International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 7, Issue 4 (May 2013), PP. 75-79

Source Location Privacy Preservation in Wireless Sensor Network Using Computer Based Image Recognition

S.A. Sai Sowmeyaa[1], S. Senthil Kumar[2]
[1]PG scholar, KSR College of Engineering
[2]Assistant Professor, KSR College of Engineering

Abstract:- Abrupt due to the open nature of the sensor network, the adversary can eavesdrop and track the information. In this paper, an algorithm called computer based image recognition is introduced to overcome such problem. Here the traffic is analysed using this method. In proposed scheme, the adversary model is considered where it is assumed that the adversary can monitor the small area or the entire network. Then introducing the hotspot-Locating attack, considering that through the network traffic the adversaries identify the object's location. Finally for the effective source location privacy, the irregular shapes of fake packets are sent in the form of clouds. Insertion of cloud provides more privacy and it is made active only at the need of transmission.

Keywords:- Wireless Sensor Network Security, Source location Privacy, Content privacy, Data oriented privacy, Adversary scheme.

I. INTRODUCTION

Wireless Sensor Network (WSN) found many applications in military and security applications, environmental and habitat monitoring, medical application and in data collection. In this paper, we use WSN application for data and habitat monitoring. For example, we are trying to save the particular animal organization say pandas. The movement and the activities of the pandas are regularly monitored and send the information to sink. Since WSN is open source network, the data transmission is not secure. The possibilities of attack are higher which may results in lack of data.

In wireless sensor networks, privacy is the most important concern. The privacy threats can be classified into two ways: *data-oriented privacy* and *content privacy*. In data-oriented privacy threat, the adversary can observe the packet details and after finding the location of the source the pseudonym packet is inserted. In the content privacy threat, the adversary can eavesdrops on the data transmission in the network and tracks the traffic flow. However the adversary could not interpret the data.

Some of the existing methods are based on either routing based model or global model. In the *routing based scheme*, to avoid the adversary problem the packets are sent from source to sink through different routes. By doing so, the learning of the data by the adversary is made difficult. And also this includes the *back-tracing* method i.e. the adversary tries to get the information from sink to the source. If the adversary locate the sink, through back tracing the source route can be identified. However, this increases the need of more paths which results in the increasing of energy and bandwidth.

On the contrary, *global adversary scheme* uses weak adversary model. Here the source nodes are allowed to send the packets only at the particular time slot. If there are no packets to be sent by the source node, it must send fake packets to the sink. Hence, the adversary could not find the real and the fake packets. However due to the fake packets there may be unnecessary traffic in the network and also increase the packet losses in the network.

In this paper, we first define the hotspot phenomenon which causes the inconsistency in the network due to the higher density. Secondly the adversary model [1], assuming that it can monitor the larger area through various devices is discussed. Then, for the location privacy against the attack the cloud scheme [9] is created. The cloud with the irregular fake packets is inserted to provide effective source location privacy [2].

Finally, we proposed the scheme called *computer based image recognition.* This method, is mainly used to analyse the traffic pattern while the send from source to the sink. The intruder tries to capture the data while sending from the source to the sink. After getting the data the intruder modifies the data and sends to the sink. After sink receiving the data, it verifies with the time to be received. If there happens any delay during the packet delivery, the node confirms that there received a fake packet and try to find out the attacking node. If the node that sending the fake packets is identified then the node is removed from network.

Our contribution can be summarized as follows: 1) to develop the realistic model; 2) we define hotspot phenomenon 3) to define the novel scheme for source location privacy against Hotspot-Locating attack 4) to propose a new scheme called computer based image recognition.

The remainder of this paper is organized as follows: reviews of related works are done in section II. The network and the adversary models are discussed in section III. The details about the hotspot attack are given in section IV. We presented our scheme in section V. conclusion and future work is given in section VI.

II. RELATED WORKS

Nowadays location privacy plays an important role in both wired and in the wireless networks. Generally, the location privacy can be provided in pervasive computing by ensuring that the attacker cannot associate two or more of the following pieces of information: who, where, and when. Onion routing [7] is a technique which provides the anonymous communication over a computer network. In the proposed system the nodes conceals in the network/MAC address for the mobile ad- hoc networks.

