**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 2, Issue. 10, October 2013, pg.186 – 192*

**RESEARCH ARTICLE**

# Location Privacy and Node Compromise Attack in Wireless Sensor Networks under Global Eavesdropper

**Ms. V. Rini[1], Ms. S. Soundharya[2], Ms. M. Shyamala[3]**

[1] Department of Information Technology, Rathinam Technical Campus, Anna University, India

[2] Department of Computer Science and Engineering, Rathinam Technical Campus, Anna University, India

[3] Department of Information Technology, Rathinam Technical Campus, Anna University, India

[1] v.rinicse90@gmail.com ; [2] soundharya.cse@rathinamcollege.com ; [3] m.shyamala193@gmail.com

*Abstract*— **In a wireless sensor networks, most important problem is to provide privacy in location. Due to compromise attack, the compromised node can leak out the event location Existing techniques assumes the global eavesdropper but does not include the compromised nodes. The global eavesdropper may be able to compromise a group of nodes or individual nodes in the network and perform traffic analysis with additional knowledge from insiders. The main objective is we need to reduce the communication overhead between the nodes. The paper then proposes the scheme to give intimate to other nodes about compromised node. Through some analysis and simulation result, we demonstrate that the proposed scheme is efficient and effective for location privacy in both source and sink in wireless sensor networks.**

***Keywords***— *Compromise attack; Global Eavesdropper; Location Privacy; Sensor networks*

## I INTRODUCTION

As wireless sensor networks was emerged recently, challenges in this technology are exclusive due to its different behavior [1] .The sensor nodes self-organize into a multi-hop wireless network that collects and forwards sensor data to a sink, usually a base station acting as an entryway to the wired Internet. The computing resources of each base station are much greater than the computational abilities of the sensor nodes. More number of sensor nodes and the less number of base stations collectively form an asymmetric and hierarchical wireless sensor network.

WSN is a method of collecting data about an environment. It comprised of multiple autonomous devices one is a sinks also known as collectors other one is a motes which is also known as sensors. After sensing the data the sensed data is send from the motes back to the sink for analysis.

A wireless sensor network Model is a collection of small randomly dispersed devices that provide three essential functions; the ability to monitor physical and environmental conditions, often

 

in real time, such as temperature, pressure, light and humidity; the ability to operate devices such as switches, motors or actuators that control those conditions; and the ability to provide efficient, reliable communications via a wireless network.

There are many applications in WSN. It is used in numerous industrial and commercial applications such as Agricultural Crop Conditions, Inventory Tracking, In-Process Parts Tracking, Automated Problem Reporting, and so on.,

WSNs can be used advantageously for rare event detection or periodic data collection for manufacturing applications. In rare event detection, sensors are used to detect and classify rare and random events, such as alarm and fault detection notifications due to important changes in machine, process, and plant security or operator actions. On the other hand, periodic data collection is required for operations such as tracking of the material flows, health monitoring of equipment/process. Such monitoring and control applications reduce the labor cost and human errors.

Many applications needs position information such as in home, forest –fire detection, military, police and so on.

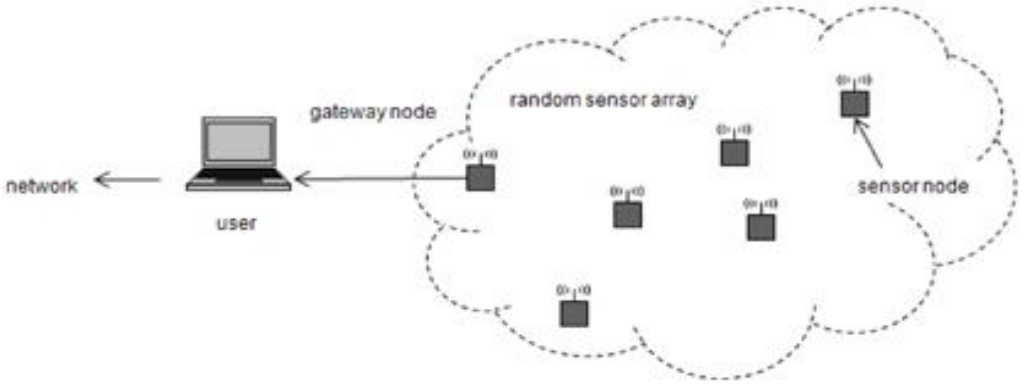


*Figure 1: Wireless Sensor Network Model*

The paper is organized as follows. Section II details the related work on location privacy. In Section III, we present the Network model and Attacks in WSN. Next, we describe the proposed scheme in Section IV. This is followed by the analysis and simulation in Section V. Finally, we have the conclusion & Future enhancement in Section VI.

