ISSN No. 0976-5697

Volume 6, No. 2, March-April 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review on Wireless Sensor Network Security

Gurwinder Singh
M.Tech Computer Science
Punjab Technical University, India

Nitin Bhagat
AP, M.Tech Computer Science,
Department of CSE

Abstract: Wireless device Network (WSN) is basically arrangement of distinct and dedicated sensors for observation and recording the healthiness of the surroundings and organizing the collected information at a central location. However, due to the open characteristic of wireless communications, an adversary can detect the location of a source or sink and eventually capture them by eavesdropping on the sensor nodes' transmissions and tracing the packets' trajectories in the networks. Thus the location privacy of both the source and sink becomes a critical issue in WSNs. Previous researches only focuses on the location privacy of the source or sink independently. In this paper, we address the importance of location privacy of both the source and sink and propose four schemes called forward random walk (FRW), bidirectional tree (BT), dynamic bidirectional tree (DBT) and zigzag bidirectional tree (ZBT) respectively to deliver messages from source to sink, which can protect the end-to-end location privacy against local eavesdropper. Simulation results illustrate the effectiveness of the proposed location privacy protection schemes.

Keywords: Wireless sensor networks, Local eavesdropper, Location privacy, Sensor Network Security

I. INTRODUCTION

Recent advancement in wireless communications and Micro-Electro-Mechanical Systems (MEMS) has enabled the development of low-cost Wireless Sensor Networks (WSNs), which are made up of a number of sensor nodes that are self-organized for various applications, such as mobile target detection, earthquake monitoring and habitat monitoring. In these applications, sensor nodes are deployed to detect the existence of an interested event, such as the appearance of a rare animal. The sensor nodes that detect the occurrence of the interested event will send the detection information to a sink (or base station) by multi-hop wireless communications. Such kind of systems is called event collection system which is one of the important applications in WSNs.

Due to the open characteristics of wireless communication, it is not difficult to attack wireless sensor networks with the goal of either obtaining confidential data or simply disrupting the normal operations of the WSN applications. In either case, they may involve threats to one of the following two types of WSN privacy, *content* privacy and *contextual* privacy. The former refers to the confidentiality of the content of the packets passing between the nodes in the network. This is usually guaranteed by using methods of encryption and authentication. The latter refers to the confidentiality of information about traffic patterns in the network, which may be used by adversaries to disrupt the network. The location privacy, i.e., the confidentiality of the location of either source or sink, or both, is a kind of contextual privacy [1].

A. *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 is thus concerned with protecting such contextual information associated with data collection and transmission.

B. *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. 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, 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 [2].

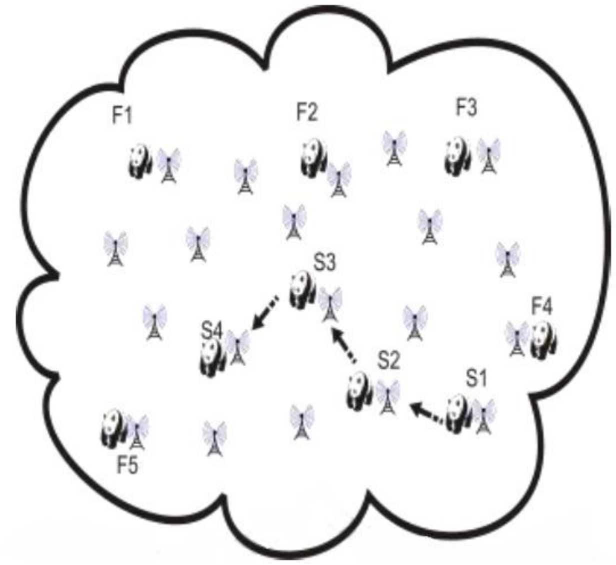

Figure 1. Movement Pattern Leaks Location Information.

We consider a WSN-based monitoring system called ‘‘Panda-Hunter’’ as shown in Fig. 1, which describes the behavior of fake objects is modeled inaccurately as remaining in one location all the time. Based on this model, the candidate traces are created at locations {F1; F2; . . . ; F6}. Sensors at each of these locations will send fake traffic to the sink, simulating a real object. However, the adversary can simply notice that the object moves around in the field along the path {S1; S2; S3; S4} and use this extra knowledge to distinguish real objects from fake ones [3].

II. PROVIDING SOURCE AND SINK LOCATION PRIVACY

A. *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.

B. *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 analyzing 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 [2].