In *Routing based scheme* [7], the node sends the data through different routes to provide the source location privacy. In this method, the adversary is assumed to be monitoring only the small area. However, this scheme fails when the adversary is capable of monitoring the large area or the entire network.

This also includes the concept of the back-tracing attack. But it also fails, when the sink is identified by the adversary then through hop by hop movement finally identifies the source. This method also increases the bandwidth and power consumption.

In *Global based scheme,* the adversary is assumed to monitor the entire network. Each node can send the packets only at the periodic time slots. In the remaining time the packet sends the fake packet. If the time interval of the packet increases, then the packet delay will rapidly increase. If the fake packet allocation is increased, then the energy consumption is also increased. Through this technique complexity increases.

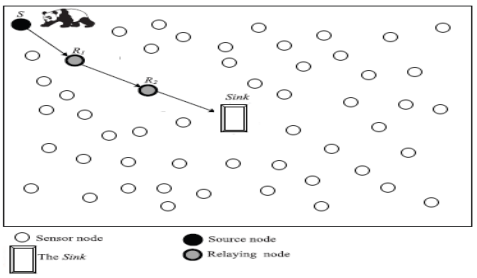

Fig .1: Architecture of WSN

Ying Jian [7] uses a routing protocol called phantom routing which is designed to protect the location privacy of the source nodes in the sensor network. In this routing method each packet takes the random walk before reaching the destination.

Many of the schemes use the asymmetric key cryptosystem which uses the two keys for the security concern. However this method requires more energy to work, so a less energy consuming cryptosystem is needed.

III. NETWORK AND ADVERSARY MODEL

A. NETWORK MODEL

As illustrated in fig.1, the architecture of the considered WSN consists of the sensor nodes deployed in the open area. The sensor nodes are the device with the low computational power and use public key cryptography, but perform the operations like sensing, data processing and communication operations. Here the communications within the network by the sensor nodes are bidirectional.

B. ADVERSARY MODEL

The adversary is capable of monitoring the data transmission in the network and learns the data. The adversary distributes the devices random to monitor the data say observation points.

Here the adversary is assumed to have the following characteristics:

1. Passive: In networks, attacks are two types, *passive and active*. In active attack, the adversary will not harm the data. But the passive attack is more dangerous because in this type of attack the adversary will harm the data by decrypting the original data.
2. Use well equipped devices: For the data monitoring, considering the adversary uses the well equipped devices which can also monitor the larger area in the network.
3. Technology: If adversary finds the location, it needs to know considered technology. Assuming that the adversary knows the privacy preserving scheme and the cryptosystem methods.

IV. HOTSPOT-LOCATING ATTACK

A hotspot is formed when the more number of packets arises from the small area. Due to more number of packets there may be traffic in the network. Through this the adversary can try to learn the data. To avoid this problem the packets are send in the form of the cloud with irregular shapes which makes inconsistency to the adversary to track the data from network. The adversary randomly distributes the devices for monitoring the data transmission. If adversary finds the area but there is no animal say panda, then it is known as the false positive. However the adversaries are well equipped to track the data during the transmission.

The adversary attempts to make use of the fact that the sensor nodes at the hotspot send more packet than the other region. Since hotspot means the group of animals stay together for several reason, example, shelter and food.

Different phases are considered for the hotspot-Locating attack [9] using the adversary model. This process involves the three phases: Identifying, Monitoring, Analysis phase. In the identifying phase, the adversary searches the hotspot location area by its distributed device which is placed at random. In monitoring phase, the monitoring device collects the traffic information. Finally in the analysis phase, the adversary uses the network traffic to collect the data for searching the panda and to change the location.