## II RELATED WORK

Privacy in sensor networks has been studied in detail with some researchers giving significance to hiding the base station whereas others providing source privacy.It focuses on privacy-preserving communication methods in the presence of a global eavesdropper who has a complete view of the network traffic [3]. The contributions in this paper are two-fold. They point out that the assumption of a global eavesdropper who can monitor the entire network traffic is realistic for some applications. They also formalize the location privacy issues under this assumption and provide bounds on how much communication overhead is needed to achieve a given level privacy. They propose two techniques that prevent the leakage of location information: periodic collection and source simulation. These two schemes are both very effective at hiding the source sensors that initiate communication with the base station.

They analyze their effectiveness and evaluate their communication overhead in both analysis and simulation. 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 sink

 

simulation and backbone flooding. 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, message overhead, and latency [5]. Different applications have different requirements that may affect the usage of the periodic collection method in real-world scenarios.

To create multiple candidate traces in the network to hide the traffic generated by real objects sink-location privacy in sensor networks: sink simulation and backbone flooding. The sink simulation method achieves location privacy by simulating sinks at particular 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 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. 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. 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. If an uncovered sensor receives an election message, it will send an accept message to the sender [6]. The sender then becomes the node's parent. These accept messages are being successfully sent, all other sensors that can overhear these messages reduce their count of number of sensors they can cover by the number of unique accept messages heard.

## III NETWORK MODEL

The sensor network is a homogeneous network of sensor nodes spread over a vast area. The sensor nodes detect events and report back to the base station. The occurrence of the events can be sporadic and irregular in nature. The base station is secure and extremely powerful when compared to the deployed sensor nodes.

## IV PROPOSED SCHEME

In terms of privacy, we have already shown that none of the previous methods can provide location privacy under the assumption of a global eavesdropper. Both methods provide sink-location privacy against a global eavesdropper. The sink simulation and backbone flooding methods can provide location privacy for the sinks. The backbone flooding method is clearly more suitable for the cases where a high level of location privacy is needed. In the backbone flooding, we need to always keep the backbone connected and rebuilds the backbone from time to time to balance the communication costs between nodes.

*Eavesdropping*—for the open features of wireless channel used by sensor networks, any adversary can intercept radio communications between the wireless sensor nodes freely and easily. Data wrap may be used for malevolent acts [2].

Proposed scheme can be used for many applications requiring source node privacy. One class of applications is for tracking species of endangered animals or birds. Entities of such species need to be protected from hunters and poachers as they have great market value while at the same time they need to be studied. We consider an application in which the sensor network is deployed in a forest for sensing endangered birds (e.g. bald eagle). It is a homogeneous network, except for a secure base station, and consists of light weight sensor nodes dispersed over a large area [3]. Nodes sense the environment for the presence of endangered bird(s), and on detecting the same, report back to the base station. Multiple sensor nodes can detect the event and will independently report it back to the base station. Aggregation of the data occurs at the base station [7]. The base station gathers the information and is able to correlate it to identify the presence of the tracked entity, while also being able to study the flight patterns and their nesting habits. Given the tracked entity being swift and airborne, we can

 

have multiple sensors detecting the event in a short period of time, and then not having any detection for a prolonged duration of time. The assumption is that, if the bird swooped down at a particular location, it did so to either prey or to get water, and this increases the possibility of the bird descending to that location thereby requiring source location privacy (secrecy) for the event reporting packet. In some applications the event can be sporadic, but it must be noted that there is still other communication between the sensor nodes, resulting in the generation of packet traffic. It is a sparse deployment which has fewer nodes in the network.

When compared to existing system, the proposed scheme ensures less overhead [2]. It is much more efficient with reasonable delay and trade off is more against energy consumption. Lifetime of battery is in increased level with enormous processing speed. The anonymous technique used to hide the information between sensor nodes and sinks is more stealth than in existing scheme. Data are highly encrypted after reaching the sink. So an adversary could not locate sinks and make the sensor network non-functional by destroying them. Construct protocol for location privacy for sinks that broadcast packets. i.e. active sinks.

## V SIMULATION

We demonstrated the performance of the sensor nodes through Glomosim [4].The simulated scenario has one sink and 15 nodes which is movable nodes. During initial stage of the network deployment, the nodes are randomly deployed in a network. During this stage, the nodes grouped separately and choose the head node and form a group.

