A Novel Approach towards Defeating Global Eavesdropper in Wireless Sensor Network for Location Privacy using Global Inspector

Revati A. Parate
ABHA GAIKWAD – PATIL
College of Engg., Nagpur.
revatiparate@gmail.com

Roshani Talmale
TULSIRAMJI GAIKWAD – PATIL
College of Engg. & Tech., Nagpur.
roshanikambe@rediffmaill.com

Abstract

Sensor networks are used in variety of application areas to monitor the objects. Privacy is one of the major issues of wireless sensor network as wireless transmissions are susceptible to illegal interception and detection. There are many protocols that provide content-oriented security in wireless sensor network that deals with protecting actual content of the messages but context-oriented information which is related to the actual content of the message eg. location information generally remains insecure. Such context-oriented information can be used by an adversary to infer sensitive information such as the locations of objects monitored and sinks in the network field. No. of techniques exist that are capable of defeating the limited adversary called local eavesdropper who can only observe network traffic in a small region but very few techniques has been proposed to achieve protection against the stronger adversary called global eavesdropper. Existing approaches provides different techniques for Preserving source location privacy and sink location privacy.

The proposed technique uses backbone formation algorithm and Global Inspector. Each packet is passed from source to destination through Global Inspector. This approach provides location privacy to the source as well as sinks in the sensor networks. The proposed technique also provides trade-off between privacy and communication cost.

***Keywords**: Context oriented security, eavesdropper, global inspector, location privacy, wireless Sensor network*

1. INTRODUCTION

The encroachment of wireless communication and deployment of pervasive computing technologies grow, privacy and security in such scenarios has become a great concern. People are often grateful to trade their privacy for miniature benefits and amenities brought by the modern devices and avoid the consequences of potential privacy violations. A design of new technologies taking privacy risks into account has been the talk of the town in past decade. Wireless sensor network appears to be one of the new technologies posing a serious privacy risk.

1.1 Wireless Sensor Network (WSN)

Wireless sensor network refers to a group of spatially dispersed and dedicated devices called nodes and few general purpose computing devices called base stations or sinks for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. The base stations usually act as gateways between the WSN and other networks (e.g., Internet). Nodes are outfitted with communication unit, processing unit, battery and sensor. Sensor networks can be used for wide range of applications where it is difficult or infeasible to set up wired networks.

1.2 Privacy in WSN

Privacy is one of the major issues in wireless sensor network. Privacy may be categorized into two sub-classes: content-oriented privacy and contextual privacy. Content-oriented privacy is concerned with the ability of adversaries to learn the content of transmissions in the sensor network. Contextual privacy concerns the ability of adversaries to infer information from observations of sensors and communications without access to the content of messages. In contrast to content-oriented security, the issue of contextual privacy is concerned with protecting the context associated with the dimensions and transmission of sensed data. For many scenarios, general contextual information surrounding the sensor application, specially the location of the message originator and the base station called as sink, are sensitive and must be protected. Among the different security threats in wireless sensor networks one is eavesdropping which involves attack against the confidentiality of data that is being transmitted across the network. Various privacy-preserving routing techniques have been developed for sensor networks. Most of them are designed to protect against the local eavesdropper and some of them are capable of protecting against global eavesdropper.

2. EXISTING APPROACHES

This section describes previously-proposed algorithms for source location privacy and destination location privacy.

The baseline flooding technique [2, 3] 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.

Kamat et al. describes two techniques for location privacy. First, they propose fake packet generation technique [2, 3] in which a destination creates fake sources whenever a sender 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. The other technique is called the phantom single-path routing, which achieves location privacy by making every packet generated by a source walk a random path before being delivered to the destination.

In [3] author has discussed the Single Path Routing technique in which the node forwards message only to one of its neighbours. This technique requires pre-configuration phase where sink initiates the flood setting the hop count to zero. Every time the node receives the message the hop count is incremented by one and stored in its local memory. The neighbour that has shortest distance to the sink is chosen as a path to forward the message to the sink.

In [4] author has put forward the Cyclic Entrapment Method that creates looping paths at various places in the sensor network. When message is routed from source to destination each node on a route will check if it is on a loop. If so, it will activate the loop by sending fake message. Energy consumption and privacy provided by this method will increase as the length of the loops increase.

In LPR technique [5] each sensor divides its neighbours into closer list and further list. Then the sensors select the neighbour as the next hop randomly from either of the two lists. If sensor selects the next hop from closer list then energy efficiency will be greater and if it selects next hop from the further list, privacy protection will be stronger. The LPR is augmented with fake packet injection so as to minimize the retrieval of traffic direction information by the adversary.