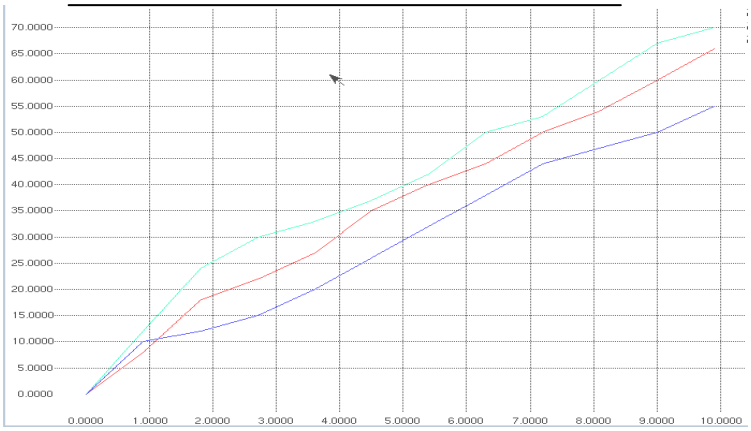

Fig.2. No. of packets vs. time

The adversary may attack the data in two ways: *Inside tracing and boundary tracing.* For the event packet transmission, the fake packet is inserted along with the real data to make the inconsistency to the adversary. The packets are encrypted using a shared key and sent to the sink. Then sink after getting the information it decrypts the data using the shared key. Then moves the fake packet to the next node periodically.

Finally, the clouds are merged to get the entire information. The merging of the two clouds reduces energy consumption and the adversary has an inconsistence in finding the fake packet and the real data. The main advantages of merging cloud are it provides the stronger privacy to the network and as said before it reduces the energy costs. Also by the cloud merging we can increase the anonymity set without the extra set.

For the merging cloud splitting attack, the adversary tries for the reduction of the cloud size. Considering the source and sink unlink ability, when the adversary eavesdrops on both, it cannot link the packet.

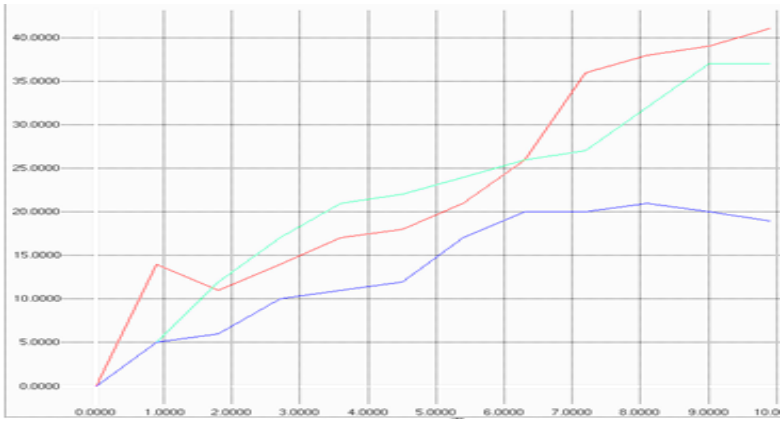

Fig.3. Network-Throughput graph

Table 1 Simulation Parameters

PARAMETER	VALUE
Number of nodes	4000
Network size	3500m x 3500m
Number of hotspot	1
Number of sensor nodes in hotspot	100
Sink location	Origin
Nodes and hotspot	Uniformly distributed

V. COMPUTER BASED IMAGE RECOGNITION ALGORITHM

The image recognition algorithm, is mainly used to analyse the traffic pattern while the send from source to the sink. The intruder tries to capture the data while sending from the source to the sink. After getting the data the intruder modifies the data and sends to the sink. After sink receiving the data, it verifies with the time to be received. If there happens any delay during the packet delivery, the node confirms that there received a fake packet and try to find out the attacking node. If the node that sending the fake node is identified then the node is removed from network.

A. Simulation results

Table 1 illustrate four thousand nodes are uniformly distributed over size of 3500m x 3500m; the sink is located at the origin. The network has one hotspot and is fixed. The number of source nodes in the hotspot is 100.

Fig.2. illustrate the energy consumption of the packet in the network. To reduce the energy cost, our scheme uses efficient cryptosystem which includes symmetric key cryptosystem and hash function. Comparing with the existing method, this method consumes less energy because the packets are sent only during the event and not periodically. So it saves the energy.