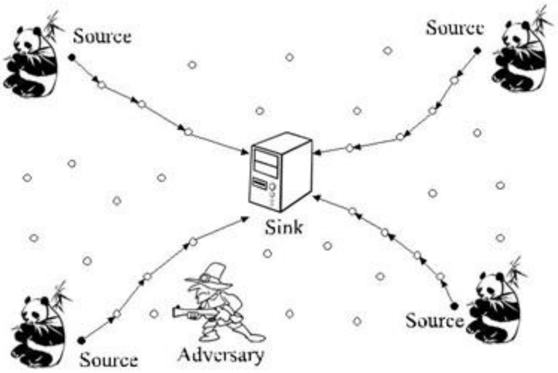

Figure 2. End-to-end location privacy threat in the habitat monitoring system.

III. RELATED WORK

Location privacy protection [4, 5–7] for WSNs has been a hot research topic during the past years. Most of existing schemes have addressed the location privacy protection of the source or sink independently:

Source location privacy protection: In [4, 8], a source location privacy protection scheme was proposed, which uses the ‘‘Panda-Hunter’’ problem as an application scenario for monitoring-oriented sensor networks where the location privacy is important. The Phantom routing protocol makes use of a random walk to prevent attackers identifying the source. Xi et al. [5] proposed a two-way random walk routing protocol (from both the source and sink) called greedy random walk, which can reduce the opportunity for an eavesdropper to collect the location information.

Sink location privacy protection: In [6], Deng et al. proposed a base station privacy scheme against the traffic-rate analysis attack by randomly delaying the transmission time of each packet. They also proposed in [9] to defend against the traffic analysis attacks. They first designed a multi-path routing to multiple destination base stations to provide intrusion tolerance against isolation of a base station. They also proposed anti-traffic analysis strategies to disguise the location privacy of the base station. LPR [7] provides receiver location privacy against the packet tracing attacks. In LPR, the directions of both incoming and outgoing from a sensor node are uniformly distributed, which makes it difficult for the adversary to ascertain the direction of the sink. Fake messages are also injected to get a longer safety period with the cost of increasing the energy consumption in the network. This motivates us to design protection schemes that aim to protect the location privacy of both the source and sink for the WSNs, which is particularly important for applications such as the habitat monitoring system in Figure 2.

In previous papers, we studied that four methods are used for location privacy protection schemes:

A. Forward random walk (FRW)
B. Bidirectional tree (BT)
C. Dynamic bidirectional tree (DBT)
D. Zigzag bidirectional tree (ZBT)

A. In ***forward random walk (FRW)*** scheme, every node relays a received packet to a node randomly chosen from its forward neighbors whose hop count to the sink is not larger than its own.

B. In ***Bidirectional tree (BT)*** scheme, real messages are delivered along the shortest path, making it possible for the Eavesdropper to infer the location of the source or sink by extending the line of the shortest path.

C. In ***dynamic bidirectional tree (DBT)*** scheme, branches of the trees are generated dynamically to further improve the performance.

D. ***Zig-zag bidirectional tree (ZBT)*** scheme is used to prevent the adversary from inferring the direction of the source or sink. Here we employ the proxy source and the proxy sink to make the real messages be delivered along a zigzag path, which includes three segments: from the source to the proxy source, from the proxy source to the proxy sink and from the proxy sink to the sink.

IV. REFERENCES

[1] Honglong Chen, Wei Lou, “On protecting end-to-end location privacy against local eavesdropper in Wireless Sensor Networks,” Elsevier, January 2014.

[2] Pavitha N, S.N. Shelke, “Providing Source and Sink Location Privacy against a Global Eavesdropper in Sensor Networks: a Survey”, International Journal of Research (IJR), vol. 1, July 2014.

[3] Deewakar Samajdar, Toran Verma, “A SURVEY ON LOCATION PRIVACY IN WIRELESS SENSOR NETWORK”, JETIR, vol. II, March 2015.

[4] P. Kamat, Y. Zhang, W. Trappe, C. Ozturk, “Enhancing source-location privacy in sensor network routing” IEEE, 2005, pp. 599–608.

[5] Y. Xi, L. Schwiebert, W. Shi, “Preserving source location privacy in monitoring-based wireless sensor networks” in: Proc. of 2nd International Workshop on Security in Systems and Networks, SSN, in Conjunction with IPDPS, 2006.

[6] J. Deng, R. Han, S. Mishra, “Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks” in: Proc. of IEEE International Conference on Dependable Systems and Networks, DSN, 2004, pp. 637–646.

[7] Y. Jian, S. Chen, Z. Zhang, L. Zhang, “Protecting receiver-location privacy in wireless sensor networks” IEEE, 2007, pp. 1955–1963.

[8] C. Ozturk, Y. Zhang, W. Trappe, “Source-location privay in energy constrained sensor network routing” ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN, in Conjunction with ACM Conference on Computer and Communications Security, 2004, pp. 88–93.

[9] J. Deng, R. Han, S. Mishra, “Countermeasures against traffic analysis attacks in wireless sensor networks” in: Proc. of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm, 2005, pp. 113–126.