International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Detection and Localization of Spoofing Attackers in Wireless Sensor Network using IDS and Rerouting

Balasubramanian.C.V[1], Karnaprabu.B[2], Naawiin.D[3], Naveenkumar.V[4], Umanesan.R[5]

[1,2,3,4]UG Students, Department of Information Technology
Valliammai Engineering College, Kattankulathur, Kancheepuram, Tamil Nadu, India-603203
[5]Assistant Professor, Department of Information Technology
Valliammai Engineering College, Kattankulathur, Kancheepuram, Tamil Nadu, India-603203

Abstract – *The wireless spoofing attack is an attack carried out to either eavesdrop on the network or to crash the network by Denial of Service attacks (DoS). This has always remained a privacy and security issue to network users. There are many algorithms to detect and prevent this kind of attack but none them prevents before an attack occurs. These attacks may cause some serious damage to the user. Usually, these attacks are used in areas like bank fraud, theft of confidential military data, identity theft etc. A wireless spoofing attack is carried out by attackers by masquerading as an intermediate node in a wireless sensor network. This may result in attacker eaves-dropping the communication channel. In the existing technique these attacks are countered with the help of dynamically changing the Media Access Control (MAC) address of the data packet being sent. But this has disadvantages like loss of data until the MAC address of the packet is changed and also the energy loss is high in this method. The proposed system suggests an Intrusion Detection System based technique to solve this wireless spoofing attacks, by detection and localization of these an attacked node.*

Key Words: **IDS, MAC address, wireless spoofing attacks, AOMDV routing algorithm.**

1. INTRODUCTION

The wireless spoofing attacks involves masquerading an intermediate node in a network and eaves dropping on the data being transferred. These attacks can be efficiently solved by using IDS technology and, Ad hoc On-demand Multipath Distance Vector routing algorithm. Here, the IDS localizes an attacked node and the AOMDV algorithm gives an alternate path that does not comprises of attacked node.

2. OBJECTIVES

- Using an IDS based communication to detect attacked node.
- Using AOMDV to transfer the data packet in an alternative route.
- Reduce the overhead created through the existing technique.
- In general, nodes in wireless sensor networks (WSNs) can detect a target and send data packets.
- WSNs are significant in national security, monitoring, military, healthcare, environment, and other applications.

3. RELATED WORKS:

[1] "SPOOFING ATTACK DETECTION AND LOCALIZATION IN WIRELESS SENSOR NETWORK, IJCSET, P.KIRUTHIKA Research scholar Department of Computer Science K.S.Rangaswamy College of Arts and college, 2014"

Spoofing attack is an identity based attack through which a malicious user can spoof the MAC address of a node to create multiple illegitimate identities that highly affect the performance of wireless sensor network. The identification of spoofing and localization of the same is a challenging task in wireless sensor network. This paper presents expository survey of various spoofing attack detection techniques in wireless sensor network.

[2] "DETECTING AND LOCALISING WIRELESS SPOOFING ATTACKS, Yingying Chen et al, 2007"

Proposed two approaches, K-means cluster analysis and Area-based or Point-based algorithms for dealing with wireless spoofing attack. The K-means is integrated as attack detector into a real-time indoor localization system for localizing the positions of the attackers using either area based or point based localization algorithms . The results showed that it is possible to detect wireless spoofing in both a high detection rate and a low false positive rate.

[3] "Controlling IP Spoofing Through Inter-Domain Packet Filters, Zhenhai Duan, Member, IEEE, Xin Yuan, Member, IEEE, and Jaideep Chandrashekar, Member, IEEE, 2008"

The distributed denial-of-service (DDoS) attack is a serious threat to the legitimate use of the Internet. Prevention mechanisms are thwarted by the ability of attackers to forge or spoof the source addresses in IP packets. By employing IP spoofing, attackers can evade detection and put a substantial burden on the destination network for policing attack

packets. In this paper, we propose an interdomain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. A key feature of our scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in border gateway protocol (BGP) route updates and are deployed in network border routers.

