Providing Source and Sink Location Privacy against a Global Eavesdropper in Sensor Networks: a Survey

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

Abstract-

Many of the protocols used to provide sensor network security, provide confidentiality for the content of the messages but contextual information usually remains exposed. Such contextual information can be misused by an adversary to derive sensitive information such as the locations of monitored objects and data sinks in the field. Attacks on these components can significantly undermine any network application. Existing techniques protect the leakage of location information from a limited adversary who can only observe network traffic in a small region. However, a stronger adversary, the global eavesdropper, is realistic and can overthrow these existing techniques.

This paper formalizes the location privacy issues in sensor networks under this strong adversary model.

Keywords-

Sensor Network security, location privacy

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

pavithanrai@gmail.com

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

Santo.shelke@gmail.com

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. 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. Examples include wildlife habitat monitoring, security and military surveillance, and target tracking.

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 allocation finding system. Finally, a mobilizer may sometimes be needed to move the sensor node, depending on the application.

Security Issues in WSN

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 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 isthus concerned with protecting such contextual information associated with data collection and transmission.

Location Privacy

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 receiver physically [1]. For applications like military surveillance, adversaries have strong incentives to eavesdrop on network traffic to obtain valuable intelligence. Abuse of such information can cause monetary losses or endanger human lives. To protect such information, researchers in sensor network security have focused considerable effort on finding ways to provide classic security services such as confidentiality, authentication, integrity, and availability. Though these are critical security requirements, they are insufficient in many applications.

It is very important to protect the receiver’s location privacy in a sensor network. First, in many sensor networks, the receiver is the most critical node of the whole network, as the responsibility of the receiver (i.e., the base station) is to collect data from all sensors. Since all sensors send data to a single node (the receiver), this creates a single point of failure in the network. A sensor network can be rendered useless by taking down its receiver. Second, in some scenarios, the receiver itself can be highly sensitive. Imagine a sensor network deployed in a battlefield, where the receiver is carried by a soldier. If the location of the receiver is exposed to adversaries, the soldier will be in great danger.

The communication patterns of sensors can, by themselves, reveal a great deal of contextual information, which can disclose the location information of critical components in a sensor network. For example, in the Panda-Hunter case [2], a sensor network is deployed to track endangered giant pandas in a bamboo forest. Each panda has an electronic tag that emits a signal that can be detected by the sensors in the network. (A sensor that detects this signal is called as a source sensor.) The source sensor then forwards the location of pandas to a data sink (destination) with help of intermediate sensors. Adversary may use the communication between sensors and the data sinks to locate and later capture the monitored pandas. As another example, in military applications, the enemy can observe the communication and locate all data sinks in the field. Disclosing the locations of destinations during their communication with sensors may allow the enemy to launch calculated attacks against them and disable the network.

Location privacy is, thus, very important, especially in hostile environments. Failure to protect such information can completely subvert the intended purposes of sensor network applications. Location privacy measures, thus, need to be developed to prevent the adversary from determining the physical locations of source sensors and sinks. Due to the limited energy lifetime of battery-powered sensor nodes, these methods have to be energy efficient.

Providing location privacy in a sensor network is very challenging. First, the adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets. He can use information like packet generation time and packet generation frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. Second, sensors are usually resource constrained. It is not feasible to apply traditional anonymous communication techniques for hiding the communication between sensor nodes and destinations. We need to find alternative means to provide location privacy considering resource limitations of sensor nodes.

Recently, privacy-preserving routing techniques have been developed for sensor networks. However, the performance and efficiency of most of these existing solutions are measured against an adversary capable of eavesdropping on limited portion of the network at a time. A highly motivated adversary can easily eavesdrop on the entire network and defeat all these solutions. For example, the adversary may decide to deploy his own set of sensor nodes to monitor the communication in the target network. This is especially true in a military or industrial spying context where the adversary has strong, potentially life-or-death, incentives to gain as much information as possible from observing the traffic in the target network. Given a global view of the network traffic, the adversary can easily infer the locations of monitored objects and destinations. For Example, a region in the network with high activity should be close to a destination and region where the packets originate should be close to a monitored object.

II. PROVIDING SOURCEAND SINK LOCATION PRIVACY

Location privacy can be defined as a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others. In short, control of location information is the central issue in location privacy.

Privacy in smart environments has traditionally been related to what is known as social privacy, which refers to the ability of collecting and analysing user data without explicit consent. However, the privacy problem in WSNs has been broadened to embrace network privacy aspects. In this scenario, an attacker might analyse the network operation in order to retrieve information about the network itself and the data being collected. In the case of social privacy, the owner of the network is usually the privacy perpetrator because height collects user data when the user interacts with the environment. In the network privacy case, the adversary is an outsider who takes advantage of a sensor

Network deployed for legitimate purposes in order to obtain information which was not intended for him. Pai et al. [3] show how much information can be obtained from the network and the environment being monitored by simple observation of the network traffic.

