JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN COMPUTER ENGINEERING (ISSN 0975 – 6760, GIF: 01.1135, SIF: 02.502)

THE PROBLEM OF GLOBAL EAVESDROPPER IN WIRELESS COMMUNICATION IS SOLVED BY GI

Harsha C.Kunwar
Department of Computer Technology
GHRP, Nagpur, Maharashtra,
India.
E-mail: harsha.kunwar@raisoni.net

Shreya B. Pandey
Department of Computer Technology
GHRP, Nagpur, Maharashtra,
India.
E-mail: shreya.pandey@raisoni.net

Abstract— **Due to open nature of wireless sensor network it is relatively very easy for an attacker to eavesdrop and trace the packet movement in the network in order to capture the location of node physically. Such sensitive information can be trace by an adversary to derive the location of monitored object and data sink in the network. Existing scheme first formalizes location privacy issues and then proposes two techniques to provide location privacy to monitored object & two techniques to provide location privacy to data sink. After studying the adversary behavior, we present a counter measure to this problem. We propose a global inspector to preserve the privacy of packets. Global inspector will make use of Adhoc on-demand distance vector (AODV) Routing protocol to ensure security at the source as well as at sink node. This paper then performs traffic analysis to reduce the time and communication overhead based on throughput, jitter and delay. Through analysis and simulation, we demonstrate that the proposed technique are more efficient and effective for preserving location privacy at source and sink node in sensor network.**

Keywords- Sensor network, Location privacy, Global Inspector, Global Eavesdropper

I. INTRODUCTION

As the popularity and deployment of pervasive computing technologies grow, privacy of individuals is slowly steaming away. Peoples are often grateful to exchange their privacy for small benefits and conveniences brought by the modern devices and neglect the consequences of potential privacy violations. So a responsible design of new technologies should take privacy risks into account. One of the new technologies posing a serious privacy risk is the wireless sensor network.

A wireless sensor network typically comprises a large number of cheap, small and resource-constrained sensor that are self organized as an adhoc network to interact with and study the physical world[1].Sensor network can be used in application where it difficult or infeasible to setup a wired network.

Wireless sensor network

A wireless sensor network (WSN) is a heterogeneous network composed of a large number of tiny low-cost devices, denoted as nodes (or motes), and one or few general purpose computing devices referred to as base stations (or sinks). A general purpose of the WSN is to monitor some physical phenomena (e.g., temperature, barometric pressure, light) inside an area of deployment. Nodes are equipped with a communication unit (e.g., radio transceiver), processing unit, battery and sensor(s). Nodes are constrained in processing power and energy, whereas the base stations have laptop capabilities and not severely energy resources [1]. The base stations usually act as gateways between the WSN and other networks (e.g., Internet).

There is a wide variety of applications for WSNs [2], ranging from military applications (e.g., perimeter

monitoring [2] through environmental (e.g., animal habitat monitoring and health applications (e.g., patient health monitoring) to commercial applications (e.g., shopping habits monitoring, bridge structural health monitoring.

WSNs can be classified according to several aspects with impact on the security protocol design. One such aspect is the mobility of nodes and the base station. The nodes can be mobile or placed on static positions. The same holds true for the base station. Another consideration is the way the nodes are placed. The nodes can be deployed manually on specific locations following some predefined network topology or randomly deployed in an area, e.g., by dropping from a plane. The number of nodes is also a very important factor – number of nodes in a network can range from tens to tens of thousands.

II. REVIEW LITERATURE

Location privacy need to be developed to prevent the adversary from determining the physical location of source sensors and sink .Due to limited energy lifetime of battery powered sensors-nodes, these method have to be energy efficient.