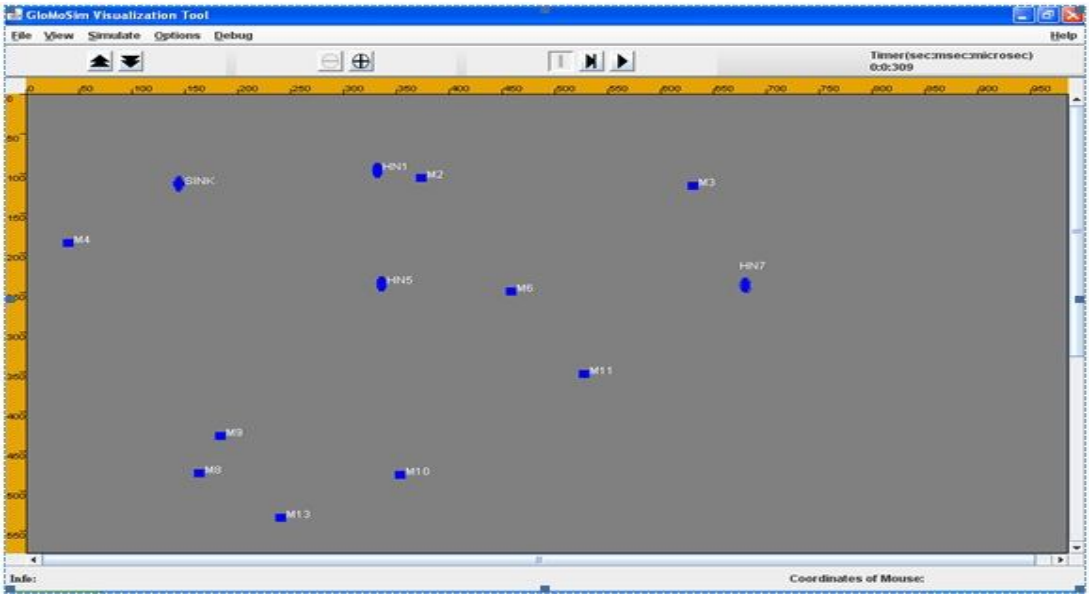


*Figure 2: Initial stage*

After the Sparse deployment of the sensor nodes sink node send the pairwise key to all the nodes. In this simulation scenario white line indicates that the key predistribution which is shown in Fig.3.This will give the location privacy.

 

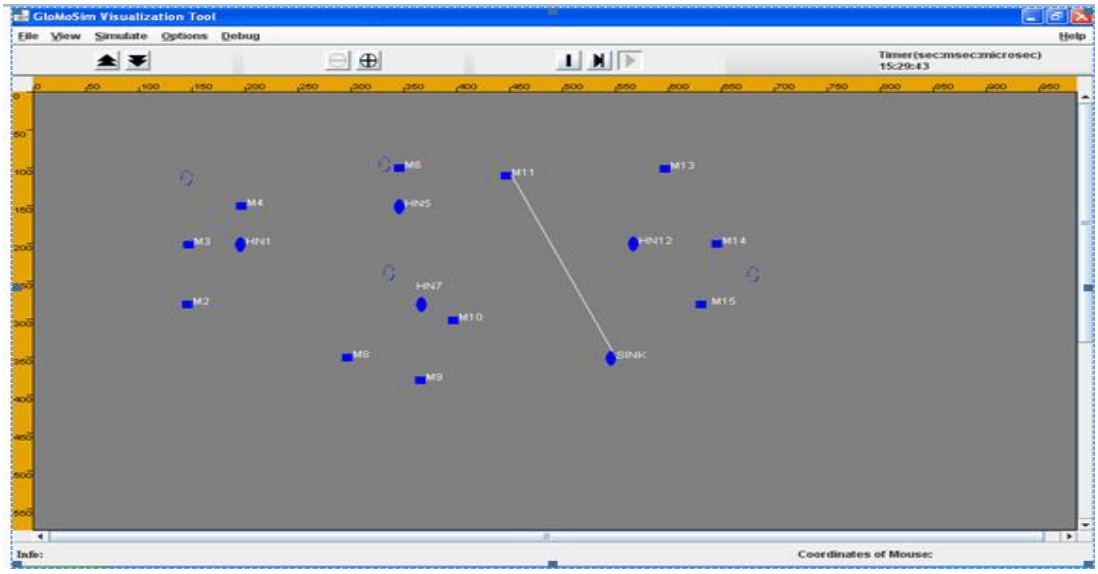


*Figure 3: Keys generation*

The nodes Hn1 and Hn2 select the member which has same capapbilities.Based on this the groups are formed. During this time it checks for Head node send the member list to that group. If the node compromises means the key for that node was changed so that node mark it as compromised node and it is denoted as black node in the simulation scenario which is shown in Fig.4 and The red line indicates success message transfer between the nodes and the sink. It is shown in Fig.5

