International Journal of Engineering Research and General Science Volume 2, Issue 4, June-July, 2014
ISSN 2091-2730

Protecting Source and Sink Node's Location Privacy against Adversaries in Sensor Network: A Survey

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

[1]PG Scholar, Sinhgad Academy of Engineering, Pune, Maharashtra, India

[2]Assistant Professor, Sinhgad Academy of Engineering, Pune, Maharashtra, India

E-mail-pavithanrai@gmail.com

Abstract- Due to the open nature of a sensor network, it is 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. This paper is a survey of various techniques to provide location privacy in sensor network. We have analysed various techniques to provide location privacy for source node and also for sink node.

Keywords— sensor network, location privacy.

I. INTRODUCTION

Sensor networks have been extensively used in many various applications because of their ease of installation, cost efficient and portability. A WSN is usually composed of hundreds or thousands of sensor nodes. These sensor nodes are often densely deployed in a sensor field and have the capability to collect data and route data back to a base station (BS). A sensor consists of four basic parts: a sensing unit, a processing unit, a transceiver unit, and a power unit. It may also have additional application- dependent components such as a location finding system, power generator, and mobilizer. Sensing units are usually composed of two subunits: sensors and analog-to-digital converters (ADCs). The ADCs convert the analog signals produced by the sensors to digital signals based on the observed phenomenon. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes.

A transceiver unit connects the node to the network. One of the most important units is the power unit. A power unit may be finite (e.g., a single battery) or may be supported by power scavenging devices (e.g., solar cells). Most of the sensor network routing techniques and sensing tasks require knowledge of location, which is provided by a location finding system. Finally, a mobilizer may sometimes be needed to move the sensor node, depending on the application.

II. NETWORK MODEL

Usually, sensor nodes are deployed in a designated area by an authority such as the government or a military unit and then, automatically form a network through wireless communications. Sensor nodes can be either static or dynamic according to application requirements. One or several base stations (BSs) are deployed together with the network. A BS can be either static or mobile. Sensor nodes keep monitoring the network area after being deployed. After an event of interest occurs, one of the surrounding sensor nodes can detect it, generate a report, and transmit the report to a BS through multihop wireless links. Collaboration can be carried out if

multiple surrounding nodes detect the same event. In this case, one of them generates a final report after collaborating with the other nodes. The BS can process the report and then forward it through either high-quality wireless or wired links to the external world for further processing. The WSN authority can send commands or queries to a BS, which spreads those commands or queries into the network. Hence, a BS acts as a gateway between the WSN and the external world. An example is illustrated in Figure 1.[17]

Because a WSN consists of a large number of sensor nodes, usually, each sensor node is limited in its resources due to the cost consideration in manufacturing. For example, MICA2 MPR400CB , which is the most popular sensor node platform, has only 128 KB of program memory and an 8-bit ATmega128L CPU. Its data rate is 38.4 kbaud in 500 feet, and it is powered by only two AA batteries. The constrained resource cannot support complicated applications. On the other hand, usually, BSs are well designed and have more resources because they are directly attached to the external world.[17]

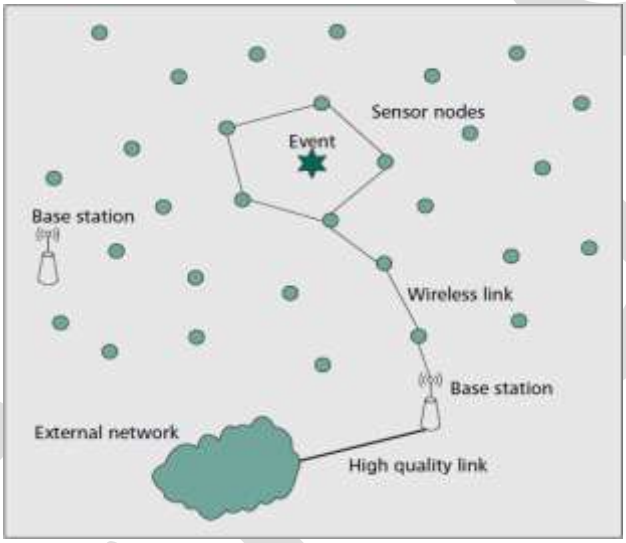

Figure 1: A wireless Sensor Network

III. SECURITY ISSUES IN SENSOR NETWORK

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.

One of the ways to increase the reliability and range of the WSNs is to employ multi-hop routing. The concept of multi-hop routing is to forward a packet to the destination using different path in case of the node failure. But, the critical issue still remains of providing security and privacy in WSNs. Therefore, preserving location privacy of the source node remains critical. Wireless sensor

networks are used in many areas such as military supervision where possibility of the eavesdropping the traffic is high to get hold of sensitive information. Exploitation of such information can cause economic losses or cause danger to human lives. To protect such information, researchers are finding out new ways to provide standard security services such as, availability, integrity, confidentiality and authentication. The exchange of information between sensors can disclose sensitive information which can reveal the location information of the critical modules present in the network.

