Online Grievance Management System at Institute level

Dr.S.Vimala[1], Varanasi Prudhvi Viswanath[2], Syed Mehafeez Ahammad[3], E.S.Vijay[4]

[1] Associate Professor & Prathyusha Engineering College, Tamilnadu, India
[2]Student ,Student &[4]Student
[1]Electronics and Communication Engineering
[1]Prathyusha Engineering College, Chennai, India

***Abstract* -** Wireless spoofing attacks are easy to launch, it plays a significant role in the performance of wireless sensor networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. The challenging tasks in Wireless Sensor Network are identification of spoofing attackers, determination of number of attackers, localization of multiple adversaries and eliminating them. The enhanced clustering approach is used to detect the spoofing attackers and localize them. This approach fails to predict the attackers accurately. To overcome this problem, Enhanced Intrusion Detection System (EIDS) to detect the spoofing attackers. The cluster head act as IDS to monitor the behavior of nodes in their cluster such as packet transmission which helps to identify the misbehaving nodes in wireless sensor network.

***Index Terms* –EIDS, Spoofing attackers, Routing algorithm.**

1.INTRODUCTION

Wireless sensor network is a network of simple sensing devices which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Wireless networks are usually deployed in an unattended manner and are controlled remotely by the network operator. The unattended nature of wireless networks can be exploited by attackers. Specifically, an attacker can capture and compromise wireless nodes and launch a variety of attacks by leveraging compromised nodes. Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. In a large-scale network, multiple adversaries may masquerade as the same identity and collaborate to launch malicious attacks such as Network Resource Utilization attack and Denial-of-Service attack quickly. Among various types of attacks, spoofing attacks are easy to launch that degrades the network performance highly. Spoofing is when an attacker pretends to be someone else in order to gain access to restricted resources or steal information. Therefore, it is important to

i) Detect the presence of spoofing attacks,
ii) Determine the number of attackers, and
iii) Localize multiple adversaries and eliminate them.

2. WORKING ENVIRONMENT

2.1 HARDWARE REQUIREMENTS

Here we do not specifically require any hardware as it is being simulation kind of paper. But using system with 512MB of RAM and at least of 40GB of Hard disk makes smoother operation.

2.2 SOFTWARE REQUIREMENTS

Network Simulator version is used for fast simulation in Linux OS and N map Files are also installed for output display . If the User uses Windows Os then VM Ware helps to install Dual Os with virtual memory allocation for temporary use.

3. PROBLEM DEFINITION

3.1 Problem Definition and Description

Intrusion detection is a set of actions that determine and report unauthorized activities in wireless sensor network. It detects the violation of confidentiality, integrity and availability. In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. The threats that damage the security in WSN can be detected by the Enhanced Intrusion detection and prevention systems (EIDPS). IDPS had an ability to identify the network intrusions and misuse by gathering and analyzing data. The wireless EIDPS can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations in WSN. Thus, it is desirable to monitor the attacks and report the same to a source node to avoid losing an important event. The group of nodes forms a cluster and a cluster head act as an Enhanced Intrusion Detection and Prevention System (EIDPS). The Control Authenticator (CA) distributes the public key and private (secrete) key to each node in the cluster. The EIDPS monitor the activities of all the nodes in the cluster. The source node S starts to send the packets to their destination node D. Based on the public key the EIDPS monitor each and every activity of the nodes in the cluster such as transmission power and energy level. At the time of packet sending, the sender node check the receivers secrete key of the receiver. If there is any change in the transmission power or the secret is not matched then EIDPS consider it as an attacker.

4. SYSTEM ANALYSIS

4.1 EXISTING SYSTEM

Here the existing system being used to detect and localize multiple attackers based on RSS values is presented. The main disadvantage is that it does not prevent that attacks. The existing system, which uses the following key elements:

- **GADE**: Generalized *A*ttack Detection
- **RSS**: Received Signal Strength
- **IDOL**: Integrated Detection and Localization

Framework

A. Working of the existing system:

GADE*:*

In order to detect the spoofing attacks, the GADE (Generalized *A*ttack Detection) method is used. GADE is a method that can both detect a spoofing attack as well as determine the number of attackers present in the network using cluster analysis which is grounded on RSS based spatial correlation.

