Implementation of Mobile Attack Detection in Wireless Sensor Network

Anjali Waghade

Department of Electronics Engg.

KDKCE, Nagpur

tejas0315@gmail.com

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 source and sink node in sensor network.**

I. INTRODUCTION

Nowadays the popularity and deployment of pervasive computing technologies are growing vastly. Due to this, privacy of individuals is slowly steaming away. People get easily convinced 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

A wireless sensor network (WSN) is a heterogeneous network composed of a large number of tiny low-cost devices, denoted as nodes, 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. 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, ranging from military applications (e.g., perimeter monitoring 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.

B. Clone Attack

A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate in order to achieve a common goal. Due to their operating nature, WSNs are often unattended, hence prone to several kinds of novel attacks. An adversary may replicate captured sensors and deploy them in the network to launch a variety of insider attacks. This attack process is known as Clone Attack. A particularly dangerous attack is the replica node attack, in which the adversary takes the secret keying materials from a compromised node, generates a large number of attacker-controlled replicas that share the compromised node's keying materials and ID, and then spreads these replicas throughout the network. One of the first solutions for the detection of node replication attacks relies on a centralized base-station. In this solution, each node sends a list of its neighbors and their claimed locations (i.e., the geographic coordinates of each node) to a Base Station (BS).

II. LITERATURE REVIEW

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 .Through Lightfoot et al proposed technique as the Sink Toroida region (STAR) routing technique, the source node randomly selects intermediate node within the designed star area located around the SINK node [2]. 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.

Main limitation of this technique is message delivery ratio is slightly lower than the other schemes. Limited energy lifetime of battery powered sensors-nodes, these methods have to be energy efficient. STAR routing scheme can achieve excellent performance in energy consumption and delivery latency.

Bamba et al described the Privacy Grid framework [3] 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.

III. SYSTEM ARCHITECTURE

A. *Creation of Network:-* The first stage is to create more than 10 wireless sensor nodes in a wireless sensor network . Each node having

a capacity of sending a packet and receiving the same.

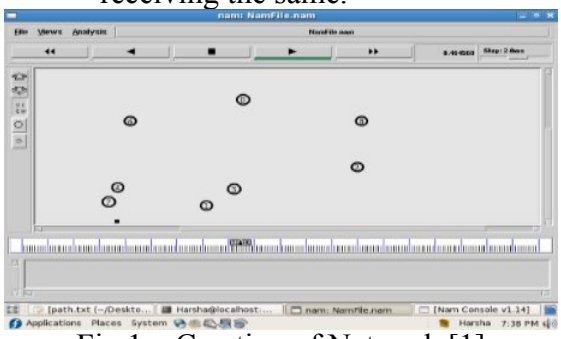

Fig 1. . Creation of Network [1]

B. *Imposing a GI in Network:-* Now as per the global inspector algorithm, we'll select one node as a global inspector 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.

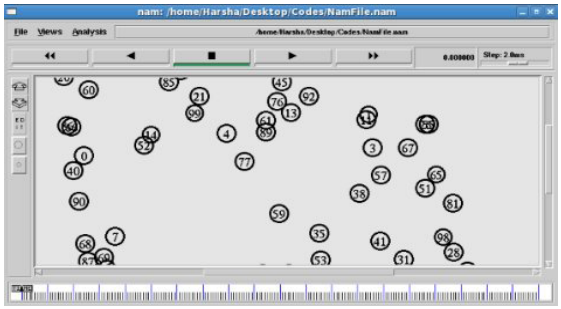

Fig 2. Selection of Node 0 as GI [1]

C. *Pass packet from trusted node:-* Packets need to travel from source to global inspector and from global inspector to destination node. If the flow of packet sending is as above then only destination node will come to know that the data is from party not from adversary (intruder).

Fig 3. Results shows packets send from Global inspector [1]

D. *Packets receive from untrusted source:-* If any packet receive from untrusted party (i.e. not from GI) global eavesdropper (secret listener to private conversations). When packet receives from untrusted node i.e. global eavesdropper that packet is dropped in a network.

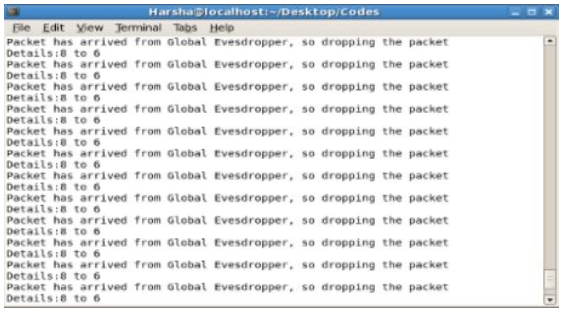

Fig 4. Results shows packets send from GE [1]

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

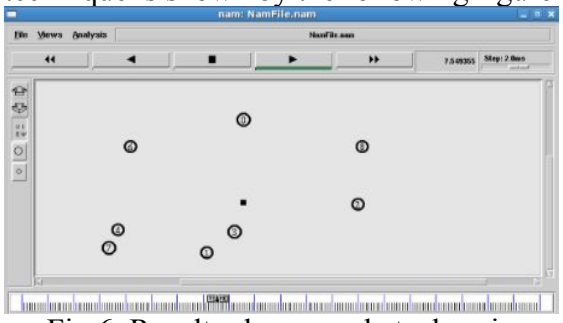

Fig.6. Results shows packets drop in network [1]

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.

