ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

# A Framework for Secure Mechanism to Detecting Localizing Multiple Spoofing Attacks in Wireless Sensor Network

R.Poornima[1], C.Premanand[2]

Assistant Professor, Department of CSE, K.S.Rangasamy College of Technology, Tiruchengode, Tamilnadu, India[1]

M.E, Department of CSE, K.S.Rangasamy College of Technology, Tiruchengode, Tamilnadu, India[2]

**ABSTRACT -** Wireless sensor networking is an evolving technology, which supports for many application for common and also military applications. Node compromise is the very important and exclusive security problem in sensor networking. This compromise node which leads to decreased the performance of the whole network. Mainly there are three stages are involving in node compromise attack. Past few years' node compromise work is tackled second or in third stage. In which addressing the node compromise problem is about first stage and analyzed the performance detection method done by various routing protocols. After that sensor nodes are deployed physically and couple of node is built in ad-hoc patter. Both the node are will monitor periodically send/receive by beacon signal. Couple node will check the received beacon signal and its information. If the information is same it believe that the partner node is not compromised and if it is not same partner is compromised. Likewise building couple of nodes among the neighbor node in local area, physical node can be easily compromised and attack can be detected at higherrate.

**KEYWORDS** – Wireless sensor, Network, compromise, nodes.

## I. INTRODUCTION

Sensors are embedded into various machines and environment which also providing the effective delivery of sensing information which provides unbelievable benefits to society. Possible benefits include: few disaster failure, conserving natural resources, improving the productivity, enhanced emergency response and security [2]. Using sensors in various structures and machines remain a problem. Maintenance and installation of large bundles of wire is pretty hard also it may leads to breakage and connection failures could happen. But the wireless sensing networks can eliminate the costs and maintenance also installation. A good wireless senor is network and scalable which consumes very little energy, programmed software, fast data gathering, performance and accurate over a long period, easier cost to purchase and install, requires no real maintenance.

Modern advancement has resulted in able to combine sensors, radio communications and digital electronics into single Integrated circuit package (IC). These types of networks at low cost sensor are easily communicable with other sensor with low power routing protocol. A wireless sensor network mainly consisting of a gateway that can communicate through radio links. Wireless sensor node collects data which is compressed and transmitted through gateway or else forward thorough other wireless sensor node gateway. Finally transmitted data will presented to the system by gateway.

### 1.2 Sensor Node Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Wireless Sensor Network (WSN) contains hundreds or thousands of these sensor nodes. Those sensor nodes are communicating each other directly to an External base station (BS). A large number sensor which allows for sensing over vast geographical regions with high accuracy. Every sensor node contains transmission, processing, mobilizing, GPS and power units. A sensor node works among them and gives high original information about sensor field. Base station is fixed or mobilized the node will connect the sensor node to the existing communication infrastructure or by internet where it requires.

## II. DETECTION OF COMPROMISED NODE ATTACK

Wireless sensor networks (WSNs) have following special characteristics.

1. Every Sensor nodes have their energy level, computational speed and power, memory, external capacity, and communication capability.
2. Every Sensor nodes are tightly coupled with their environments.
3. every sensor nodes easy to get after the deployment and much easier to attack physically.

### 2.1 Stages in Node Compromise Attack

The node capture attack is regarded one of most serious security loopholes for WSNs [12]. The low cost requirement has made hardware measures to prevent tampering literally impossible. A node capture attack consists of three stages:

1. Physically capture and compromise the sensors
2. Redeploy the compromised nodes and/or cloned node
3. Launch insider attacks after redeployed nodes rejoin the network.

### 2.2 Physically Capturing the Node

Physically node capturing is one of common attack in wireless sensor network. Enemies can get full access about a sensor directly by knowing physical location. Enemies extracting the cryptographic functions and attain unlimited access of information on the nodes memory this will leads to severe damage to the system. Using reverse engineering by probing method but it requires chip level component access of the device. Due to their physical restriction node capturing is done have to prevent it.

There are three facts which is supports enemies during node capturing to compromising the whole sensor network communication.

- Larger threat in node capture attacks while sensor node sharing their keys to neighbor node for encrypting and decrypting information. How much level of key sharing leads to same level of threat attacks.
- Structure of the wireless sensor network is also one of the impact for capturing the node and attacking. Links between the source and destination also designing the topology is important tp prevent from attackers.

- More number of sensor network which gives high influence over the node capturing and also happened in node structure.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

### 2.3 Effects of Node Capture Attack

Adversaries can physically compromise few sensor node and make them to lunch false data attacks that makes not existing event in the network. Thus the false report leads to drain the energy resources of the wireless network being delivering through base station over multiple hop. Mainly false alarms wasted the real world response effort. Importantly minimizing the energy draining and preventing false alarms and report should be identified and discarded.