- the frequency range might reveal the sensor platform being used. In addition, carrier frequency can help to determine the owner of the network, since different frequency bands are assigned for different purposes and organizations.
- The transmission rate at which messages are being delivered is a good indicator of the quantity and the nature of the events being monitored. The occurrence of events triggers the delivery of messages to the base station. Also, the non-occurrence of events might be an indicator of sensitive information.
- The size of the packets provides information about the type and precision of the data being collected. In particular, the use of some data aggregation protocols might produce privacy breaches because the nodes receiving a message incorporate their own sensed data into the packet payload, thus increasing the size of the packets. This feature can help an adversary to infer the proximity to the base station.
- The communication pattern might reveal the network topology. In order to extend battery lifetime, messages are usually transmitted in the shortest path between the source and the destination. Adversaries can take advantage of this knowledge to find out the location of important nodes in the network such as the base station or the sources of messages.

Another consideration about privacy in WSNs is made by Kamat et al. in [4]. They suggest that not only the occurrence of an event is important but that also the time at which this event takes place. This concept is named as temporal privacy. In mobile asset monitoring scenarios if an adversary is able to make an association between the time and position of the events being monitored, then he will be able to predict future behaviours. For example, in military scenarios, being in possession of such information can be tremendous advantage in developing more effective plans of attack. Consequently, a large amount of contextual information can be gathered by simply observing the messages being exchanged by the nodes during the network operation.

Several techniques have been proposed in the literature for protecting location privacy against global eavesdropper. In location-based services, a user may want to retrieve location-based data without revealing the location.

Source Location Privacy

Source location privacy refers to the ability of protecting the location of the events being reported by sensor nodes**.** Prior work in protecting location privacy to monitored objects sought to increase safety period, which is defined as the number of messages initiated byte current source sensor before a monitored object is traced.

The flooding technique [5] requires a source node to send out each packet through numerous paths to a destination to make it difficult for an adversary to trace the source. However, the problem is that the destination will still receive packets from the shortest path first. The adversary can thus quickly trace the source node using backtracking. This method consumes a significant amount of energy without providing much privacy in return.

Kamat et al. [4] describes two techniques for location privacy. First, they propose fake packet generation technique in which a destination creates fake sources whenever asunder 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. The other technique called Phantom routing is designed to protect the location privacy of source nodes (senders) in a sensor network. In Phantom routing, every packet takes a random walk before reaching the sink, which makes it harder for an adversary to trace the movement of packets. However, even with the ability to alter routing paths randomly, Phantom routing cannot protect the receiver’s location privacy well, because when there are many source nodes in sensor network, the traffic as a whole still points to the receiver.

Cyclic entrapment [5] creates looping paths at various places in the sensor network. This will cause a local adversary to follow these loops repeatedly and thereby increase the safety period. After deployment nodes decide whether to generate a network loop based on some probability. A loop is triggered when a real data packet is received at any of the loop activation nodes. When tracing back the path to the source node, local adversaries will at some time reach the loop, where the path forks in several directions Energy consumption and privacy provided by this method will increase as the length of the loops increase.

Yang et al. [6] propose to use proxies for the location privacy of monitored objects under global eavesdropper. The network is partitioned into cells where sensors in each cell communicate with the nearest proxy. Each cell sends traffic that follows an exponential distribution to its nearest proxy. The traffic will include dummy packets if real packets are not available. The proxies filter out dummy packets and send data to destination. The proxies also send dummy packets to destination if real event packets are not available. All packets are appropriately encrypted so that adversary is not able to distinguish between real and dummy packets. Proxy-based filtering and tree-based filtering schemes are proposed to position proxies.

In addition, Shoo et al. [8] propose to reduce the latency of real events without reducing the location privacy under a global eavesdropper. The technique makes sure that the adversary cannot determine the real traffic based on statistical analysis.

Destination Location Privacy

Destination location privacy is usually devoted to protecting the location of the base station. The base station is the most important asset in the network because it irresponsible for processing and analysing all the information collected by the sensor nodes. Additionally, it serves as an interface between the user and the monitored field, allowing the user to access or send commands to sensor nodes. Thus, an adversary aware of the location of the base station can compromise it, or even destroy it, rendering the WSN useless.

Deng et al. described techniques to provide fault tolerance against failure or compromise of individual destination or sensor nodes [7]. They also introduced a technique to protect the locations of destinations from a local eavesdropper by hashing the identification fields in packet headers. DEng et al. also presented four techniques to protect the location privacy of destination from a local eavesdropper who is capable of carrying out time correlation and rate monitoring [9]. First, they propose a multiple parents routing scheme in which for each packet a sensor node selects one of its parents randomly and forwards the packet to that parent. This makes the traffic pattern between the source and the destination more dispersed than the schemes where all the packets travel through same sequence of nodes. They then introduce techniques using controlled random walk, random fake paths, and hot spots. The controlled random walk technique adds a random walk to the multiple parents routing scheme causing the traffic pattern to be more spread out and hence less vulnerable to rate monitoring. The random fake path technique is introduced to confuse an adversary from tracking a packet as it moves towards the destination, mitigating the time correlation attacks. In differential fractal propagation (DFP) technique, whenever anode transmits a real packet, its neighbour node generates a fake packet. This fake packet travels configured number of hops to confuse the adversary. They also designed a scheme for creating some areas of high activity locally in the sensor network called hot spots.