GADE consists of two phases

a) The attack detection phase: this detects the presence of an attack
b) Number determination: this determines the number of adversaries.
In the attack detection phase GADE makes the use of RSS (Received Signal Strength).

RSS: Is a property closely correlated with the locations in physical space. The RSS reading at different locations in the physical space are distinct. If for each MAC address, the sequence of RSS sample vectors will be close to each other then no attacker is present. Under a spoofing attack, there are more than one nodes at different physical locations claiming the same MAC address. As a result, the RSS sample readings from the attacked MAC address will be mixed with RSS readings from at least one different location. Attack detection using cluster analysis method: Here we will be using the K-means cluster analysis method for identifying the spoofing attack. Using K-means algorithm the nodes in the network are partitioned into the best possible cluster. Under the normal conditions, the distance between the two centroids must be close to each other. However, when there is spoofing attack, the distance between the two centroids is large as the clusters are derived from the different RSS cluster associated with different locations.

4.2 PROPOSED SYSTEM

In the proposed system, the received Signal Strength is analyzed for attack detection and Medoid based Clustering for detecting multiple attackers. Based on the analysis, a threshold value has been setup for detecting attack occurrence. In order to prevent a spoofing attack, a novel scheme Dynamic MAC address assignment has been adopted. Based on this approach, the spoofing attack has been prevented. Moreover, dynamic MAC address has been assigned to the victim node based on the threshold value to prevent the attack.

In addition, the node has been authenticated using passkey. A special DAM (Dynamic Allocation MAC) table has been designed for maintaining both passkey value of node and Dynamic MAC address logger. Each MAC address has been used for one session and periodically updated in the DAM table. Whenever a node requests for authentication through their MAC address, it has been checking and verifying from the register table. If the authentication success then MAC address of node would be changed dynamically with the help of DAM table.

In the proposed system, the same method for detecting the attackers is used.

(1) RSS-a physical property closely correlated with locations in the physical space and
(2) K means algorithm for formation of the clusters.

Further the attackers have been detected using the GADE mechanism. After the attackers have been detected, we will be using the IDOL method for localizing these attackers. The major difference is that we use a dummy node or an intermediate node between the server and the other users. Before the user's request is received by the server it has to pass through this dummy node or the intermediate node.

This intermediate node serves 2 purposes,
a) Ignore the data requests by the attackers
b) Reduce the traffic on the server

5.SYSTEM DESIGN

5.1 FLOW CHART

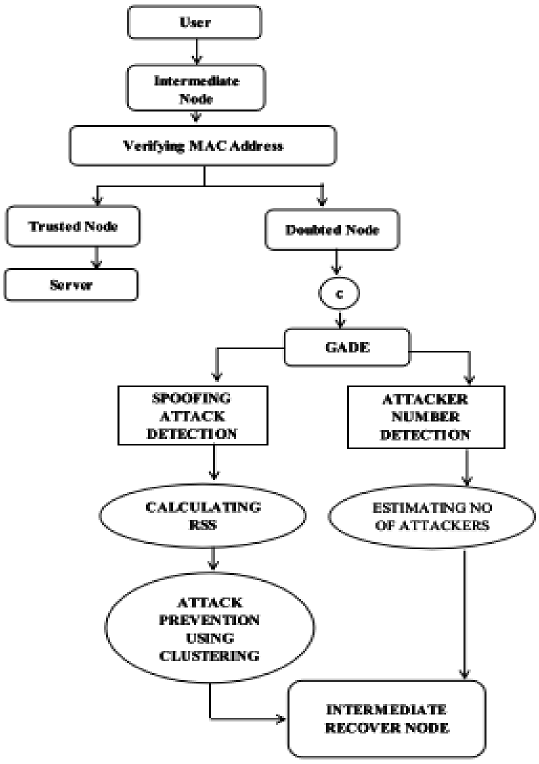

User
Intermediate Node
Verifying MAC Address
Trusted Node
Server
Doubted Node
c
GADE
SPOOFING ATTACK DETECTION
ATTACKER NUMBER DETECTION
CALCULATING RSS
ESTIMATING NO OF ATTACKERS
ATTACK PREVENTION USING CLUSTERING
INTERMEDIATE RECOVER NODE