### 2.4 Need for First Stage Detection

Song et al planned to deal the attacks at the second step [10]. Using that approach detecting the redeployment and not capturing. Design is based on assuming the difference between location of original node and redeployment node. Also argued GPS device is not sufficient for human attacker. It only helps to monitor and if the sensor node is very low loaded, data transmission is disconnected.

To make the approach work redeployed node has to repeat the booting-up process and it broadcasting message at various power levels. The attacker definitely let the redeployed node to do that "I am compromised node".

To make the approach more efficiently every node in sensor network repeat the probe message periodically. If the power is in multiple range is used, this type of procedure will be very costly in terms of time, energy, cost. In between two neighbors node one neighbor node includes accessible with low radio transmission power and another includes higher radio transmission power.

### 2.5 Couple Based Detection of Compromised Nodes

Over the past few years, more work has to be tackled in the node compromise attack [8]–[9]. Though all of them addressing the node compromised problem can be detected in either second stage based redeployment detection or third stage based on node misbehaving detection. Unluckily it easy to visualize the attacker can easily compromise the large number of nodes in small amount of time and explore the weakness of sensor node only while losing the effects. Early detection mechanism of the compromising node attack can be defending against it.

This couple based scheme detects the node compromise attack in the first stage. Specifically, after sensor nodes are deployed in a local area, they first build couples in ad hoc pattern. Then, the nodes within the same couple can monitor each other.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

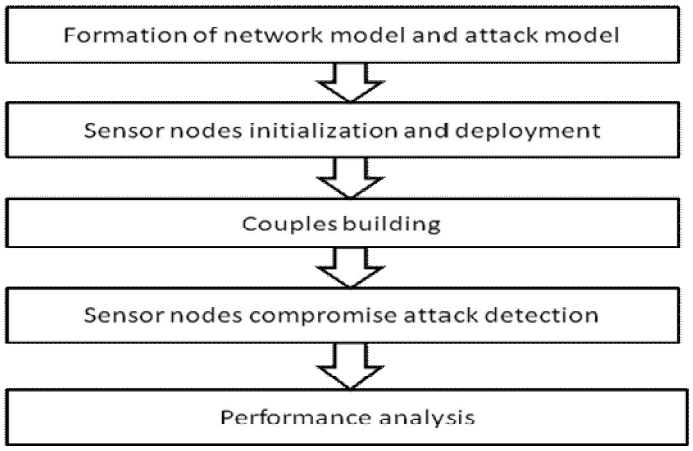


**Fig 2.5 Steps in detection scheme**

### 2.5.1 Network Model

Consider a typical wireless sensor network which is comprised of a sink and large numbers of sensor node N= {N1, N2...} uniformly deployed at a certain interested area, as shown in figure. The sink is a trust and powerful data collection device, which is responsible for collecting the data sensed by sensor nodes. Each sensor node Ni ∈ N has a unique nonzero identifier and is stationary in a location. The communication in the network is bidirectional that is two nodes within the wireless transmission range may communicate with each other. Without loss of detail, it assumes each sensor node periodically collects the sensed data and reports them to the sink via a predefined routing.

### 2.5.2 Attack Model

In these attack model, it assume that an enemies A can capture a small fraction of sensor nodes in a local area, reprogram

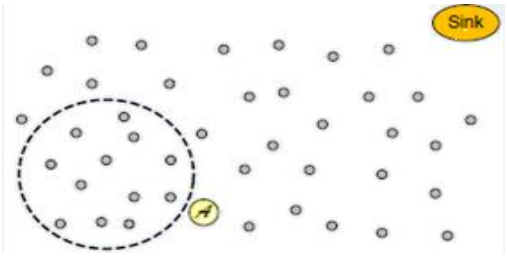


**Fig 2.5.2 Network model**

them with malicious code, and redeploy them back into the network using the physical node compromise attack. The adversary has two physical attack policies: 1) directly physically attack the sensor node at the sensor node's original position; 2) firstly shut down some sensor nodes and launch physical attack at other place. Without loss of generality, assume that there are n sensor nodes in a local area, and the adversary A can only simultaneously compromise k sensor nodes in the local area, where k <n.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

## III. ANT COLONY OPTIMIZATION

In ACO, artificial ants build a solution to a combinatorial optimization problem by traversing a fully connected construction graph, defined as follows. First, each instantiated decision variable $Xi=vji$ is called a solution component and denoted by $cij$ . The set of all possible solution components is denoted by $C$ . Then the construction graph $GC(V,E)$ is defined by associating the components $C$ either with the set of vertices $V$ or with the set of edges $E$.

