Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Integrated Security and Attack Detection Scheme for Wireless Sensor Networks

N. S. KAVITHA[1], P. SUGANTHI[2], Mr. R. Subramanian[3]

Assistant Professors, CSE,,
[1,2]Erode Sengunthar Engineering College, Thudupathi, Palakarai, Tamil Nadu, India

Abstract- The wireless sensor node is a tiny device that is used to capture environment information. Sensor devices are used to capture temperature and pressure details from the environment. The sensor devices are used in hospitals, home and production plants. The main components of a sensor node are microcontroller, transceiver, external memory and power source. A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices. Sensors are used to cooperatively monitor physical or environmental conditions. Sensor network is equipped with a radio transceiver or other wireless communications device. The sensor networks are deployed with consideration of sensing and transmission coverage factors.

Sensor network security protocols provide confidentiality for the messages. Object location and data sink information are the sensitive elements in the sensor network. Two techniques are used to provide location privacy to monitored objects. They are Source-location privacy and Sink-location privacy. Periodic collection and Source simulation models are used in Source-location privacy technique. Sink simulation and backbone flooding models are used in Sink-location privacy technique. Communication cost and latency factors are consider in the privacy protection model. Source and destination location details are protected in the privacy model.

The proposed system integrates the location privacy and data security process for the wireless sensor network. Region based query model is used to improve location privacy. Confidentiality and integrity techniques are used for the security process. Rivest Cipher (RC4) algorithm and Secure Hashing Algorithms (SHA) are used for the data security.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of spatially deployed wireless sensors by which to monitor various changes of environmental conditions in a collaborative manner without relying on any underlying infrastructure support. Recently, a number of research efforts have been made to develop sensor hardware and network architectures in order to effectively deploy WSNs for a variety of applications. Due to a wide diversity of WSN application requirements, however, a general-purpose WSN design cannot fulfill the needs of all applications. Many network parameters such as sensing range, transmission range, and node density have to be carefully considered at the network design stage, according to specific applications. To achieve this, it is critical to capture the impacts of network parameters on network performance with respect to application specifications.

Intrusion detection a WSN can be regarded as a monitoring system for detecting the intruder that is invading the network domain. The intrusion detection application concerns how fast the intruder can be detected by the WSN. If sensors are deployed with a high density so that the union of all sensing ranges covers the entire network area, the intruder can be immediately detected once it approaches the network area. However, such a high-density deployment policy increases the network investment and may be even unaffordable for a large area. In fact, it is not necessary to deploy so many sensors

to cover the entire WSN area in many applications, since a network with small and scattered void areas will also be able to detect a moving intruder within a certain intrusion distance. In this case, the application can specify a required intrusion distance within which the intruder should be detected. The intrusion distance is referred as D and defined as the distance between the point the intruder enters the WSN, and the point the intruder is detected by the WSN system. This distance is of central interest to a WSN used for intrusion detection.

In this system derived the expected intrusion distance and evaluate the detection probability in different application scenarios. Given a maximal allowable intrusion distance $D_{max} = \varepsilon$, we theoretically capture the impact on the detection probability in terms of different network parameters, including node density, sensing range, and transmission range. For example, given an expected detection distance E(D), we can derive the node density with respect to sensors' sensing range, thereby knowing the total number of sensors required for WSN deployment.

In a WSN, there are two ways to detect an object: single-sensing detection and multiple-sensing detection. In the single-sensing detection, the intruder can be successfully detected by a single sensor. On the contrary, in the multiple-sensing detection, the intruder can only be detected by multiple collaborating sensors. In some applications, the sensed information provided by a single sensor might be inadequate for recognizing the intruder. It is because individual sensors can only sense a portion of the intruder. For example, the location of an intruder can only be determined from at least three sensors' sensing data. In view of this, we analyze the intrusion detection problem under two application scenarios: single-sensing detection and multiple-sensing detection.

II. RELATED WORKS

Location privacy has been an active area of research in recent years. In location-based services, a user may want to retrieve location-based data without revealing her location. Techniques such as k-anonymity [2] and private information retrieval [10] have been developed for this purpose. In pervasive computing, users' location privacy can be compromised by observing the wireless signals from user devices [7]. Random delay and dummy traffic have been suggested to mitigate these problems. Location privacy in sensor networks also falls under the general framework of location privacy. The adversary monitors the wireless transmissions to infer locations of critical infrastructure. There are some challenges unique to sensor networks. First, sensor nodes are usually battery powered, which limits their functional lifetime. Second, a sensor network is often significantly larger than the network in smart home or assisted living applications.

