Identification Of Packet Droppers And Effective Routing Of Packets In Wireless Sensor Networks

Achuthan Gandhi G, G. Vijayalakshmi

Computer Science and Engineering Department, SRM University, Chennai, Tamilnadu, India,
achuthangandhi@gmail.com

ABSTRACT: In the wireless sensor networks there is the chance for the packets to be dropped due the attacker at the intermediate nodes. The packet droppers are being identified. The packets are routed from source node to the destination by AODV Routing protocol. Some of the intermediate nodes may act as the packet dropper. This is because the third party may change the characteristics of the nodes. The type of attack that we are going to consider here is the worm-hole attack. The droppers are identified by our system. The packets are then routed in the alternative path avoiding those packet droppers.

Keywords: WSN, Packet Droppers, Re-Routing.

1 Introduction

The wireless sensor networks are made of the several nodes. The nodes may have been deployed in different work places. The sensor nodes sense the temperature, light and other information and sends to the different work locations for the various purposes. Sometimes while transmitting those data's there may be the chance for the attack by the third party. One among those attacks is the worm-hole attack. The node may drop the entire packets. No packet will reach the destination. In this system the packers are routed by the means of AODV routing protocol. The two important features of AODV routing protocol is route discovery and route maintenance. AODV routes the packets through the path discovered. The packets have to pass through several intermediate nodes. Some of the intermediate nodes may act as the packet dropper. The system first identifies the packet droppers. Once the packet dropper is identified by our system that route is eliminated and the packets are sent through the other alternate path. Clearly the packets reach the destination. The packet delivery ratio is calculated. PDR value during the attack will be zero and after the overcome the value will definitely be high.

2 Proposed Scheme

A scheme for identification of the packet droppers has been proposed here. In the existing system the packets are being broadcasted to all the nodes. So there occurs the redundancy of data. Further there is the wastage of the energy at the nodes. All this things has to be avoided in our proposed system. In the proposed system the Packets are not broadcasted. The packets are forwarded by means of AODV routing protocol. The two main features of this protocol is route discovery and route maintenance. The packets are transmitted from the source node to the destination node. There are several intermediate nodes between the source node and the destination node. These nodes may sometimes act as a packets dropper. The type of attack we consider is the worm-hole attack. The node completely drops the entire packets that are being sent. This type of attack is being identified by AODV routing protocol. First it first identifies the attacker nodes and then transmits the packets through the alternative path.

3 System Model

This system is designed for the identification of the packet droppers and effective routing of the packets in the wireless sensor networks. The following are the components which are essential for designing the system

3.1 Node Creation

The wireless sensor networks are made up of several nodes. The node may have the sensor. The nodes does the function of gathering the sensory information from the outside environment and also communicate with the other nodes in the environment .There is the transmitter and the receiver with each of the sensory nodes. There is a source node and sink node and several intermediate nodes. The main components of a sensor node are a microcontroller, transceiver, external memory, power source and one or more sensors. The selection of files is being carried out at the source node. The certain nodes are designed with specific characteristics that it drops the packet.

3.2 Packet Forwarding

The packets have to be forwarded from the source node to the destination node. The packets are forwarded from the source node to the destination node with the help of the intermediate nodes. AODV Routing protocol is used in the routing of the packets. The two important features of AODV routing protocol is the route discovery and route maintenance. AODV maintains its own routing table. AODV forwards the packets to the destination node with the help of the routing table. One of the important features of AODV is that it can modify the path automatically when the error in the path is detected.

3.3 Packet Droppers

During the forwarding process some packets may be lost by some of the nodes. Some nodes are designed in such a way to drop the packets. The type of attack we consider here is the worm hole attack. The attacker sometimes may modify the characteristics of some of the nodes in such a way it drop the packets. When a node drop the packet the dropper node can easily be identified during the evaluation of the trace file. The diagrammatic representation of packet dropper node is explained in fig 5.

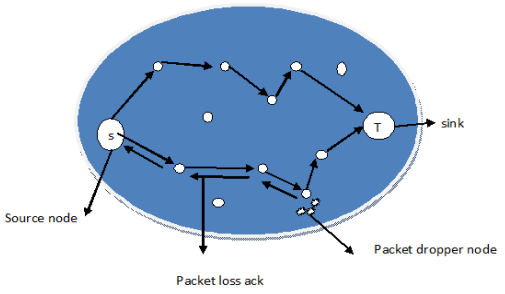

Fig 3.3 System Diagram

3.4 Re-Routing

Once the dropper node is being identified by using AODV routing protocol the packets has to be re-routed via alternative path. AODV protocol at first evaluates the path for the transmission of the packets. If any packet dropper node is found in that path AODV neglects that path and send the packets through the alternative path.