Mehta et al proposed a technique source simulation, periodic collection at source node and sink simulation, backbone flooding at sink node to provide location privacy and also .formalizes the location privacy issues under a global eavesdropper and estimate average communication overhead needed to achieve a given level of privacy by imposing

Lightfoot et al proposed technique as the SinkToroidal Region (STaR) routing [6]. With this technique, the source node randomly selects an intermediate node within a designed Star area located around the SINK node The Star area is large enough to make it unpractical for an adversary to monitor the entire region. This routing protocol ensures that the intermediate node is neither too close, nor too far from the SINK node in relations to the entire network. STaR routing scheme can achieve excellent performance in energy consumption and delivery latency. Main limitation of this technique is message delivery ratio is slightly lower than the other schemes. Bamba et al described the Privacy Grid framework [5] that allows users the customization based on privacy requirements in terms of location hiding and QoS measures to control query processing overheads. Three dynamic grid-based spatial cloaking algorithms are developed for providing location k-anonymity and location l-diversity in a mobile environment. Experimental evaluation results reported and showed that compared to existing grid cloaking approaches, the dynamic grid cloaking algorithms provide much higher anonymization success rate and yet are highly efficient in terms of both time complexity and update cost.

Kamat et al portrayed that Sensor networks can be deployed to monitor valuable assets. The author studied the ability of different routing protocols to obfuscate the location of a source sensor. To achieve improved location privacy, the author proposed a new family of routing techniques, called *phantom routing*, for both the flooding and single-path classes that enhance privacy protection. *Phantom routing* techniques are desirable since they only marginally increase communication overhead, while achieving significant privacy amplification.

Ouyang et al proposed a new approach, Cyclic Entrapment, to lead adversaries into traffic loops in a sensor network. A comparison of CEM with existing methods shows that it can get a comparable source location protection while adding a comparatively low cost in terms of message latency and energy usage. As an advantage over existing techniques, it can protect a source's location while allowing for an optimal routing time for messages from that source. However investigation of the impact of source mobility, multiple sources, and message rate from the source on this problem and our approach is not known.

Deng et al addressed the issue securing a wireless sensor network against a variety of threats that can lead to the failure of the base station. First, multipath routing to multiple destination base stations is analyzed as a strategy to provide tolerance against individual base station attacks or sensor node compromises. Second, confusion of address and identification fields in packet headers via hashing functions is explored as a technique to help disguise the location of the base station from eavesdroppers. Third, relocation of the base station in the network topology is studied as a means of enhancing resiliency and mitigating the scope of damage. The author had extensively experimented with all three strategies both via simulation in ns2 and implementation on Berkeley MICA sensor motes. The results from these experiments show that a wireless sensor network can be secured quite well against attacks on base stations and compromises of sensor nodes.

III. SYSTEM ARCHITECTURE

The important part is to provide more security or authentication using Global Inspector algorithm.

A. Creation of Network

Create a network of more than ten nodes in a network. Each node having a capacity of sending a packet and receiving the same.

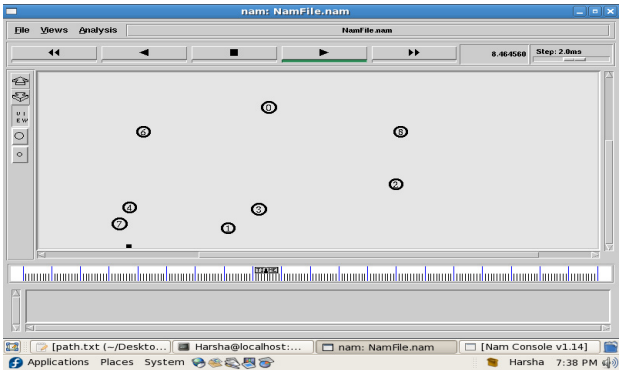


Figure 1. Creation of Network

B.

C. Imposing a GI in Network

- In a network select one node as a global inspector i.e GI which will authenticate that the packet is from trusted party.
- GI will make use of Adhoc on-demand distance vector routing i.e AODV technique to provide security at source as well as sink node.

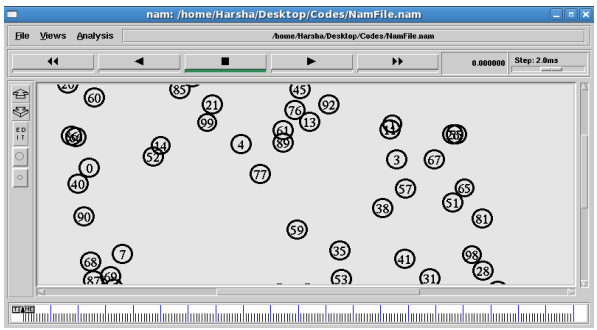


Figure 2. Selection of Node 0 as GI

D. Pass packet from trusted node

If packets travel from source to global inspector and from global inspector to destination node then destination node will come to know that the data is from party not from adversary.