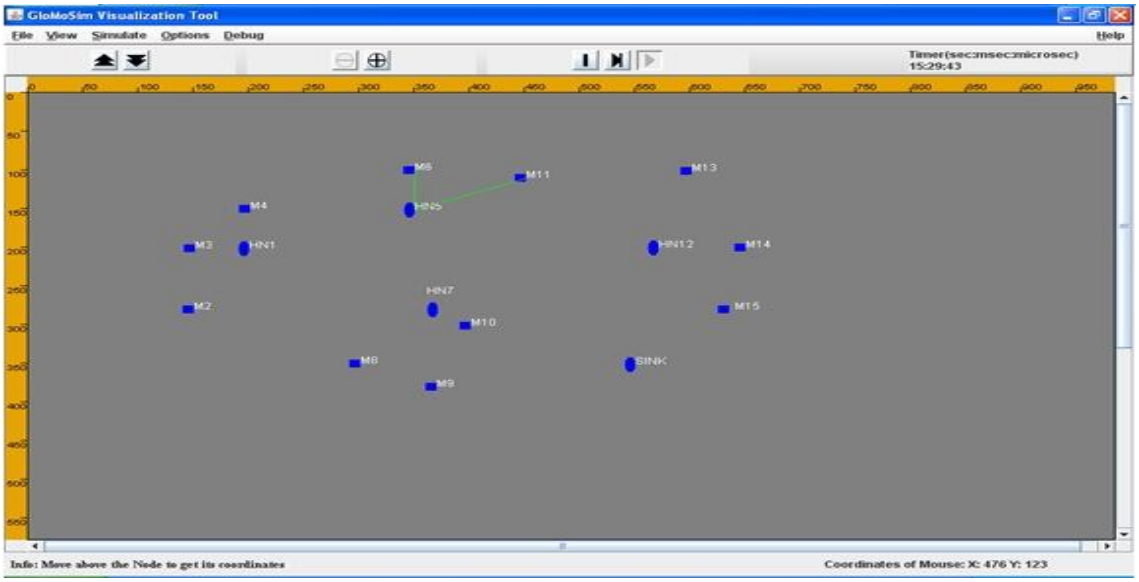


*Figure 4: Member list generation*

 

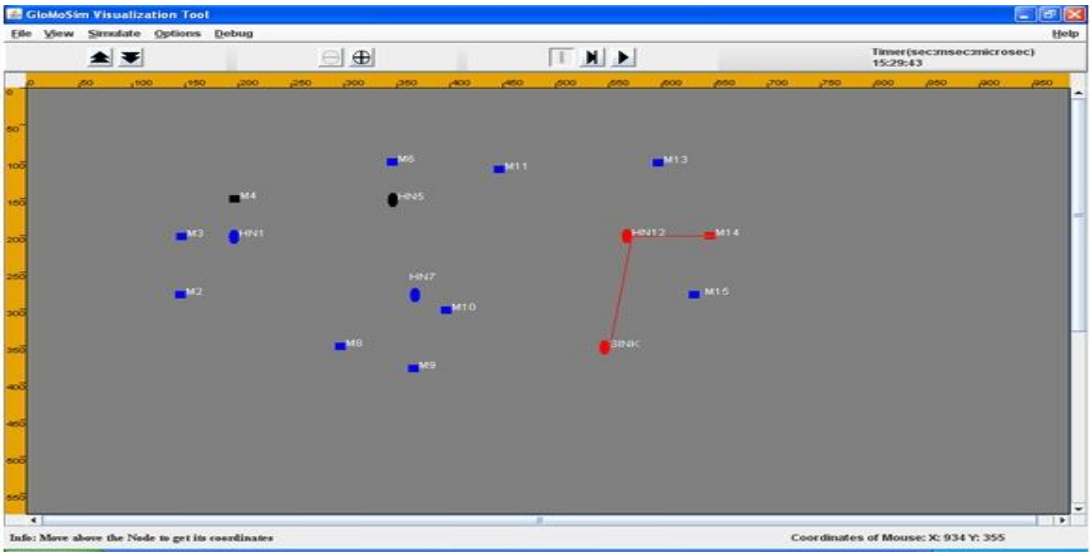


*Figure 5: Message transfers*

During run time it generates three text file one is pairwise key which is used to identify the keys of each node. Second text file is internal attack which shows the compromised node and the description of that node. Third text file is statistics file which helps to plot the graph.