In [6] two phase random data collection scheme is designed to provide location privacy to mobile sinks. In first step whenever sensor has data to forward it encrypts the message with symmetric key and forwards along the random path storing a copy locally. This message travels the random path until hop cont field equals the pre-define length of the random path. In second step mobile sink moves around the network to gather data from the sensors and store it in its buffer. To evade from getting attacked and tracked, mobile sink changes its moving direction randomly.

Mehta et al. describes four techniques for location privacy in [11]. In Periodic collection sensor nodes independently and periodically transmits packets at rational frequency without concerning whether there is real data to send or not. This method provides optimal location privacy

but consumes substantial amount of energy and is not suited for real time application. In source simulation fake objects are simulated in the network field that confuses the adversary by generating the traffic similar to the real objects. In this approach set of sensor node is selected called token node as they are preloaded with the token that has unique id. Every token node emits the signal as if real object for event detection and generates the traffic as if the real event was detected thus confusing the adversary. This method is applicable for real time applications but the communication overhear is increased in order to protect location privacy. In Sink Simulation approach fake sink are simulated receiving the same traffic as that of real sink. Each real sink will have fake sink simulated within its communication range. Here the author has assumed the static fake sink, if real sink are mobile then attacker can distinguish between them. To meet high degree of location privacy large numbers of sinks are to be simulated as a result the communication cost increases. In Backbone Flooding the backbone is created by finding out minimum number of sensors that are needed to flood a packet so that whole network can receive it. The packets are sent only to the backbone and real sink can receive it as long as they are within the communication range of at least one backbone member. In this approach author has assumed static backbone which requires forwarding more packets than other nodes leading to more power consumption.

3. PROPOSED SCHEME

In this paper the new scheme is proposed to provide location privacy to source as well as sink. The scheme is based on the GI- Global Inspector. In the proposed scheme after forming the network, backbone formation algorithm is used to create the backbone members between source to destination. Packet from the source is transmitted to every backbone members. The distance between the every backbone member and destination is computed using Euclidian distance formula and the backbone member with minimum distance is selected as a global inspector. Through this global inspector only packet is forwarded to destination. The global inspector is responsible to examine whether the packet is eavesdrop or not by the adversary. The global inspector will check whether the incoming message is eavesdrop by the adversary by checking its source address and hop count in the header. If the message is eavesdrop then it will get dropped otherwise global inspector will pass it ahead. At the destination node, it will be checked if the packet has come from the trusted node i.e. global inspector, if so the packet will be accepted otherwise it will get dropped.

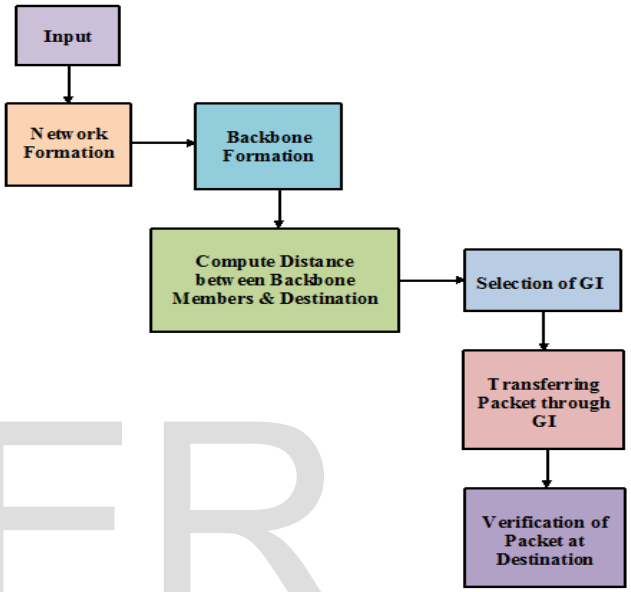

Figure1 System Architecture

4. SIMULATION RESULTS

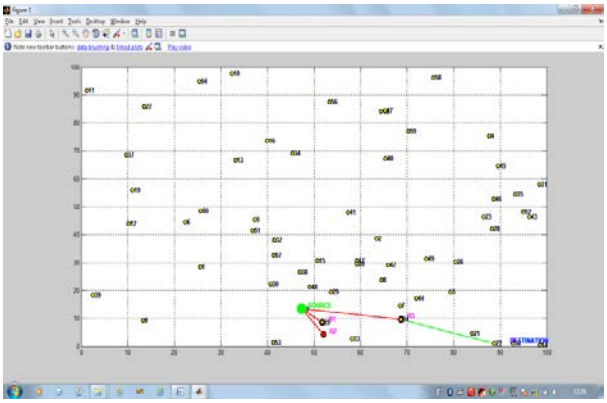

Figure 4 Transferring packets through GI

The above figure shows the packet transfer between source and destination through trusted node GI which is one of the backbone members.