4. PROPOSED SYSTEM

Attackers who have different locations then the legitimate wireless nodes are concerned, spatial information is used not only to identify the presence of spoofing attacks but also to localize adversaries. Among various types of attacks, spoofing attacks are easy to launch that degrades the network performance highly. Clustering fails to predict the attackers accurately. To overcome this problem, this paper proposes Intrusion Detection System (IDS) to detect the spoofing attackers. The nodes information in the cluster is collected by cluster head which acts as Intrusion Detection System (IDS) for monitoring the cluster member. If the IDS find the attacker, it passes the alarm message to the source node which eliminates the attacker. The K-Means clustering approach and Intrusion Detection System mechanism are implemented to determine the number of spoofing attacks and localize the same in wireless sensor network.

5. ARCHITECTURE DIAGRAM

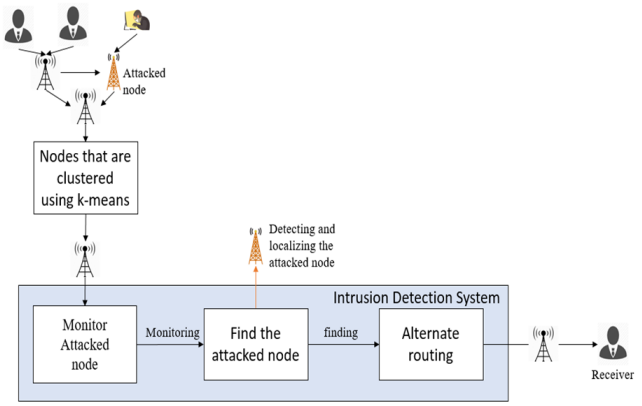

Figure 1

5.1 ARCHITECTURE DESCRIPTION:

Initially the sender will request the transfer of data , But there will be a number of senders in a network requiring to send their data. Here, a spoofing attacker will be disguised as one of the nodes in the sender's path to the receiver. In the diagram, we have highlighted the attacked node in the architecture fig no:1.

Then, the routing algorithm AOMDV in our case will propose a route. Before, the routing begins K-means clustering algorithm will be implemented to cluster the nodes for effective localization of the attacked node. The, the AOMDV routing algorithm will identify the route to destination. The important advantage about AOMDV algorithm is that it will create multiple paths to destination. But, won't have paths with identical nodes.

Then, the IDS will come into play. It will check the name profile of all the nodes in the network. If there is any anomaly, then it will be reported to the source node. That node will be isolated, In the fig no:1 we have highlighted the isolated attacked node.

Then the source node will use an alternate route provided by the AMODV routing algorithm.

6. MODULE DESCRIPTION

6.1 INTERMEDIATE NODES

This module is for the base station. It is built using TCL (Tool Command Language). The working of this module is to receive data packets sent across the network and transfer them to next intermediate node in the packet's way to its destination. Here, as the node receives a packet it will verify its MAC address to check if it is sent from a trusted node. If so, it will transfer the packet to the next node in the network. Otherwise it will cancel that packet.

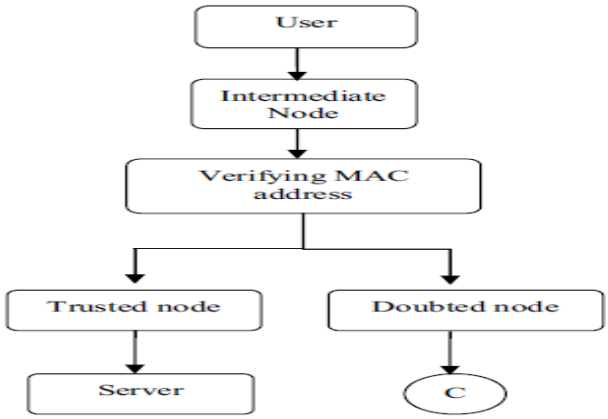

Figure 2

6.2 ROUTE DISCOVERY MECHANISM

A route request message(rreq) will be broadcasted to all neighbor nodes. On receiving the broadcast message nodes will again broadcast routing request (rreq) message to all neighboring nodes, this time along with routing information and so on When the destination node is reached then the final routing information will be reverse broadcasted to the source node. Now with this routing information data transfer will begin