For a privacy-preserving routing technique, its energy consumption is measured by the additional communication used for hiding the traffic carrying real data. Based on the transmission, the energy consumption varies for each node. From the statistics file node 13 has the energy consumption as 62.75and which is plotted in the graph likewise energy consumption values are taken for all the nodes and plotted. The axis profile for energy consumption graph is node Id on X-axis and energy consumption on Y-axis. The graph for node vs. energy consumption is shown in Fig. 6.

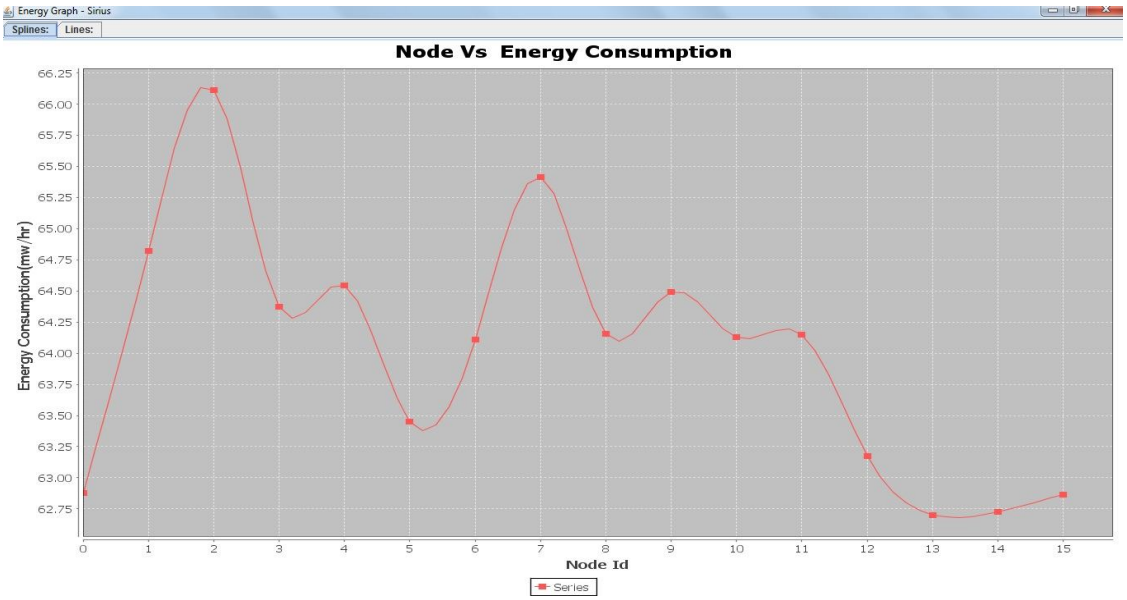


*Figure 6: Node Id vs. Energy Consumption*

 

## VI CONCLUSION

There are a number of directions that worth studying in the future. First, in this paper, eavesdropper may be able to compromise a subset of the sensor nodes in the field. So we demonstrate the solutions to the problem of providing location privacy even though nodes are being compromised. This presents interesting challenges to our methods. Second, it takes time for the observations made by the adversarial network to reach the adversary for analysis and reaction. Studying the impact of such "delayed" analysis and reaction will be another interesting research direction. Future research on the topic includes how to reduce the energy cost while guaranteeing the source and sink's location privacy. This paper aims to maintain source and sink privacy under eavesdropping and node compromise attacks. The majority of the above mentioned efforts attempt to solve privacy issues in heterogeneous WSNs where all sensor nodes have different Capabilities in the future work.

### REFERENCES

[1] L.Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf.Computer and Comm. Security (CCS '02), Nov. 2002.

[2] A. A. Nezhad, A. Miri, and D. Makrakis. Location privacy and anonymity preserving routing for wireless sensor networks. *Computer Networks*, 52(18):3433 – 3452, 2008.

[3] Md. Asri Ngadi, Syaril Nizam Omar and Junaid Chaudhry," A review on wireless sensor networks routing protocol: Challenge in energy perspective".

[4] Lokesh Bajaj, Mineo Takai, Rajat Ahuja, Ken Tang,Rajive Bagrodia, Mario Gerla GloMoSim: A Scalable Network Simulation "

[5] D Liu and P. Ning, " Establishing Pairwise Keys in Distributed Sensor Networks," Proc. ACM Conf.Computer andComm. Security (CCS '03), Oct. 2003.

[6] K. Mehta, D. Liu, and M. Wright. Location privacy in sensor networks against a global eavesdropper. In *Proceedings of the IEEE International Conference on Network Protocols (ICNP 2007)*, Oct. 2007.

[7] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk,"Enhancing source location privacy in sensor network routing," in Proc. Of IEEE ICDCS, Columbus, Ohio, USA, Jun 2005.

 