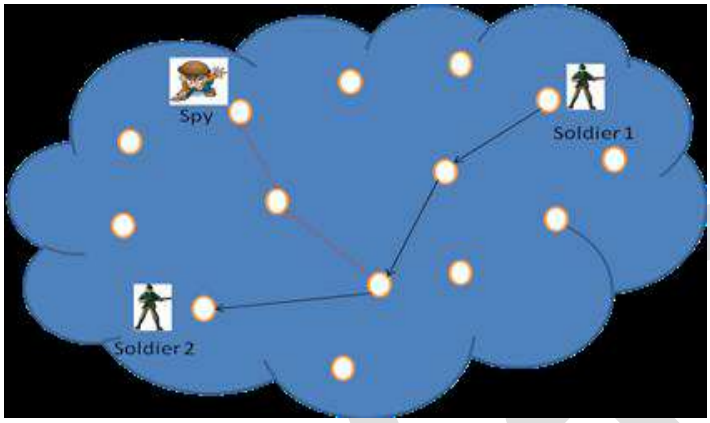

Figure 2: Threats in military surveillance

The figure 2 shows WSNs deployed in the military observation area. In this figure the soldier 1 is sending some trusted data to the soldier 2 via many intermediate nodes. Here soldier 2 is the sink node. A spy who is present on the same network tries to intercept the data by negotiating one of the intermediary nodes. The nodes may reveal trusted data to the adversary such as location of the source, location of the sink or positions of the armed forces in the locality.

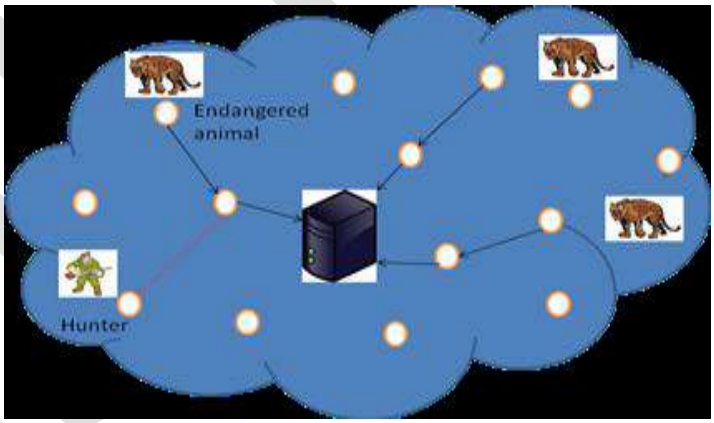

Figure 3: Threats in monitoring endangered animals

The figure 3 shows the deployment of sensor network to monitor the endangered animals in a forest. An event is generated whenever an animal is spotted in the monitored area. The hunter tries to gather this information and may capture or kill the endangered animal. The above scenario depicts the vulnerability of WSNs is more because of its open wireless medium to transmit the information from source to destination.

IV. SOURCE LOCATION PRIVACY TECHNIQUES

flooding technique[16]

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.

Fake packet generation[5]

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.

Phantom single-path routing[5]

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

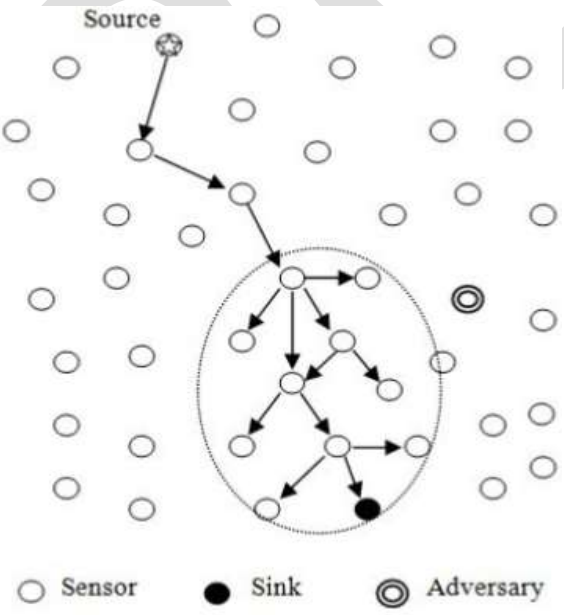

Figure 4:Phantom routing

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.

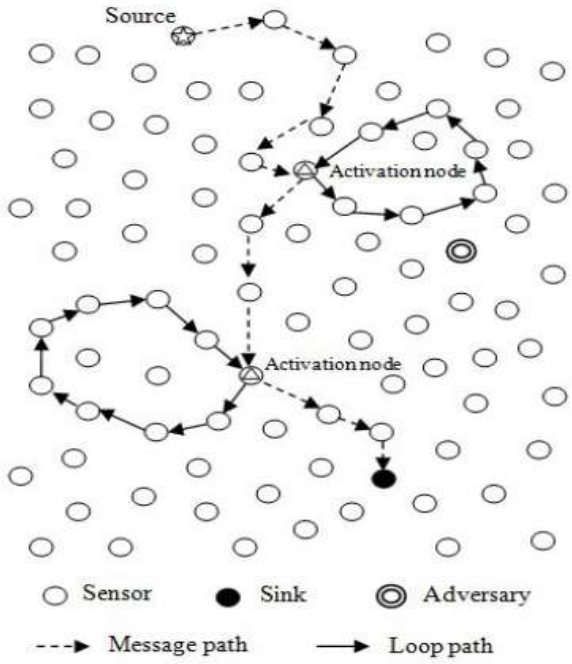

Figure 5: *Cyclic entrapment*

V. SINK LOCATION PRIVACY TECHNIQUES

Location Privacy Routing (LPR) [14]

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.

Randomized Routing with Hidden Address (RRHA) [12]

As the name suggests, the identity and location of the sink is kept private inthe 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) [11]

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.

Secure location verification using randomly selected base stations [7]

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.

Base station Location Anonymity and Security Technique (BLAST) [10]

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.

BLAST 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.

VI. 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] 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. 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 proceedings. 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] Mohamed Younis, and ZhongRen, "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.

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

[10] 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.

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

[12] 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.

[13] 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.

[14] 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.

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

[16] 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.

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