Figure 1.Flow chart

5.2 ARCHITECTURE DIAGRAM

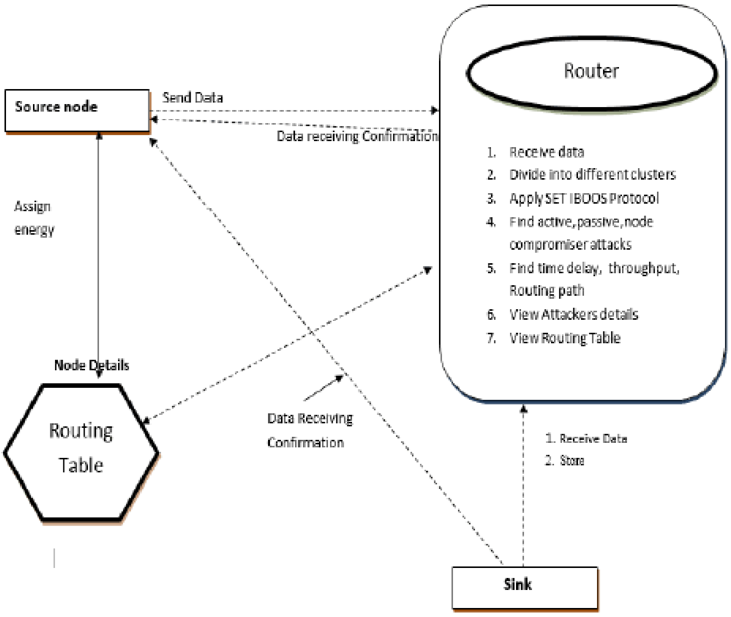

Router
1. Receive data
2. Divide into different clusters
3. Apply SET IBOOS Protocol
4. Find active, passive, node compromiser attacks
5. Find time delay, throughput, Routing path
6. View Attackers details
7. View Routing Table
Source node
Send Data
Data receiving Confirmation
Assign energy
Node Details
Routing Table
Data Receiving Confirmation
1. Receive Data
2. Store
Sink

Figure 2. Architecture diagram

5.3 MODULES

- Module 1: Traffic Reducing System
- Module 2: Testing attack detection and its localization by K-MEANS APPROACH USING RECEIVED SIGNAL STRENGTH.
- Module 3: Preventing Spoofing Attack**MODULE 1**

There would be multiple data requests from the trusted as well as the attacker nodes to the Server. Hence there would be huge traffic which would slow down the performance as the server would have to process all the requests from all the users.

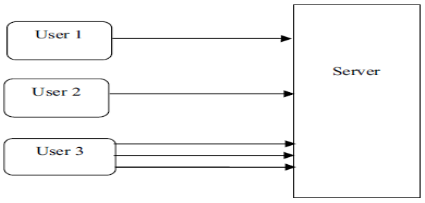


Figure 3.Traffic reducing system

As seen from figure 3, in the present system the server is receiving request from User 1 and User 2 but receiving multiple requests from User 3 as well which creates traffic. In order to reduce the traffic as well as avoid the attack which uses an intermediate node. As seen in Figure 3, the intermediate node would lie between the server and the users and would act as a proxy i.e. the users will assume that they are sending requests directly to the server but in reality, the request is being sent to the intermediate node.

MODULE 2

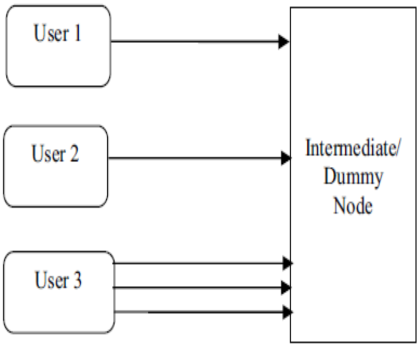


Figure 4. Testing attack detection

The intermediate node would determine the number of data requests from various nodes and then send them accordingly to the server so that the server could respond them immediately.