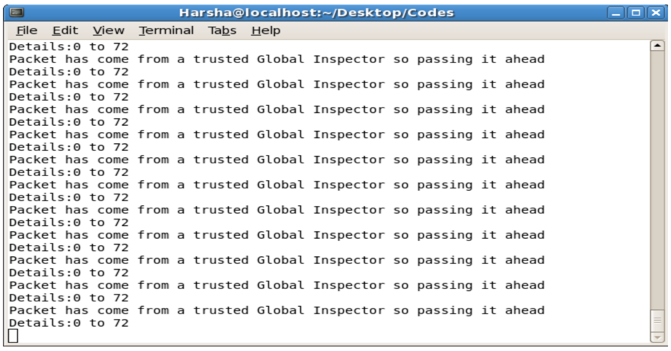
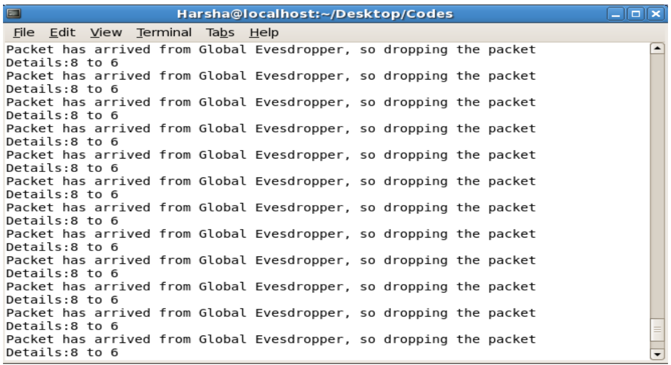


Figure 3. Results shows packets send from GI

E. Packets receive from untrusted source

- If any packet receive from untrusted party (i.e. not from GI) global eavesdropper.
- When packet receives from untrusted node i.e. global eavesdropper that packet is dropped in a network.



.

Figure 4. Results shows packets send from GE

IV. POSSIBLE CONTRIBUTION

So far to remove the drawback of existing technique we are implementing a GI i.e. global inspector and AODV routing technique to preserve the privacy at source as well as at the sink node, In GI i.e. global inspector algorithm if a packet is sent by the GI, then the nodes would accept the packet and use the same and if a packet is not sent by the GI, then the nodes would not accept the packet and drop it as it is not from a trusted source, this would ensure the privacy of the packets, and thus securing the source and sink node. The technique is shown by the following figure.

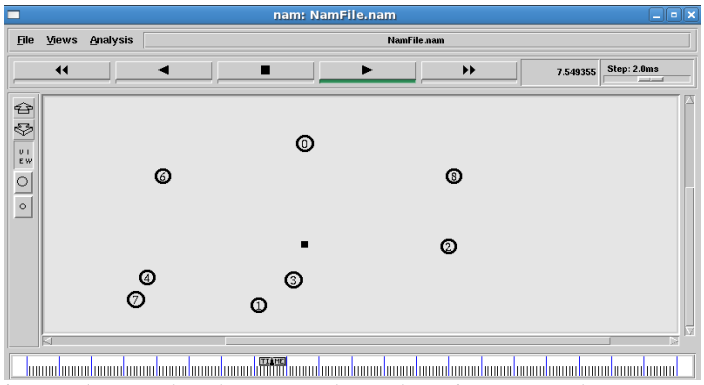


Figure 5. Results shows packets drop in Network

We are also performing traffic analysis based on various factor such throughput, jitter and delay to reduce the communication overhead at the source and destination node. The following graph shows the performance of technique.

