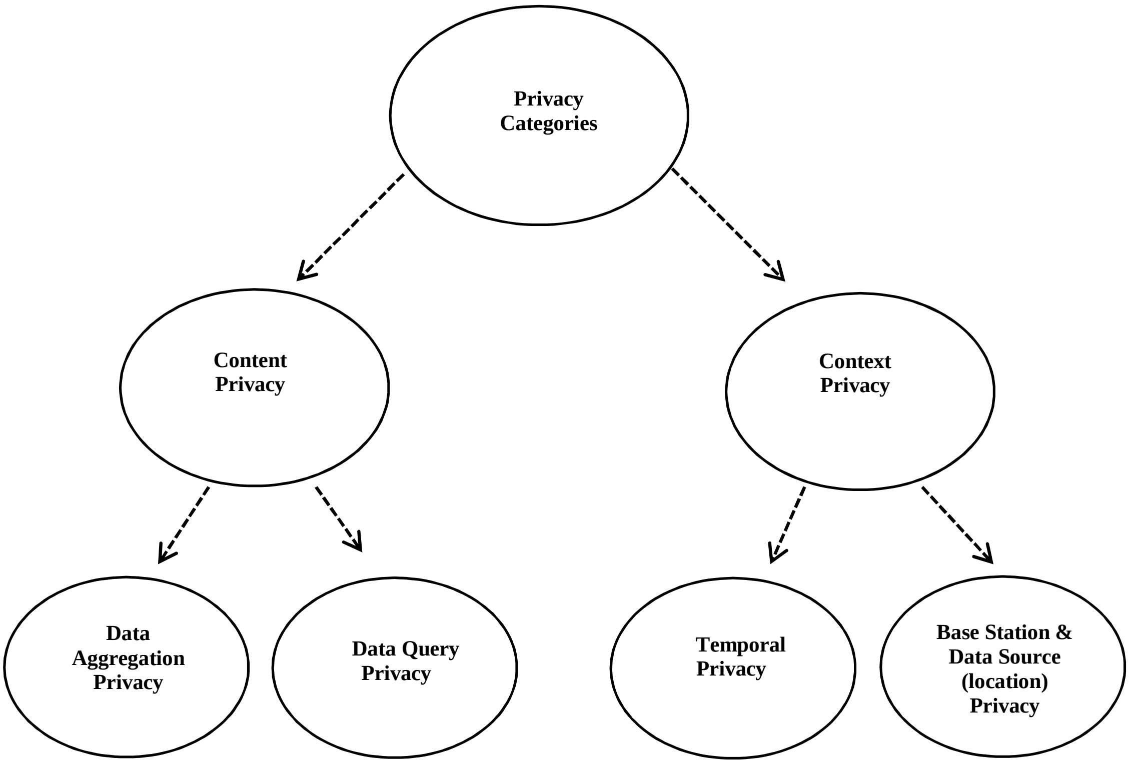

Fig. 1. Privacy Categories in Sensor Networks

II. Literature Survey

Need of Location privacy for the data source

Consider a scenario of the famous panda – hunter problem where in sensors are being deployed in the forest. The hunters are monitoring and thereby capturing the panda. A sensor node detects the presence of the panda and sends to the base station with the help of the multihop communication while rest of the sensor nodes being idle. The hunter now sees that the base station has received the presence of the panda and would like to know the exact source. The hunter can use the backtracking procedure or the traffic analysis and find the exact location of the data source. So privacy protection is needed at the data source.

Flooding technique [15]

Flooding [15] has been used to preserve the physical location of the data source .In the case of the baseline flooding mechanism a sensor node detects the presence of the panda and broadcasts it to its neighbours. These neighbours in turn broadcast to their neighbour and finally being received by the base station. The hunter notices that the base station receives multiple copies of the same message. However the effectiveness of the base lining flooding depends on the no of nodes on the transmission path between the data source and base station. If the path is too short then the hunter can use the shortest path between the data source and base station.

To address the consequence of the baseline flooding, probabilistic flooding is proposed in [15], in this mechanism not all sensors are involved in the forwarding data rather each node broadcasts with a Pre-set probability .This scheme reduces the energy consumption but there is no guarantee of the reception data by the base station due to the randomness involved this mechanism.

Higher level of privacy can be achieved with the help of the random walk mechanism [15] where in phantom routing is used. In this a random walk is performed from the data source, and then a probabilistic flooding scheme is then used.

Phantom routing [5]

In baseline routing technique the sources provide a fixed route for every message so that the adversary can easily back trace the route. Based on this observation, a new family of flooding and single-path routing protocols for sensor networks was introduced, called *phantom routing techniques*. The goal behind phantom techniques is to entice the hunter away from the source towards a phantom source.

In phantom routing, the delivery of every message experiences two phases: (1) the random walk phase, which may be a pure random walk or a directed walk, meant to direct the message to a phantom source, and (2) a subsequent flooding/single path routing stage meant to deliver the message to the sink.

Cyclic entrapment [2]

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. When an adversary is trying to analyse the traffic and trace the message’s path back to the source, if it encounters a node that is a common node of both a loop and a true path, it will need to select a direction to go on, and in doing so it may make a wrong decision and be drawn into this loop. Because there is no way for an attacker to determine that they have left the correct path until they complete a cycle, the expected time for an adversary to find the correct path is increased.

Need of Location privacy for base station

Since base station collects the entire data from the network so location privacy is needed at the data sink. Consider the scenario of the military application where in the soldiers are equipped with the sensors. The soldiers detects the presence of the enemy and send it to the base station using multihop communication, now the adversary notices that the base station receives large amount of the traffic and there by decides to destroy the base station and thus disabling the whole network. Hence the protection of the base station is very important.