4 ALGORITHM

The protocol being used here is the AODV routing protocol. The algorithm does the three important functions here. First is the identification of the packet droppers. Second is re-routing of the packets through the other alternative path. And the third is the calculation of the packet delivery ratio. The very first step is the identification of the packet droppers. This project is simulated by using Ns2. Some of the nodes are created with certain identification. Consider certain nodes with n-type=1 has to drop the packets. AODV clearly checks the path for the attacker node with n-type=1. If any of the node is found with that specification the node is identified as the packet dropper. AODV neglects the path with the certain type of nodes and carefully sends the packets through the other alternative paths. One of the biggest advantages of the system is that path checking is carried out even before the packets are being transmitted. The final step is the calculation of the packet delivery ratio. Packet delivery ratio at the time of the attack and packet delivery ratio after overcome. The packet delivery ratio at the time of attack will nil since no packets will be delivered to the destination nodes. All the packets are dropped by the attacker. After the overcome method is carried out the delivery ratio will be high up to 95% or even higher. The formula used in the calculation of the PDR ratio PDR value= (recvLine/sendLine).

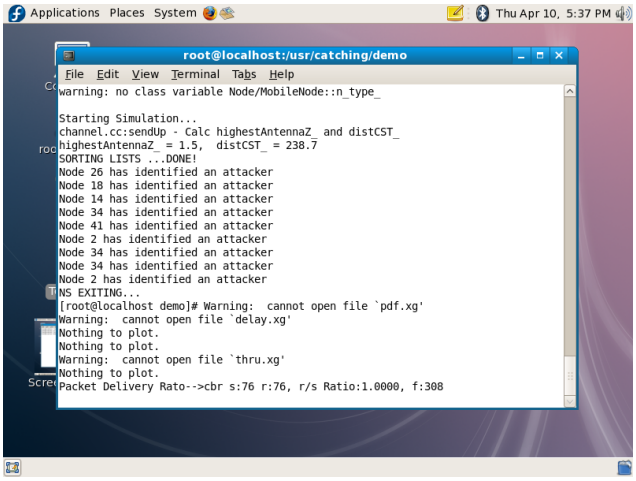

Fig 4.1 PDR value after overcome

5 Results and Analysis

The PDR values before and after overcome is being calculated and marked as a graph

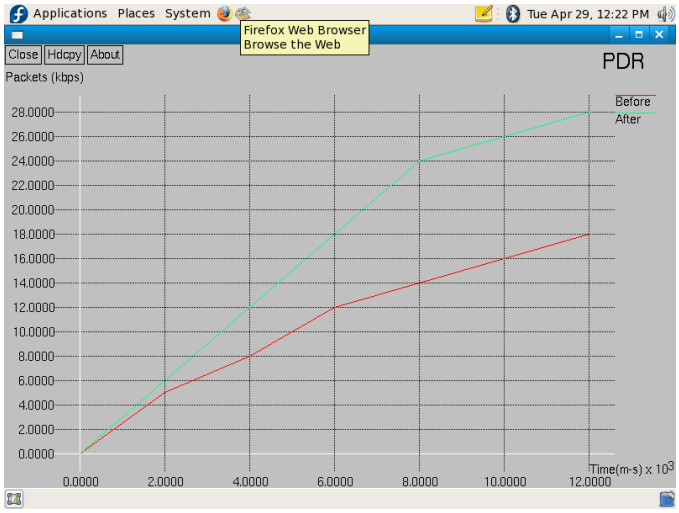

Fig 5.1 PDR Values Before and After Overcome

6 CONCLUSION

Most of the packet dropping node i.e. the attacker nodes can be identified by this system. Once the attacker node is identified in the network the packets are transmitted in the alternative path. This system helps in the reliable delivery of the packets. This system architecture is the less time consuming structure since most of the dropper in this route is identified in the beginning stage itself i.e. before the transmission of the packets. The future development can be done with the removal of attacker node from the network

7 REFERENCES

[1]. I. Khalil and S. Bagchi, "MISPAR: Mitigating Stealthy Packet Dropping in Locally-Monitored Multi-Hop Wireless Ad Hoc Networks," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm '08), 2008.

[2]. Redundancy in Network Traffic: Findings and Implications Ashok Anand1_, Chitra Muthukrishnan_, Aditya Akella_ and Ramachandran Ramjee†_University of Wisconsin-Madison, †Microsoft Research India{ashok,chitra,akella}@cs.wisc.edu, ramjee@microsoft.com

[3]. R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Secmr—A Secure Multipath Routing Protocol for Ad Hoc Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007

[4]. S. Lee and Y. Choi, "A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks," Proc. Fourth ACM Workshop on Security of Ad Hoc and

[5]. V. Bhuse, A. Gupta, and L. Lilien, "DPDSN: Detection of Packet-Dropping Attacks for Wireless Sensor Networks," Proc. Fourth Trusted Internet Workshop, 2005

[6]. Z. Yu and Y. Guan, "A Dynamic En-route Scheme for Filtering False Data in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2006

[7]. Algorithms and Protocols for Wireless Sensor Networks (http://books.google.co.in/books)

[8]. Algorithms for Routing Lookups and Packet Classification (A Dissertation submitted to The Department Of Computer Science and The Committee on graduate studies of Stanford University in partial fulfillment of the requirements for the degree Of Doctor Of Philosophy Pankaj Gupta) December 2000

[9]. Detecting Malicious Packet Dropping in the Presence of Collisions and Channel Errors in Wireless Ad hoc Networks, Thaier Hayajneh, Prashant Krishnamurthy, David(www.sis.pitt.edu/~dtipper/Apaper2009_1.pdf)