Source-location privacy: Prior work in protecting the location of monitored objects sought to increase the safety period, i.e., the number of messages sent by the source before the object is located by the attacker. The flooding technique has the source node send each packet through numerous paths to a sink, making it difficult for an adversary to trace the source. 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 [4] achieves location privacy by making every packet walk along a random path before being delivered to the sink. 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. However, all these techniques assume a local eavesdropper who is only capable of eavesdropping on a small region. A global eavesdropper can easily defeat these schemes by locating the first node initiating the communication with the base station.

Recently, several techniques have been proposed to deal with global eavesdroppers. Yang et al. propose to use proxies to shape the network traffic such that global eavesdroppers cannot infer the locations of monitored objects [9]. Shao et al. propose to reduce the latency of real events without reducing the location privacy under a global eavesdropper. This technique ensures that the adversary cannot determine the real traffic from statistical analysis.

Sink-location privacy: Deng et al. described a technique to protect the locations of sinks from a local eavesdropper by hashing the ID field in the packet header. In [8], it was shown that an adversary can track sinks by carrying out time correlation and rate monitoring attacks. To mitigate these two kinds of attacks, Deng et al. introduced a multiple-parent routing scheme, a controlled random walk scheme, a random fake path scheme, and a hot spots scheme. Redundant hops and fake packets are added to provide privacy when data are sent to the sink. These techniques all assume that the adversary is a local eavesdropper. A global eavesdropper can easily defeat these schemes. For example, the global eavesdropper only needs to identify the region exhibiting a high number of transmissions to locate the sink. We, thus, focus on privacy-preserving techniques designed to defend against a global eavesdropper.

III. DATA COMMUNICATION IN WSN

A wireless sensor network (WSN) typically consists of a large number of small, multifunctional, and resource-constrained sensors that are self-organized as an ad hoc network to monitor the physical world [1]. Sensor networks are often used in applications where it is difficult or infeasible to set up wired networks. Examples include wildlife habitat monitoring, security and military surveillance, and target tracking. 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. Since communication in sensor networks is much more expensive than computation, we use communication cost to measure the energy consumption of our protocols.

Providing location privacy in a sensor network is challenging. First, an adversary can easily intercept network traffic due to the use of a broadcast medium for routing packets. He can use information like packet transmission time and frequency to perform traffic analysis and infer the locations of monitored objects and data sinks. Second, sensors usually have limited processing speed and energy supplies. It is very expensive to apply traditional anonymous communication techniques for hiding the communication between sensor nodes and sinks. We need to find alternative means to provide location privacy that accounts for the resource limitations of sensor nodes. In this paper, we focus on privacy-preserving communication methods in the presence of a global eavesdropper who has a complete view of the network traffic. The contributions in this paper are twofold.

- We point out that the assumption of a global eavesdropper who can monitor the entire network traffic is often realistic for highly motivated adversaries. We then formalize the location privacy issues under such an assumption and apply an analysis based on Steiner trees to estimate the minimum communication cost required to achieve a given level of privacy.
- We provide the first formal study of how to quantitatively measure location privacy in sensor networks. We then apply the results of this study to evaluate our proposed techniques for location privacy in sensor networks. These include two techniques that hide the locations of monitored objects—periodic collection and source simulation—and two techniques that

provide location privacy to data sinks—sink simulation and backbone flooding. Our analysis and simulation studies show that these approaches are effective and efficient.

IV. PROBLEM STATEMENT

Sensor network security protocols provide confidentiality for the messages. Object location and data sink information are the sensitive elements in the sensor network. Two techniques are used to provide location privacy to monitored objects [15]. They are Source-location privacy and Sink-location privacy. Periodic collection and Source simulation models are used in Source-location privacy technique. Sink simulation and backbone flooding models are used in Sink-location privacy technique. Communication cost and latency factors are consider in the privacy protection model. Source and destination location details are protected in the privacy model. The following problems are identified from the current security methods in WSN. Location dependent attacks are not efficiently handled. Dynamic data update process is not managed. Communication overhead is high. Data security is not provided.

V. PRIVACY EVALUATION MODEL

We describe a model for evaluating the location privacy of critical components in sensor networks. In this model, the adversary deploys a snooping network to monitor the wireless transmission activity in the target network. We consider a scenario in which an adversary can monitor all transmissions of the sensors in the network. In practice, the adversary does not need to know exactly where a packet is sent or the exact location of the sensor node that sends the packet. A rough estimate of the location will be good enough for the attacker to conduct traffic analysis. However, we assume the worst case scenario: for every observed packet, the adversary knows where it is sent or which sensor node sends the packet. This indicates that each sensor i is an observation point, and a tuple (i, t, e) is available to the adversary by observing each packet e send by node i at time t. We assume that all transmissions are encrypted, and hence, the actual useful information available to the adversary is (i, t). We assume that the network begins operations at time t = 0.