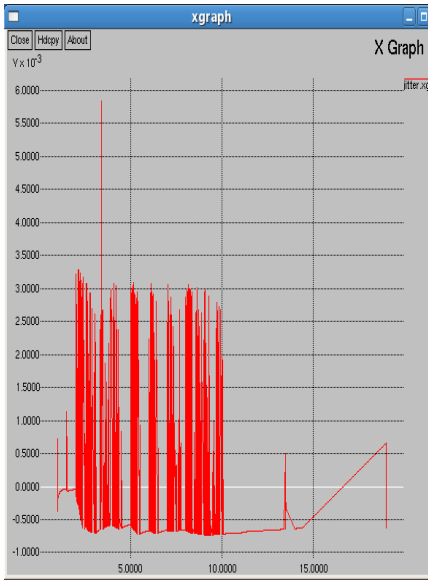


Figure 6. Results shows jitter graph

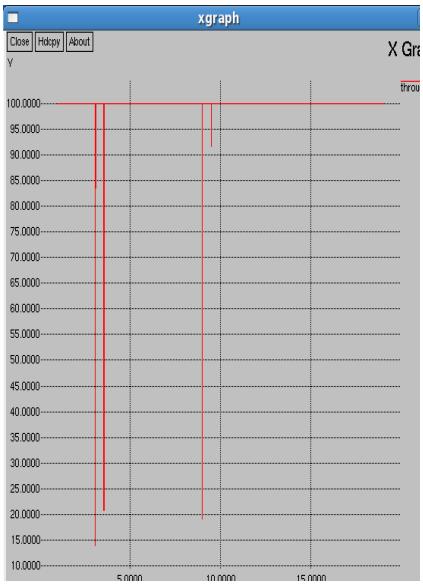


Figure 7. Results shows throughput graph

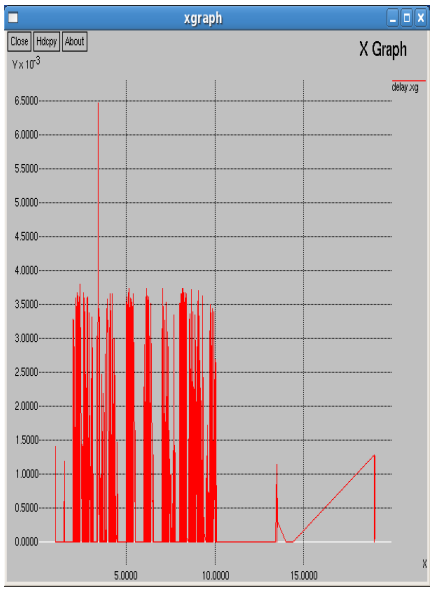


Figure 8. Results shows delay graph

Table1. Traffic Analysis

V. DESIGN

Providing location privacy in wireless sensor network using global inspector i.e. GI is implemented in NS-2.34 environment installed on Fedora Operating System in VMware Workstation and is divided into various modules as fallows :

Creation of wireless Environment and performing ping procedure module to perform verification of nodes.

A. *Selection of global inspector in a network to define trusted node.*

B. *Verification of packets either is that from trusted source or not.If packet is from trusted source then process that packet.*

C. *Received packets are not from trusted source then drop packet instead of processing.*

VI. CONCLUSION

Prior work on location privacy in sensor network assumed a global eavesdropper and provides two different techniques to protect source as well as two techniques to protect destination. We also presented technique to preserve location privacy of source object and sink against a global eavesdropper.

VII. REFERENCES

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

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

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

[4] J. Deng, R. Han, and S. Mishra, June 2004."Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks," Proc.Int'l Conf. Dependable Systems and Networks (DSN '04).

[5] Bhuvan Bamba, Ling Liu, Peter Pesti, Ting Wang, 2008 IEEE "Supporting Anonymous Location Queries in Mobile Environments with Privacy Grid".

[6] Leron Lightfoot, Yun Li, Jian Ren, 2010 IEEE "Preserving Source-Location Privacy in Wireless Sensor Network using STaR Routing".K. Elissa, "Title of paper if known," unpublished.

Yanfei Fan, 2011 IEEE "Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Network".Article in a conference proceedings:

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