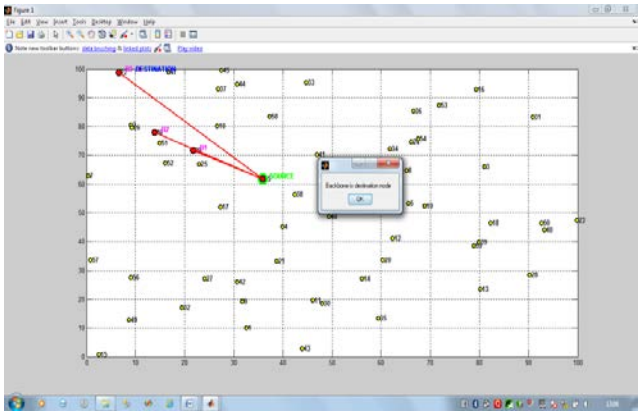

Figure 5 Packet transfer where destination is a backbone member

The above figure,shows the packet transfer between source and destination when destination itself is one of the backbone members.

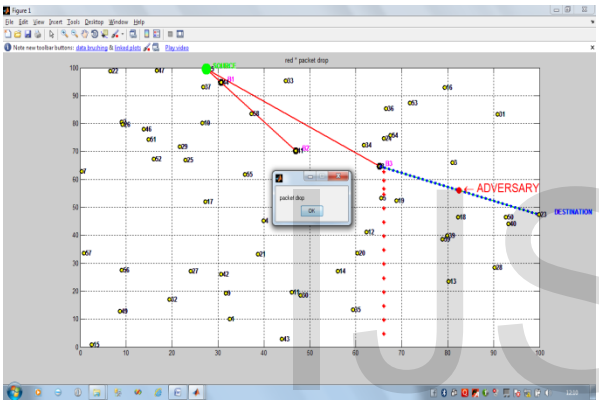

Figure 6 Packet drop due to eavesdropping of adversary

Whenever an adversary eavesdrops or monitors the wireless communication, the packet is not passed further and it is dropped as the transmission is no more reliable. Figure 6 shows the packet drop due to eavesdropping of adversary.

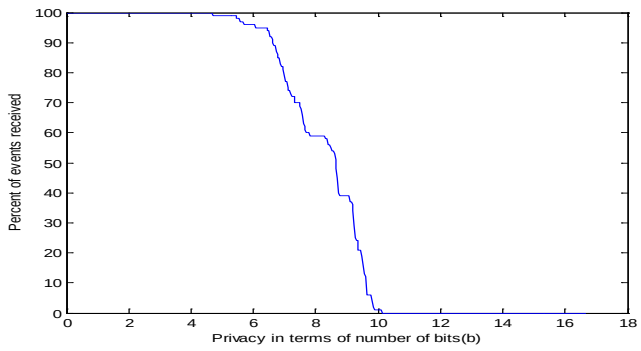

Figure 7 Event detection rate

The above graph shows that the event detection rates can be achieved better when privacy requirement is fewer i.e no. of. bits are 6 or less.

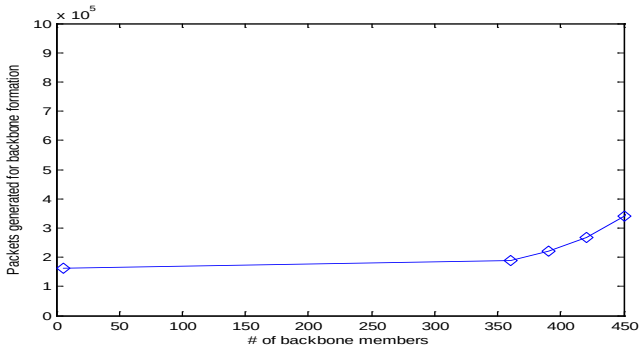

Figure 8 Energy consumed for backbone creation

The above figure shows the graph of energy consumption for creation of backbone members that is plotted in between no. of. backbone members formed and packets generated to form the backbone members. The graph shows that the no. of. packets generated increases with the size of backbone members, which in turn increases the energy consumption.