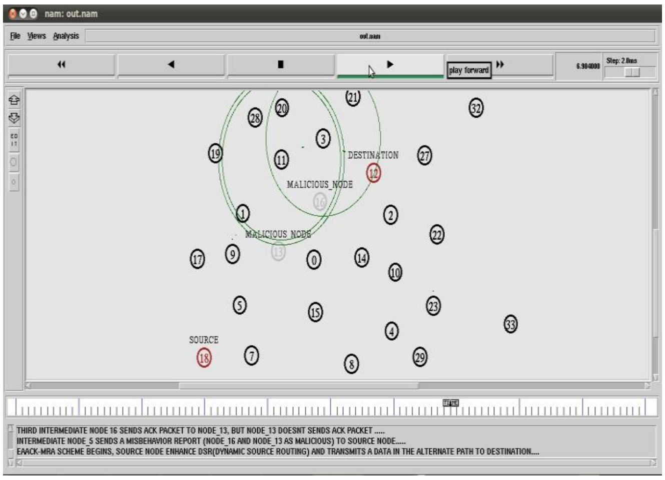
MODULE 3

Consider that there is a MAC spoofing attack. In order to prevent it we have to first detect it; which is done by using GADE and RSS whereas IDOL is used for localizing it. As seen in figure, our proposed method for preventing describes that once the attack is detected, the intermediate node may accept the data requests from the attacker, but not forwards it further to the server, thus suppressing the attacker to have data access from the server along with making the server independent from serving such requests.
Intrusion detection is a set of actions that determine and report unauthorized activities in wireless sensor network. It detects the violation of confidentiality, integrity and availability. In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. The threats that damage the security in WSN can be detected by the Intrusion detection and prevention systems (IDPSs). IDPS had an ability to identify the network intrusions and misuse by gathering and analyzing data. The wireless IDPS can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations in WSN. Thus, it is desirable to monitor the attacks and report the same to a source node to avoid losing an important event. Fig, shows that the group of nodes forms a cluster and a cluster head act as an Intrusion Detection and Prevention System (IDPS). The Control Authenticator (CA) distributes the public key and private (secrete) key to each node in the cluster. The IDPS monitor the activities of all the nodes in the cluster. The source node S starts to send the packets to their destination node D. Based on the public key the IDPS monitor each and every activity of the nodes in the cluster such as transmission power and energy level. At the time of packet sending the sender node check the receivers secrete key of the receiver. If there is any change in the transmission power or the secret is not matched then IDPS consider it as an attacker.

SIMULATION PARAMETERS

Parameter	**Value**
Simulation area	800m x 800m
Number of nodes	10
MAC protocol	802.11
Traffic	CBR
Mobility of nodes	Random way point
Placement of nodes	Random
Routing protocol	AODV
Simulation time	500s

OUTPUT



THIRD INTERMEDIATE NODE 16 SENDS ACK PACKET TO NODE_13, BUT NODE_13 DOESNT SENDS ACK PACKET .....
INTERMEDIATE NODE_5 SENDS A MISBEHAVIOR REPORT (NODE_16 AND NODE_13 AS MALICIOUS) TO SOURCE NODE.....
EAACK-MRA SCHEME BEGINS, SOURCE NODE ENHANCE DSR(DYNAMIC SOURCE ROUTING) AND TRANSMITS A DATA IN THE ALTERNATE PATH TO DESTINATION....

Figure 5. Output

Figure 5, shows the choosing alternate path with no intruder in path for safer. By using AODV which makes safer and energy conserves takes place by this routing algorithm.