Randomized Routing with Hidden Address (RRHA) [11]

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.

Bidirectional Tree Scheme (BT) [10]

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.

Base station Location Anonymity and Security Technique (BLAST) [9] with Clustering [1]

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.

III. Design Objective

To develop the techniques to provide location privacy for source node and sink node in sensor network against global adversaries.

- Location privacy to source node
  - ✓ Intervallic gathering
  - ✓ Source imitation
- Location privacy to data sinks
  - ✓ Sink imitation
  - ✓ Backbone flooding

IV. Proposed Technique

Previous techniques provide location privacy against the local adversary who has limited knowledge about the network topology. A global adversary who has the global knowledge about the network topology can easily defeat these schemes. To protect the sensor network from global adversaries we have proposed the following techniques.

A. Intervallic gathering

The main reason for the failure of previous techniques against global adversary is that the presence of a real object changes the traffic pattern. This allows the global eavesdropper to easily find out where the change happens. An intuitive solution is to make the traffic pattern autonomous of the presence of real objects. To attain this, we proposed a technique called intervallic gathering. In intervallic gathering we have every sensor node independently and periodically send packets at a realistic frequency regardless of whether there are real data to send or not.

Precisely, each of the sensor nodes has a timer that triggers an event every second. Also each sensor node has a first-in-first-out (FIFO) queue of size q for buffering received packets that transport real data reports. When the timer generates an event, the node checks whether it has any packets in its queue. If so, it removes the first packet, and forwards it to the next hop. Otherwise, it sends a dummy packet to the next hop.

B. Source imitation

Though the intervallic gathering method provides best location privacy, it consumes a considerable amount of energy. For applications that have strict latency requirements it is clearly not well suited solution. For these types of applications we proposed a technique called source imitation.

In the intervallic gathering method, every sensor node is a possible source node. To reduce energy consumption, we choose to reduce the number of possible sources in the network by selecting a subset of nodes as source nodes. In the source imitation approach, a set of virtual objects will be simulated in the field. Each of these virtual objects generates a traffic pattern similar to that of a real object to confuse the adversary.

C. Sink imitation

Similar to source imitation, an intuitive solution for sink location privacy would be to confuse the adversary by creating virtual sinks. For this purpose, we propose to create multiple virtual sinks in the network to hide the traffic between real objects and real sinks.

In sink imitation, virtual sinks will be simulated in the field. Each of the virtual sinks will receive traffic similar to the traffic received by a real sink. To achieve this, we make no distinction between fake and real sinks when sensors send packets. During deployment only we will place some virtual sinks.

In the sink imitation approach, virtual sinks are selected randomly in the network. When we need to create a large number of virtual sinks to meet high location privacy requirements, the sink imitation approach can be very expensive. The reason is that a lot of extra communication is wasted during the routing of packets to randomly selected virtual sinks. To solve this problem, we describe a backbone flooding technique in the next section.

D. Backbone flooding

In backbone flooding, we create a backbone consisting of some backbone members. While constructing backbone care should be taken such that each sink node is within the range of at least one backbone member. Also the backbone formed should cover as large an area as possible for maximum location privacy. However, finding optimal solutions to this problem is NP-hard.

We present an approximation algorithm for this problem. When we say that a sensor u covers some other sensors, we mean that u is responsible for directly transporting packets to these sensors through local broadcast. The backbone formation will terminate when the backbone members cover the essential number of sensors for the preferred level of location privacy.

V. 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, two techniques are proposed to provide location privacy to source node that is intervallic gathering, source imitation and two techniques to ensure location privacy of data sinks that is sink imitation**,** backbone flooding against global adversaries in sensor network.

References

[1] 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.

[2] 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.

[3] V. Rini, and K. Janani, "Securing the Location Privacy in wireless Sensor Networks, "International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 1, January- 2013. pp.1-4.

[4] Ying Jian, Liang Zhang, and Shigang Chen,"Protecting Receiver Location Privacy in Wireless Sensor Networks," IEEE INFOCOM 2007. pp. 1955-1963.

[5] 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.

[6] 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.

[7] Matthew Holiday, Subbarayan Venkatesan, and Neeraj Mittal, "Secure Location Verification with Randomly-Selected Base Stations," Int'l Conf. on Distributed Computing Systems Workshops 2011. pp. 119-122.

[8] Mauro Conti, Bruno Crispo, and Jeroen Willemsen, "Providing Source Location Privacy in Wireless Sensor Networks: A Survey," IEEE Communications Surveys & Tutorials, 2013.

[9] 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 Int'l Workshop on Security and Forensics in Communication Systems, 2012 IEEE.

[10] W. Lou, and H. Chen, "From nowhere to somewhere: protecting end-to end location privacy in wireless sensor networks," 2010.

[11] 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.

[12] Yong Wang, Yuyan Xue, and Byrav Ramamurthy, "A Key Management Protocol for Wireless Sensor Networks with Multiple Base Stations" IEEE Communications ICC proceedings. 2008. pp.1625-1629.

[13] 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.

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

[15] 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.

[16] YUN ZHOU, YUGUANG FANG, YANCHAO ZHANG "SECURINGWIRELESS SENSOR NETWORKS: A SURVEY" IEEE COMMUNICATIONS Surveys. 2008.

[17] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "*Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks*," Proc. ACM Conf. Wireless Network Security (WiSec 08), 2008.