If such an area receives a packet, the packet has high probability of travelling through the same sequence of nodes creating an area of high activity. A local eavesdropper may be deceived into believing that this area is close to a destination. However, a global eavesdropper can notice that only some packets generated by real objects pass through these hot-spots and conclude that the destination may not necessarily be close to those hotspots.

Jean et al. proposed the location privacy routing protocol (LPR) for destination location privacy [8]. The LPR algorithm provides privacy to the destination with help of redundant hops and fake packets when data is sent to the destination. Each time a packet is forwarded to the next hop, the packet may move either closer or away from the destination. Along with the real data packets, sensors may generate fake packets that travel away from the destination to confuse the adversary.

However, these existing techniques assume a local eavesdropper. If an adversary has the global knowledge of the network traffic, it can easily defeat these schemes. For example, the adversary only needs to identify the region of high activity to locate the destination.

Global Adversaries

Previous techniques are not effective against adversaries with a larger hearing range. More powerful adversaries are able to monitor larger areas and therefore obtain a better picture of the path followed by the messages. In particular, global adversaries are capable of monitoring all the traffic generated by the WSN. This type of adversary is not necessarily a single attacker equipped with a powerful antenna [9]. In fact, several colluding attackers wisely deployed in the field might achieve an equally effective monitoring range. Such adversaries can easily detect the source of event messages among mere intermediaries because sensor nodes are programmed to immediately report event data as soon as it is detected.

In order to deal with such powerful adversaries, the general solution is to hide event messages within fake message transmissions [10]. Note that real and fake messages must be indistinguishable from the point of view of the adversary. Consequently, both types of messages must have, on average, the same length and be encrypted with a shared secret key, which allows the next hop to authenticate the message transmission while message injection is avoided. Moreover, the use of dummy traffic implies a significant waste of energy, which reduces the operational life of the sensor nodes.

III. CONCLUSION

Location privacy is of the essence to the successive deployment of wireless sensor network. Prior work that studied location privacy in sensor networks had assumed that the attacker has only a local eavesdropping capability. This assumption is unrealistic given well-funded, highly-motivated attacker. In this paper, we formalized the location privacy issues under the model of a global eavesdropper, and show the minimum average communication overhead needed for achieving certain privacy. We also presented two techniques to provide location privacy to objects and destinations against a global eavesdropper. Analysis and simulation studies show that these techniques can effectively and efficiently protect location privacy in sensor networks.

IV. REFERENCES

[1] Kiran Mehta, Donggang Liu, Member, IEEE, and Matthew Wright, "*Protecting Location Privacy In Sensor Networks Against A Global Eavesdropper*", IEEE Transactions On Mobile Computing, Vol. 11, February 2012.

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

[3] Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "*Enhancing source-location privacy in sensor network routing*" in Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS), June 2005.

[4] 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.

[5] 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

[6] M. Shoo, Y. Yang, S. Zhu, and G. Cao, "*Towards Statistically Strong Source Anonymity for Sensor Networks,*" Proc. IEEE INFOCOM, 2008.

[7] J. Deng, R. Han, and S. Mishra, "*Enhancing Base Station Security in Wireless Sensor Networks,*" Technical Report CU-CS-951-03, Univ. of Colorado, Dept. of Computer Science, 2003.

[8] Y. Jean, S. Chen, Z. Zhang, and L. Zhang, "*Protecting Receiver- Location Privacy in Wireless Sensor Networks,*" Proc. IEEE INFOCOM, pp. 1955-1963, May 2007.

[9] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks,"Proc. ACM Conf. Computer and Comm. Security (CCS '03), Oct. 2003.

[10] H. Gupta, Z. Zhou, S. Das, and Q. Gu, "*Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution*," IEEE/ACMTrans. Networking, vol. 4, no. 1, pp. 55- 67, Feb. 2006.

[11] J. Hill, M. Horton, R. Kling, and L. Krishnamurthy, "*The Platforms Enabling Wireless Sensor Networks*," Comm. ACM, vol. 47, no. 6, pp. 41-46, 2004.

[12] D.B. Johnson, D.A. Maltz, Y. Hu, and J.G. Jetcheva, "*The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*," IETF Internet draft, Feb.2002.

[13] D. Niculescu and B. Nath, "Ad Hoc Positioning System (APS) Using AoA," Proc.IEEE INFOCOM, pp. 1734-1743, Apr. 2003.

[14] I. F. Akyildiz et al., "*A Survey on Sensor Networks*," IEEE Commun.Mag., vol. 40, no. 8, Aug. 2002, pp. 102–114.

[15] V. Paruchuri, A. Duressi, M. Duressi, and L. Barolli, "Routing through Backbone Structures in Sensor Networks," Proc. 11th Int'l Conf. Parallel and Distributed Systems (ICPADS '05), 2005.

[16] C.E. Perkins, E.M. Belding-Royer, and S.R. Das, "Ad Hoc On- Demand Distance Vector (AODV) Routing," IETF Internet draft, Feb. 2003.