The attacker's objective is to locate the source or the sink by snooping on the wireless transmissions. The main observation used by the global adversary is: there must be a sequence of spatial-temporal correlated packets involved in each communication from the source to the sink. As long as the adversary knows the routing protocol, he can easily identify all these sequences from the traffic and determine the set of possible sources and sinks. Intuitively, the defender has to create dummy sequences in the network to confuse the attacker; such dummy sequences usually require the addition of dummy traffic into the network, leading to more communication overhead. Clearly, there is a trade-off between the location privacy and the communication overhead. We develop a theoretical study of this trade-off.

We now describe our privacy model in detail. We will first describe a privacy model for source-location privacy and then extend it to include sink-location privacy. Some notations frequently used in this paper, their specific meanings will be further explained in our discussion below. A sensor network deployed for an application can be viewed as a graph G = {V, E} where the set of vertices V is the union of the set I of sensor nodes and the set of sinks. A small subset of the sensors will be the source nodes. The set E of edges includes all direct communication links between sensor nodes physically close to each other. At any point in time, from the global eavesdropper's point of view, the network can be considered to include a set SP, a set SA and a set of sensors that transfer data between sources and sinks. The adversary eavesdrops on the entire network with the intention of physically locating objects. We model each observation of the adversary as the tuple (i, t),

representing the fact that a packet has been emitted by a node i and observed by the adversary at time t.

VI. PRIVACY-PRESERVING ROUTING

We present the proposed privacy-preserving techniques for protecting the location information of monitored objects and data sinks. We assume that all communications between sensor nodes in the network are encrypted so that the contents of packets appear random to the global eavesdropper. Many key predistribution protocols can be used for this purpose [5]. We present two techniques to provide location privacy to monitored objects in sensor networks, periodic collection and source simulation. The periodic collection method achieves the optimal privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. The source simulation method provides practical trade-offs between privacy, communication overhead, and latency.

6.1. Sink-Location Privacy Techniques

Two privacy-preserving routing techniques for sink-location privacy in sensor networks: sink simulation and backbone flooding. The sink simulation method achieves location privacy by simulating sinks at specified locations, and the backbone flooding method provides location privacy by flooding the event reports in a backbone network that covers the data sinks. Both techniques provide trade-offs between privacy, communication cost, and latency. In this work, we focus on protection of passive sinks that only receive data from sensors. We will consider location privacy for sinks that broadcast packets in future work.

In backbone flooding, we send packets to a connected portion of the network, the backbone, instead of sending them directly to a few sinks. The packets are only flooded among the backbone members, the sensors that belong to this backbone. As long as the real sinks are located in the communication range of at least one backbone member, they can receive packets from any source in the field. Clearly, for a global eavesdropper, the sink could be anywhere near the backbone. We assume that the backbone is created soon after the network is deployed and that the adversary does not eavesdrop until the backbone is created.

The main component of backbone flooding is the construction of the backbone. Existing studies have focused on finding the minimal number of sensors that are needed to flood a packet so that the entire network can receive it [11]. In our case, we need to flood the packets to cover an area large enough to achieve the desired level of location privacy. In backbone flooding, we create a backbone consisting of |L| members, such that each sink is within the range of at least one backbone member. Given |L|, the backbone formed should cover as large an area as possible for maximum location privacy. However, finding optimal solutions has been shown to be NP-hard [12].

Every new sensor v added to the set L will send an election message to find the number of uncovered sensors each neighbor can cover. If $\max_v(m)$ outputs a valid sensor ID and the coverage of this node, the ID of this node will be added to L. The newly added sensor will then execute the same algorithm. If $\max_v(m) = \perp$, v will collaborate with existing nearby backbone members to find a usable sensor using Algorithm 1. The backbone is a tree structure with backbone members as the tree nodes. During the collaboration, the sensor will need to get information from its parent to find a node that can cover at least m nodes. This collaboration could continue to next level of ancestors if such a node is not known to the immediate parent. This backtracking process continues until a sensor meeting the required constraints is found. If a sensor that can cover at least m uncovered sensors is unavailable, a sensor that covers the maximum number of uncovered sensors is used.

Algorithm 1. Backtrack Procedure

```
1: procedure BACKTRACK(Coverage, Id,m)
2: ResultId← Id
3: Max ← Coverage
4: LocalMaxId← -1
5: CollectCoverageInfo(GetMyId(),NULL)
6: (LocalMaxId,Max) ←MaxId(m)
7: if Max ≥ m then
       return LocalMaxId, Max
8: else if Max < Coverage then
9: ResultId = LocalMaxId
10: Max = Coverage
11: end if
12: for EachUnvisitedNeighborBKMember do
13: (Id,Coverage) = Backtrack(Max, ResultId,m)
14: if Coverage ≥ m then
15: ResultId = Id
16: Max = Coverage
17: break
18: else if Coverage > Max then
19: Max = Coverage
20: ResultId = Id
21: end if
22: end for return ResultId,Max
23: end procedure
```

The beginning and termination of the backtracking process depends on the value of m. A value of m ≤ 1 would mean that backtracking would start only if v cannot find any neighbor that can cover at least one uncovered sensor. If m has a value greater than the number of neighbors any sensor could have, then the backtracking process would ensure that the sensor that covers the maximum number of uncovered sensors is selected. Intuitively, this would mean that an increase of m would help in covering more sensors with the help of fewer backbone members. More energy will be consumed to form a backbone for a large m due to more backtracking steps.