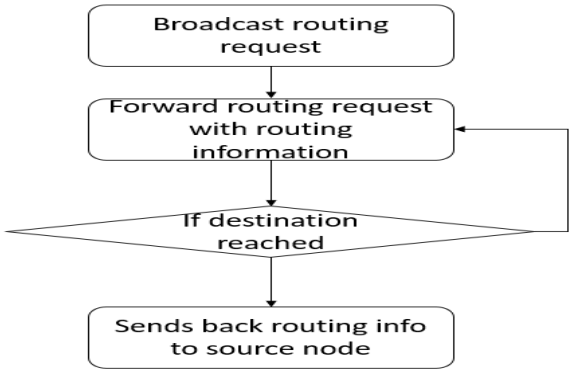

Figure 3

6.3 DETECTION OF ATTACKED NODE BY INTRUSION DETECTION SYSTEM

IDS analyses the transmission power and energy levels of nodes in the network. If it finds any anomaly in transmission power of a node, then an attack has occurred. Then, the IDS will alert all the nodes in the network and the source node. And eventually drop the packet that is being transferred.

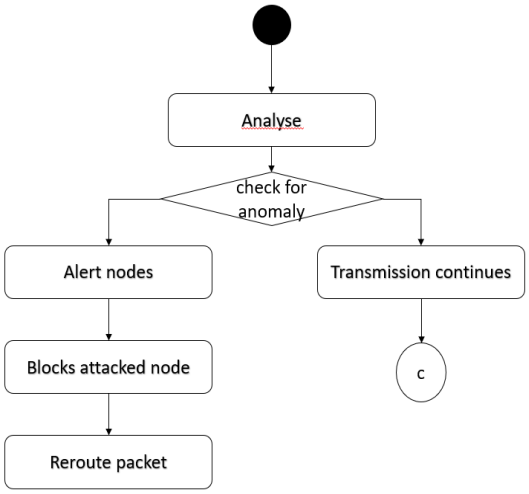

Figure 4

7. METHODOLOGIES

7.1. AOMDV ALGORITHM

The AOMDV algorithm is the routing algorithm used in our system. There are two specialties when it comes to our AOMDV.

They are,

- It will create multiple paths to the destination

- It will only create disjoint paths to destination

So, whenever there is an attack found. The data can be sent through the alternate route available. And also we can be sure that the alternate route that we get will not pass through the attacked node.

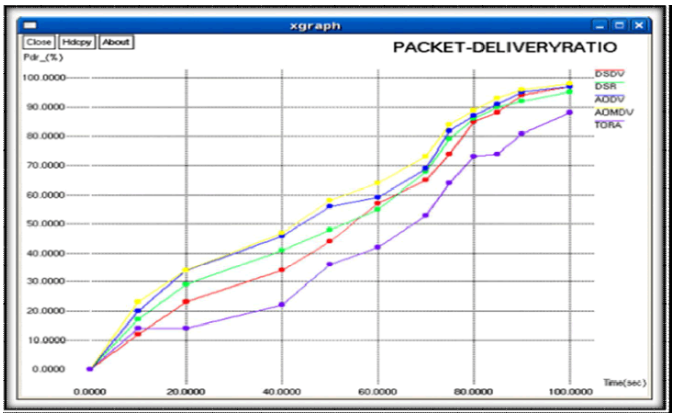

Figure 5

From the "figure 5" we can see that AOMDV algorithm has the highest energy efficiency compared all the other routing algorithms available.

7.2. INTRUSION DETECTION SYSTEM

The intrusion detection system will maintain a cluster head, which will monitor the nodes in the network by creating a network profile for each node. The network profile will contain information such as energy level and transmission power of the nodes.

These values will be compared to the threshold values. if these values for a node is greater than the threshold value. Then it will be detected an attack has occurred. In that case the source node will be alerted. If the threshold value is less than or equal to the threshold value, then it is assumed that particular node is not attacked.

7.3. K-MEANS CLUSTERING

The K-means clustering mechanism is a commonly known clustering technique, where a node in the network will be taken as a centroid and all the nodes that are within a particular range will be clustered with that centroid being at the centre of that particular cluster.

Likewise, a number of centroids will be considered based on the size of the network. And a number of clusters will be created.

