ISSN:0975-9646

Prevention of Spoofing Attacks in Wireless Sensor Networks

B.Dineshbabu , T.Thirunavukarasu

Information Technology, SNS college of Technology, Coimbatore

***Abstract*— The Wireless Sensor Networks are vulnerable to spoofing and spoofing related attacks. Even though various methods have been imposed for detecting and locating the attackers but it does not focuses to prevent the node from the attackers. In this we propose to show how the spoofing and spoofing related attacks like the flooding attack ad the man in the middle occur, where the flooding attacks send empty packets to disrupt the data send from the node and the man in the middle attack by redirect the packets to the different path. by using the neighbor node signature verification method by sending the keys to the nodes by the key provider by which we can prevent the node from being attacked. The shortest path from the source node to destination node was selected by using the AODV,. prevention mechanism will be very helpful for the quick identification of the attackers and also improve the network performance.**

***Keywords*— Neighbor node signature verification, AODV, Flooding attack, Man-In-The-Middle Attack**

I. INTRODUCTION

The Wireless sensor networks have been recently focused due to various areas are available for the development of application and due to the challenges in its design. The wireless network nodes can be attacked with the help of using the low cost sensor devices in which the spoofing attacks can be launched easily and make damage in the network and affect the performance of the network. The assumption on detecting the spoof node should be powerful for that some security measures are essentially needed to prevent these attacks, but the detection and locating the attackers are largely focussed on preventing the attacks. the detection mechanism is used once the node is being attacked with the help of using the RSS and the cluster analysis method to find out the number of attackers and the Integrated and Detection and Localisation(IDOL) method to find out the location of the attackers and it requires lot of mechanisms to these process. In these methods we are going to solve the spoofing and spoofing related attacks such as the flooding attack and the independent node attack where the only the spoofing attack was detected in the previous approaches. The advantages in the current approach is that it can prevent the attacks and hence it reduce the additional cost and modification done by the wireless devices. The Main contribution of our work is that by showing the spoofing and the spoofing related attacks like the flooding attack.

These flooding attacks which will try to stop the correct users from accessing the network resources then the independent user will does not respond properly and it will redirect the data to another side. By distance vector algorithm to find out the shortest distance and then by using the neighbour node signature verification method the attack can be prevented.

II. ROUTE SELECTION

In wireless sensor networks when two disjoint nodes communicate with each other then the communication distance is limited. hence each node in the network have to play as the host as well as the router. each node have to fix a path before send the message. AODV is the routing technique which pass the messages to the neighbours to nodes with which they cannot directly communicate. AODV is doing this by identifying the routes through which the message is passed. AODV can be able to handle changes in routes and it will create the new routes if there is an error. The most efficient protocols in obtaining the shortest path and lower power consumption. It is mainly used in the Ad-hoc networks and wireless networks. The concept used in this protocol is route discovery and maintenance. It will find the routes only if there is a need. It uses the sequence number to find out the accuracy of information. It will track the next hop in the route instead of the tracking the entire route. It will send the periodic hello messages to the neighbours to update its position of the node. To control the routing process it does not require any central administrative system. It uses the routing table to store the routing information where routing tables for the unicast routes and the routing tables for the multicast routes. There are various mechanisms are used to find out the route selection like the On-Demand Distance vector, DSR have been imposed in which the AODV is imposed through which the path can be selected efficiently to transfer the data.

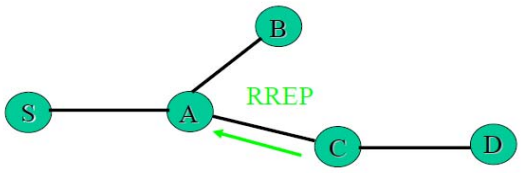

Fig 1.1 Sending the Route Request

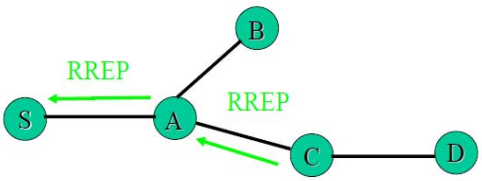

Fig 1.2 Forward Path Setup

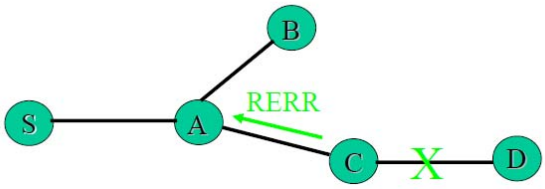

Fig 1.3 Route Maintainance

The routing table stores the destination addres, next hop address, Destination Sequence number, Life_Time. The Life time updated every time the route is used, if the route is not used within its life time then the route expires. If there is an increase in the sequence number it indicates that there is change in topology. The AODV contains mainly two process such as route discovery and route maintenance. When the node wishes to send packets to send some destination, It checks its routing table to determine if it has a current route to the destination. If Yes, forwards the packet to next hop node, If No, it initiates a route discovery process. Route discovery process begins with the creation of a Route Request (RREQ) packet that RREQ was created by the source node. Once an intermediate node receives a RREQ, the node sets up a reverse route entry for the source node in its route table . if a node S wants to send the data to node D it sends the route request to its neighbour nodes the route C receives the route request and C creates the route reply to the node A. A sends the route reply to node S and the node S receives the route reply and makes the forward route entry to route D that is it sends the packet to the destination D. It helps in reducing the cost of increased latency in finding new routes.

III. DDOS FLOODING ATTACK

DDoS Flooding attacks are the biggest problems in area of security. These flooding attacks make the explicit attempts to disturb the correct users to access the services. These attacks gain control over the nodes in the network by exploiting their vulnerabilities. Some mechanism is usually requires the comprehensive understanding of the problem and the techniques to prevent the attacks.