A pheromone trail value $\tau ij$ is associated with each component $cij$ . Pheromone values allow the probability distribution of different components of the solution to be modelled. Pheromone values are used and updated by the ACO algorithm during the search.

The ants move from vertex to vertex along the edges of the construction graph exploiting information provided by the pheromone values and in this way incrementally building a solution. Additionally, the ants deposit a certain amount of pheromone on the components, that is, either on the vertices or on the edges that they traverse. The amount $\Delta\tau$ of pheromone deposited may depend on the quality of the solution found. Subsequent ants utilize the pheromone information as a guide towards more promising regions of the search space.

The metaheuristic consists of an initialization step and of three algorithmic components whose activation is regulated by the SCHEDULE_ACTIVITIES construct. This construct is repeated until a termination criterion is met. Typical criteria are a maximum number of iterations or a maximum CPU time.

The SCHEDULE_ACTIVITIES construct does not specify how the three algorithmic components are scheduled and synchronized. In most applications of ACO to NP-hard problems however, the three algorithmic components undergo a loop that consists in (i) the construction of solutions by all ants, (ii) the (optional) improvement of these solution via the use of a local search algorithm, and (iii) the update of the pheromones. These three components are now explained in more details

### 3.1 Sensor Nodes Initialization and Deployment

The sink first chooses a proper elliptic curve $E$ built in Tiny ECC and a base point $G$ of order $r$ in $E$. Then, the sink initializes sensor nodes $N = \{N0,N1,N2, \cdot \cdot \cdot ,Nm\}$ by invoking the Algorithm . Finally, the *sink* will deploy these initialized sensor nodes in a geographical area in various ways such as by air or by land. Given the rich literature in wireless sensor nodes deployment, we here do not address the deployment in detail. Without loss of detail, it assumes that all sensor nodes mostly uniformly distributed in an interested area after deployment. Finally, every sensor node $Ni$ will have multiple immediate neighbors and the neighbors can communicate with each other.

### 3.2 Couples Building

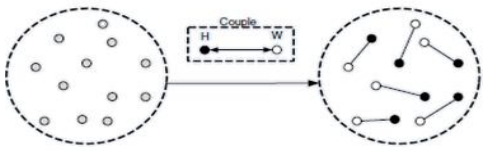


**Fig 3.2 Building couples (H-W nodes) in wireless sensor networks**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

In order to equipped for detecting the possible node compromise attack in a particular area, all the sensor node will build couples in adhoc manner in few minutes after the deployment. For example there are number n of nodes in a local area, any two neighboring sensor node forms a couple, one is husand node (H- node) and another is wife node (W- node).

## IV. CONCLUSION

Security is critical for many sensor networks. Due to the limited possibilities of sensor nodes, provides security and privacy to a sensor network is a challenging task. In this project, couple-based detection scheme to early detect the node compromise attack in the first stage is discussed. Early detection of node compromise attack can lead to a more effective defense against the node compromise attack. By simply building couples among neighboring sensor nodes in a local area, physical node compromise attack can be detected immediately. Simulation is done using the NS-2 simulator in Linux platform. I have finished the literature survey. The first module of this detection technique that is Sensor Nodes Initialization and Deployment has been completed. Work is going on. As our future work, the performance of this detection scheme will be analyzed under different routing protocols.

## REFERENCES

[1] CAT: Building couples to early Detect Node Compromise Attack in Wireless Sensor Networks, Xiaodong Lin, IEEE communication Society 2009.

[2] Lewis, F.L., "Wireless Sensor Networks," Smart Environments: Technologies, Protocols, and Applications, ed. D.J. Cook and S.K. Das, John Wiley, New York, 2004.

[3]A. Tiwari, A., Lewis, F.L., Shuzhi S-G.; "Design & Implementation of Wireless Sensor Network for Machine Condition Based Maintenance," Int'l Conf. Control, Automation, Robotics, & Vision (ICARV), Kunming, China, 6–9 Dec. 2004.

[4]Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.

[5] Wang, B-T. and Schulzrinne, H., "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.

[6] Pfleeger, C. P. and Pfleeger, S. L., "Security in Computing", 3rd edition, Prentice Hall 2003.

[7] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).

[8] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[9] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

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

[11] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.

[12]Adrian Perrig, John Stankovic, and David Wagner, Security in Wireless Sensor Networks, Communications of the ACM, Volume 47, Issue 6, Pages: 53 - 57, June 2000.

[13] Hui Song, Liang Xie, Sencun Zhu, and Guohong Cao, Sensor Node Compromise Detection: The Location Perspective, IWCMC 2007, August, 2007, Honolulu, Hawaii, USA.