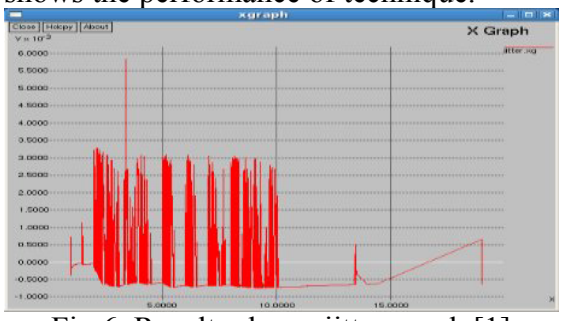

Fig 6. Results shows jitter graph [1]

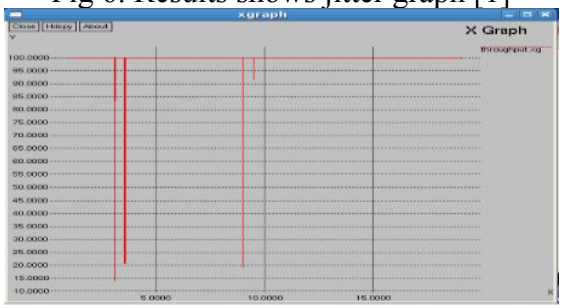

Fig 7. Results shows throughput graph [1]

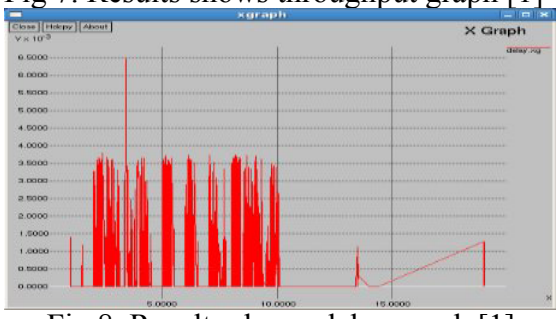

Fig 8. Results shows delay graph [1]

IV. Design and Implementation

Providing location privacy in wireless sensor network using global inspector i.e. GI is implemented in NS-2 environment installed on Fedora Operating System in VMware Workstation and is divided into various modules as follows:

Creation of wireless Environment and performing ping procedure module to perform verification of nodes. Selection of global inspector in a network to define trusted node. Verification of packets either is that from trusted source or not. If packet is from trusted source then process that packet. Received packets are not from trusted source then drop packet instead of processing.

Let's understand this in detail: In the design, we'll create one of the movable node as a global inspector. Each packet passes through global inspector. Let's suppose node 1 is global inspector. let node 2 is sender node and node 3 is receiver node . Then data goes from node 2 to node 1 and then delivered to node 3.

If any node wants to send data, then it has to pass through node1 i.e. global inspector. In each communication node1 would be there. In case there is no Node 1, then the data would be dropped. Thus disallowing any eavesdropper in the network.

V. Applications

1) Ranging from military applications (e.g., perimeter monitoring 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).[2]
2) These advanced sensor network architectures could also be used for a variety of applications including intruder detection, border monitoring, and military patrols. In potentially hostile environments, the security of unattended mobile nodes is extremely critical.[2]
3) The attacker may be able to capture and compromise mobile nodes, and then use them to inject fake data, disrupt network operations, and eavesdrop on network communications.

VI. Advantages

1) Highly Secure MANETs (mobile ad hoc network) : Our system is advantageous it secures MANET from various attacks in MANET like session hijacking, flooding,

interference, traffic jamming, eavesdropping and makes it highly secure .

2) VANETs with high security: These applications imply different security and privacy requirements with respect to the protection goals integrity, confidentiality and availability. Nevertheless, there is a common need for a security infrastructure establishing mutual trust and enabling cryptography. Simply using digital signatures and a public key infrastructure (PKI) to protect message integrity is insufficient taking into account multilateral security and performance requirements.
3) Secure WSN : It also advantageous in keeping WSN secure from attacks, malicious node detection, access control, authentication, cryptographic protocols, key management, and secure routing.
4) We are not implementing Source and Sink location privacy separately, thus our algorithm is more robust. This is the main advantage of our project.

VII. 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 techniques to provide the location privacy to object and sink against a global eavesdropper. We conclude that through analysis and simulation, we demonstrate that the proposed technique are more efficient and effective for source and sink node in sensor network. We've performed traffic analysis to reduce the time and communication overhead based on throughput, jitter and delay. We also conclude that the global inspector algorithm to preserve the privacy of packets is more efficient than other algorithms. 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. [4]

References

1) Harsha C. Kunwar and Ranjana S. Shende . "Proposed a Global Inspector in Wireless Communication to Solve the Problem of Global Eavesdropper". Department of Computer science and Engg, G.H.R.I.E.T For Women's, Nagpur, India.
2) Leron Lightfoot, Yun Li, JianRen, "Preserving Source-Location Privacy in Wireless Sensor Network using STaR Routing" 2010 IEEE .K. Elissa, "Title of paper if known,"unpublished.
3) Bhuvan Bamba, Ling Liu, Peter Pesti, Ting Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacy Grid" 2008 IEEE.
4) C.E. Perkins, E.M. Belding-Royer, and S.R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," IETF Internet Draft, Feb.2003.
5) J. Ho, M. Wright, and S.K. Das, "Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis," Proc. IEEE INFOCOM, pp. 1773-1781, Apr. 2009.
6) A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," Proc. Seventh IEEE Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 245-256, Apr. 2008.
7) Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless

Mesh Networking". O'Reilly Wireless Dev Center. Retrieved 2009-01-20.