There are two methods to make the DDoS attack in the network

First method is that the attacker will send some empty or unrelated packets to the node to confuse the protocol running on it. It is also called as the vulnerability attack.

The second type of attack is the most common one where the attacker do that one or they will do both by the following ways

- By exhausting the bandwidth and router processor capability we can disrupt the correct users.
- By exhausting the server resources like sockets, cpu, memory, database will disrupt the correct users and then it mainly include application level flooding attacks. The DDoS flooding attacks had launched in many organisations. There are about 7000 DDoS attacks have been observed daily.

IV. MAN-IN-THE-MIDDLE ATTACK

Phishing is the process of attempting the sensitive information like the password and the user name by masquerading as the trusted user to attain benefit financially. Man-In-The-Middle Attack is one of the most famous for Phishing. The Man-In-The-Middle(MITM) attacks are the most famous and the basic attacks on Distributed Computing Technologies. The Man-In-The Middle attack is an attack in which the intruder can read and write messages when two parties communicate with each other. The attack appears in many forms and shapes due to the evolution in computing. For example in the http transaction the TCP connection between the client and server is the target. By using the different techniques the attacker break the original TCP connections into two new connections. The first one is between the client and the attacker and the second one is between the attacker and the server. By intercepting the TCP connection, the attacker will act as a proxy and it can be able to read, write, modify the data in the intercepted communication. This attack is very effective due to nature of the http protocol and data transfer which are all ASCII based. By this it is possible to view and interview within the http protocol and also in the data transferred.

MITM is not only an attacking technique and also used up in the during the development setup for web application and it still used for web vulnerability assessments.

V. SIGNATURE VERIFICATION

Neighbour node signature verification is the process which is done to prevent the attacksrather than detecting the attacks. By doing so the spoofing and the spoofing related attacks like the flooding attack and the man in the middle attack are greatly reduced .At first the node have to be deployed and then after the setting up the path where the data have to be transferred. The key provider will provide the keys to the nodes which was selected. The node will make the request to the neighbour node where the data have to be transferred by asking them the key and the node will be immediately respond and then send the keys to the node which ask the request and then node which sends the requests will verify the keys if it verified then it will send the file or the data to the node. In digital signature the node A will encrypt the message by using the private key of A and it distributes the public key of A to other users and they will decrypt the data with the public key of A.

When there is a known path and if there is no such spoofing attack the data transfer will be effective but in case of multiple data requests to node to get access to the resources then there will be a confusion to the node which sends the data, to which node it have to send because many nodes are claimed to be the same node. Then the sender who sends the data will sends a requests to all the nodes who claimed to be the same node to send the signature where only the original node have it. The nodes sends the key, the sender checks the keys send by the nodes and it find out the original node and then the spoof node it send the data to the original node and it becomes active and then

the remaining nodes are indicated as the idle node to indicate that they are the attackers. The node which becomes active will start asks the request to the other node like that the process continues until it reaches the destination.

VI. CONCLUSION

The attack prevention mechanism in the spoofing and the spoofing related attacks like the flooding and the man in the middle attack are effective compared to that of the detection mechanism where the attack is detected and then determining the number of attackers and then the location of the attacker is obtained. Using the neighbour node signature verification method the attackers are identified and prevented through which the data is transferred through the correct node. The performance level of this prevention mechanism is better as that of the detection mechanism which is obtained theoretically. It reduce the time, cost and energy consumption, and by only using this prevention method cannot guarantee that it can prevent all the attacks and there may be a chance of some exception that attacker exists, hence we can make this as the future enhancement using the advanced detection mechanism through which some attackers which exists in the prevention mechanism can be detected and prevent the other nodes in the network by giving alert information and prevent them by providing access to the network resources.

REFERENCES

[1] Sharma.p,Trivedi,A “An Approach to Defend Against Warm hole Attack In Ad Hoc Network Using The Digital Signature” Communication Software and Networks(ICCSN) 2011 IEEE 3rd International Conference on may 2011.

[2] Youngsoo Kim, Daejeon, Jungchan Na, Seungwon Sohn “A Secure Method For Transferring Active Packet Using The Digital Signature Schemes” Telecommunications, 2003. ICT 2003. 10th International Conference Vol.01 on 23 Feb 2003 .

[3] Zhijun Li and Guang Gong “On The Node Clone Detection In Wireless Sensor Networks” IEEE/ACM Transactions on networking, Vol.21,No.6,December 2013.

[4] Saman Taghavi Zargar, James Joshi, David Tipper “A Survey of Defence Mechanisms Against Distributed Denial of Service(DDoS) Flooding Attacks” IEEE Communications Surveys & Tutorials Vol.15 Fourth Quarter 2013.

[5] Joshi, Y, Das, D. ; Saha, S.”Mitigating Man in the Middle Attack Over Secure Socket Layer” on Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference on Dec.2009.

[6] Guha, R.K. Furqan, Zeeshan ,Muhammad, Shahabuddin “Discovering Man in The Middle Attacks in Authentication protocols” Military Communications Conference, 2007. MILCOM 2007. IEEE on 31 oct 2007.

[7] Chakeres, I.D. Belding-Royer, E.M. "AODV Routing Protocol Design Implementation” Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on march 2004

[8] Royer, E.M. “An Implementation Study of the AODV Routing Protocol” Wireless Communications and Networking Confernce, 2000. WCNC. 2000 IEEE Vol.3 Sep 2003.

[9] Jensen, M. Gruschka, N. ; Luttenberger, N “The Impact of Flooding Attacks on Network-Based Services” Availability, Reliability and Security, 2008. ARES 08. Third International Conference on March 2008.