VII. INTEGRATED SECURITY AND ATTACK DETECTION SCHEME

The proposed system integrates the location privacy and data security process for the wireless sensor network. Region based query model is used to improve location privacy. Confidentiality and integrity techniques are used for the security process. Rivest Cipher (RC4) algorithm and Secure Hashing Algorithms (SHA) are used for the data security. The system is designed to provide location privacy and data security for sensor networks. Adhoc query processing is performed in the system. Location privacy is provided in node and sinks level. The system is divided into six major modules. They are network deployment, data capture, query submission, sink level privacy, node level privacy and security management. The network deployment module is designed to construct wireless sensor networks. The data capture process module is designed to perform data sensing operations. Query submission module is designed to handle query submission tasks. Sink level privacy is provided under Sink privacy module. The node level privacy is provided under the node privacy module. The security management module is designed to handle key and data distribution process.

7.1. Network Deployment

The network deployment module is designed to setup wireless sensor nodes. Sensor node and its properties are collected from the user. Sensor nodes are placed with its coverage information. The network is divided into a set of clusters.

7.2. Data Capture

The data capture process is performed in the sensor nodes. The data values are captured and updated into the memory. The data values are updated with time information. The sensor nodes are managed by the sink nodes.

7.3. Query Submission

The query submission process is initiated from the base station or external systems. The query values are issued with node and time information. Node and sink level query values are used in the system. Query values are prepared with node identification protection process.

7.4. Sink Level Privacy

The sink level privacy model protects the query processing under the sink nodes. The sink node collects the query value from the base station. The sink node redirects the query value to the downlink nodes. The query response is collected from the node by the sink node.

7.5. Node Level Privacy

Node level privacy model is used to protect sensor node based query values. The query values are issued for the selected node. Query details are encrypted with node level key values. Node identification values are protected by the system.

7.6. Security Management

The system provides security for query response from the sensor nodes. Rivest Cipher (RC4) algorithm is used for the data confidentiality process. Data integrity is verified using the Secure Hashing Algorithm (SHA). Key values are distributed from the base station.

VIII. CONCLUSION

Sensor networks are constructed to capture environment information. Data centers collect information from sensor devices. Location privacy is provided for the sensor node and sinks node levels. Data security is integrated with the location privacy scheme. The system manages the data collection and analysis operations in sensor networks. The system reduces the bandwidth and battery power consumption. Sensitive location and data values are protected by the system. Traffic level is reduced by the system.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: A Survey," *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002.

[2] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacygrid," *Proc. Int'l Conf. World Wide Web (WWW '08)*, 2008.

[3] BlueRadios Inc., "Order and Price Info," http://www.blueradios. Comorder info.htm, Feb. 2006.

[4] 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.

[5] H. Chan, A. Perrig and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *Proc. IEEE Symp. Security and Privacy (S&P '03)*, pp. 197-213, May 2003.

[6] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security Protocols for Sensor Networks," *Proc. ACM MobiCom,* July 2001.

[7] V. Srinivasan, |. Stankovic and K. Whitehouse, "Protecting Your Daily In-Home Activity Information from a Wireless Snooping Attack," *Proc. Int'l Conf. Ubiquitous Computing (UbiComp '08),* 2008.

[8] Deng, R. Han and S. Mishra, "Decorrelating Wireless Sensor Network Traffic to Inhibit Traffic Analysis Attacks," *Pervasive and Mobile Computing |.,* Special Issue on Security in Wireless Mobile Computing Systems, vol. 2, pp. 159-186, Apr. 2006.

[9] 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.

[10] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi and K.L. Tan, "Private Queries in Location Based Services: Anonymizers are not Necessary," *Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '08),* 2008.

[11] H. Gupta, Z. Zhou, S. Das and Q. Gu, "Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution," *IEEE/ACM Trans. Networking,* vol. 14, no. 1, pp. 55-67, Feb. 2006.

[12] 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.

[13] Kiran Mehta, Donggang Liu, Matthew Wright, "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper," *IEEE Transactions on Mobile Computing,* vol. 11, no. 2, pp. 320-336, Feb. 2012.

[14] Yun Wang, Weihuang Fu and Dharma P. Agrawal, "Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks" IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 2, February 2013.

[15]Kasim Sinan Yildirim and Aylin Kantarci, "Time Synchronization Based on Slow-Flooding in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, no. 1, January 2014