These clusters can be used for localization of the attacked node in a wireless sensor network

8. OUTPUT

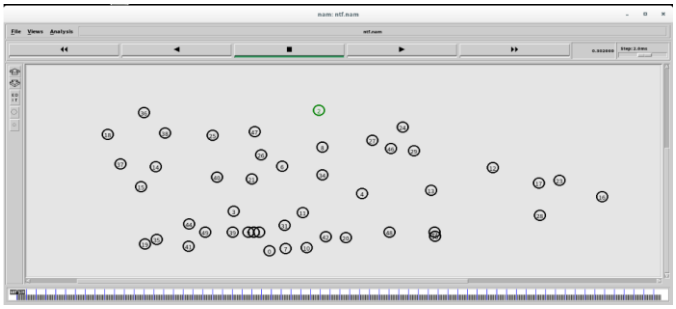

Figure 6.1 These are the intermediate nodes

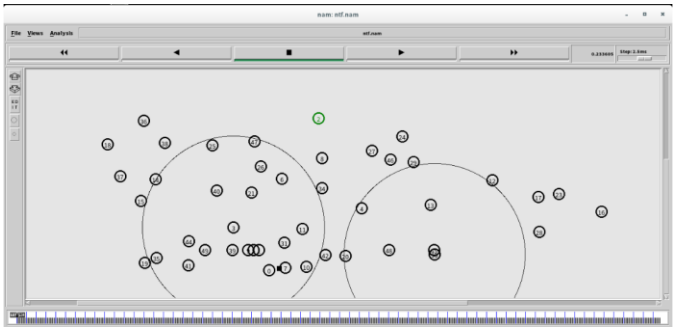

Figure 6.2 It shows the clustering using K-means

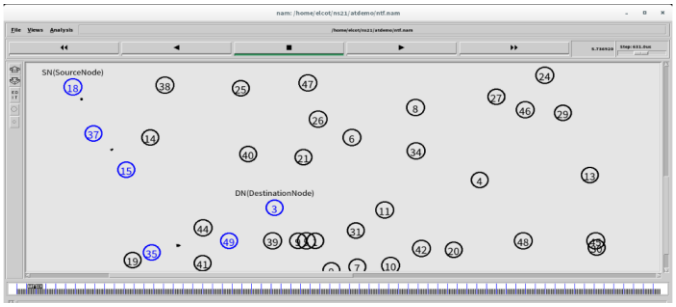

Figure 6.3 It shows the routing of data using AOMDV algorithm

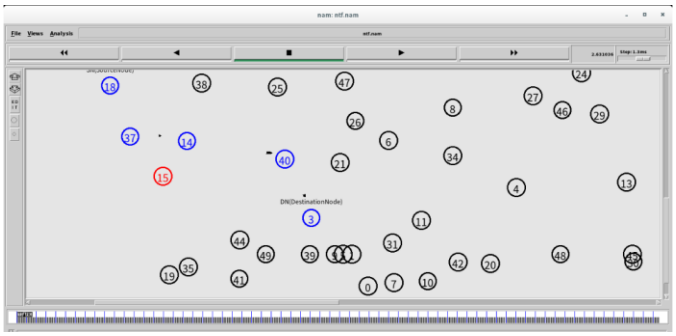

Figure 6.4 It shows the data being transferred in alternate path after detection of spoofing attackers

9. CONCLUSIONS

The sender will send the packets in a network but after receiving those packets, the true receiver will reply to the sender and the communication will continue. But when the packets are received by the attackers, its route will be diverted towards the Dummy node thus stopping their communication with the sender as the dummy node will receive the requests from attackers but will discard it i.e. receive the requests but not processing it further and thus preventing the data from being stolen.

10. REFERENCES

[1] P.KIRUTHIKA Research scholar Department of Computer Science K.S.Rangaswamy College of Arts and college "SPOOFING ATTACK DETECTION AND LOCALIZATION IN WIRELESS SENSOR NETWORK ",IJCSET,2014.

[2] Yingying Chen et al "DETECTING AND LOCALISING WIRELESS SPOOFING ATTACKS", IEEE, 2007.

[3] Zhenhai Duan, Member, IEEE, Xin Yuan, Member, IEEE, and Jaideep Chandrashekar, Member, IEEE "Controlling IP Spoofing Through Inter-Domain Packet Filters", IEEE, 2008.