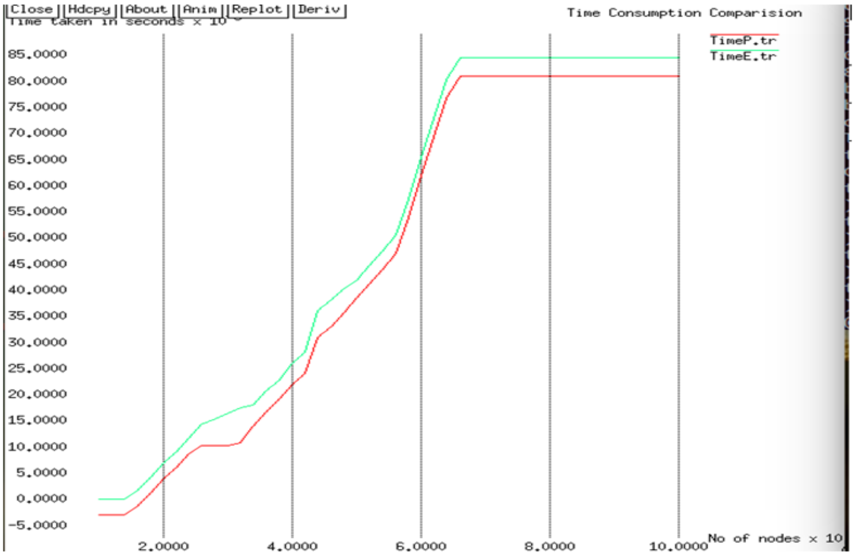


Figure 6. Number of nodes Vs timetaken

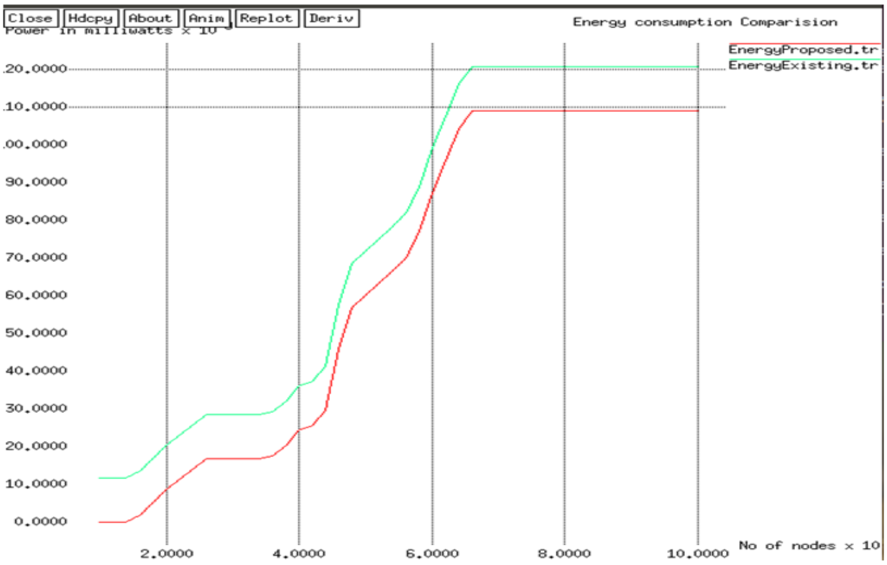


Figure 7. Number of nodes Vs power

6. CONCLUSION

Wireless sensor networks are a highly effective and widely used means of communication. At its present state however, it is vulnerable to a lot of malicious attacks. The system needs to be made more robust in order to prevent loss of data and maintain optimal network performance. The proposed approach tries to introduce the concept of an Intrusion Detection System that can facilitate this task without adding any additional costs or requiring any type of modification to the existing wireless network. The results obtained are highly encouraging and can be easily visualized using tools such as Network Simulator. The future also holds various challenges with adversaries launching new types of attacks in order to gain illegitimate advantage. It is imperative then to be able to introduce other such concepts like the one based on RSS here, whose data is hard to falsify and cannot be easily manipulated by these attackers.

7. REFERENCES

[1] Jie Yang, Yingying (Jennifer) Chen, Senior Member, IEEE, Wade Trappe and Jerry Cheng. (2013). Detection and Localization of Multiple Spoofing Attackers in Wireless Networks. *IEEE*. 24 (1), p44-58.

[2] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.

[3] A. Wool, "Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation," ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.

[4] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.

[5] L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 4646- 4651,June 2007.

[6] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," Proc. 14th ACM Int'l Conf. Mobile Computing and Networking, pp. 116-127, 2008.

[7] F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," Proc. Eighth International Conf. Recent Advances in Intrusion Detection, pp. 309-329, 2006.

[7] L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 21372145, 2008.

[8] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," Proc. IEEE INFOCOM, Apr. 2008.

[9] D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signal prints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[10] E. Elnahrawy, X. Li, and R.P. Martin, "The Limits of Localization Using Signal Strength: A Comparative Study," Proc. IEEE Int' Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.

[11] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF Based User Location and Tracking System," Proc.IEEE,INFOCOM,2000.