Fig.3. illustrate the throughput performance of the packet. Since the packet is sent only at the event, the network traffic can get reduced which results in the reduction of packet loss.

VI. CONCLUSION AND FUTURE WORK

The image recognition algorithm, is mainly used to analyse the traffic pattern while the send from source to the sink. The intruder tries to capture the data while sending from the source to the sink. After getting the data the intruder modifies the data and sends to the sink. After sink receiving the data, it verifies with the time to be received. If there happens any delay during the packet delivery, the node confirms that there received a fake packet and try to find out the attacking node. If the node that sending the fake node is identified then the node is removed from network.

In future work, we can use different algorithms to locate hotspots in the traffic-pattern image by the traffic analysis techniques.

REFERENCES

[1]. Na Li, Nan Zhang, Sajal K. Das, Bhavani Thuraisingham, "*Privacy preservation in wireless sensor networks: A state-of-the-art survey in Ad Hoc Networks*" (2009), p. 1501–1514, 2009.

[2]. C. Karlof and D. Wagner "*Secure routing in wireless sensor networks: Attacks and countermeasures*". Elsevier's Ad-Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, (2–3) 293–315, September 2003.

[3]. C. Ozturk, Y. Zhang, and W. Trappe, "*Source-location privacy in energy constrained sensor network routing*" in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN), October 2004, pp. 88-93.

[4]. M. Shao, Y. Yang, S. Zhu and G. Cao, "Towards statistically strong source anonymity for sensor networks", Proc. of IEEE INFOCOM'08, pp. 51–59, Phoenix, Az, USA, April 2008

[5]. T. Roosta, S. Shieh, S. Sastry: "*Taxonomy of Security Attacks in Sensor Networks*", 1st IEEE Int. Conference on System Integration and Reliability Improvements 2006, Hanoi (2006) pp. 13–15.

[6]. M. Mahmoud and X. Shen, "*Lightweight privacy-preserving routing and incentive protocol for hybrid ad hoc wireless networks"*, Proc. of IEEE INFOCOM, International Workshop on Security in Computers, Networking and Communications (SCNC), Shanghai, China, April 10-15, 2011.

[7]. Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "*A Novel Scheme for Protecting Receiver's Location Privacy in Wireless Sensor Networks*" IEEE Trans. Wireless Comm., vol. 7, no. 10, pp. 3769-3779, Oct. 2008.

[8]. Y. Li and J. Ren, "*Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks*" Proc. IEEE INFOCOM '10, Mar. 2010.

[9]. Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, "*A Cloud-Based Scheme for Protecting Source-Location Privacy against Hotspot-Locating Attack in Wireless Sensor Networks*", IEEE transactions on parallel and distributed systems, vol. 23, no. 10, pp. 1805-1818, Oct. 2012.

[10]. R. Lu, X. Lin, H. Zhu, and X. Shen, "*Timed Efficient Source Privacy Preservation Scheme for Wireless Sensor Networks*," Proc. IEEE Int'l Conf. Comm., May 2010.

[11]. Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "*An Efficient Privacy- Preserving Scheme against Traffic Analysis Attacks in Network Coding,*" Proc. IEEE INFOCOM '09, Apr. 2009.

[12]. H. Wang, B. Sheng, and Q. Li, "*Privacy-Aware Routing in Sensor Networks*," Computer Networks, vol. 53, no. 9, pp. 1512-1529, 2009.

[13]. P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "*Preventing Location-Based Identity Inference in Anonymous Spatial Queries,*" IEEE Trans. Knowledge and Data Eng., vol. 19, no. 12, pp. 1719-1733, Dec. 2007.

[14]. B. Gedik and L. Liu, *"Protecting Location Privacy with Personalized K-Anonymity: Architecture and Algorithms,"* IEEE Trans. Mobile Computing, vol. 7, no. 1, pp. 1-18, Jan. 2008.

[15]. K. Pongaliur and L. Xiao, "*Maintaining Source Privacy under Eavesdropping and Node Compromise Attacks,"* Proc. IEEE INFOCOM, Apr. 2011.