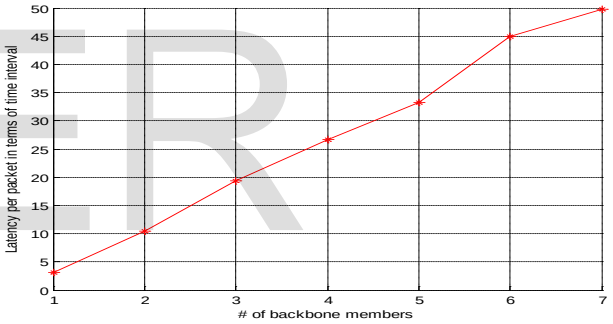

Figure 9 Effect of backbone size on latency

The above graph shows how backbone size affects the latency of packet delivery. The more the size of backbone members, the more will be packets generated for backbone formation which will result in buffering more packets and in turn increase in the latency.

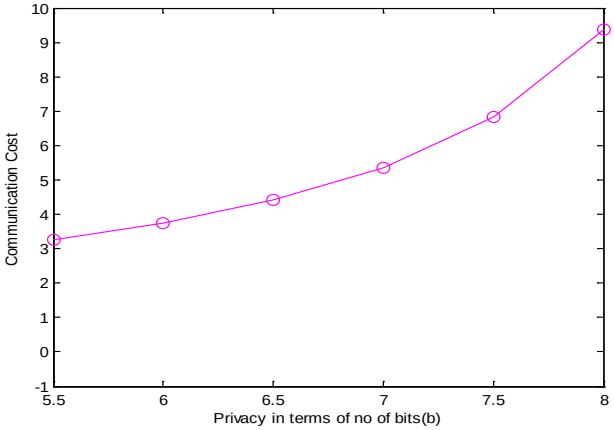

Figure 10 Effect of privacy on communication cost

The above graph shows effect of privacy on communication cost. As the privacy increases, the communication cost also increases. Thus it can be said that there is a trade-off between privacy and communication cost.

6. CONCLUSION & FUTURE WORK

Prior work about the location privacy in sensor networks had maximum time assumed that the attacker has only a local eavesdropping capability and very few approaches had assumed global eavesdropping capability. The location privacy issues are formalized under the model of a global eavesdropper. Results show the minimum average communication overhead needed for achieving certain privacy. The technique is proposed to provide location privacy to source and destination against a global eavesdropper. Analysis and simulation studies show that they can effectively and efficiently protect location privacy in sensor networks. From the results it can be concluded that:

a) Better detection rates can be achieved when privacy requirement is b=6 or fewer bits.

b) Increase in the backbone size will cause more energy to consume.

c) Latency of packet delivery increases as the size of backbone increases. This is because increase in the backbone size will cause an increase in the number of packets in the network, causing buffering of more packets and corresponding increase in latency.

d) There is a trade-off between the privacy and communication cost.

There are a number of directions that worth studying in the future. In particular, here we assume that the global eavesdropper will not compromise sensor nodes; it only performs traffic analysis without looking at the content of the packet. However, in practice, the global eavesdropper may be able to compromise a few sensor nodes in the field and perform traffic analysis with additional knowledge from insiders. This presents interesting challenges for the proposed approach. In addition, this approach can also be implemented in real sensor platform.

7. 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] 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.

[3] 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.

[4] 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.

[5] Ying Jian, Shigang Chen and Zhan Zhang, “Protecting Receiver Location Privacy in Wireless Sensor Networks”, Proc. IEEE INFOCOM, 2007.

[6] Edith C., H. Ngai and Lona Rodhe, “On Providing Location Privacy for Mobile Sinks in Wireless Sensor Networks”, Proc. ACM MSWiM, Oct 2009.

[7] Yong Xi, Loren Schwiebert and Weisong Shi, “Preserving Source Location Privacy in Monitoring Based Wireless Sensor Networks”.

[8] Yun Li and Jein Ren, “Source Location Privacy Through Dynamic Routing in Wireless sensor Network”, Proc. IEEE INFOCOM, 2010.

[9] Leron Lightfoot, Yun Li and Jian Rein, “Preserving Source Location Privacy in Wireless sensor Network using Star Routing”, Proc. IEEE Globecom, 2010.

[10] Yi Ouyang, Zhengyi Le, Donggang Liu, James Ford, Fillia Makedon, “ Source Location Privacy against Laptop–Class Attacks in Sensor Networks”, Proc. ACM SecureComm, Sept. 2008.

[11] K. Mehta, D. Liu, and M. Wright, “Protecting Location Privacy in Sensor Networks against a Global Eavesdropper,” Proc. IEEE Transactions on Mobile Computing, vol. 11, No. 2, Feb 2012.

[12] Revati A. Parate, Pragati Patil, Girish Agarwal, "Survey on Location Privacy preserving Schemes in Wireless sensor Network" International Journal of Engineering & Research Technology, Issue , Volume 1, November 2012.

[12] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz," Security Issues in Wireless Sensor Networks" International Journal of Communications, Issue 1, Volume 2, 2008, pp.106-115.