Asian Journal of Electrical Sciences (AJES)
Vol.3.No.1 2015 pp 29-32.
available at: www.goniv.com
Paper Received :08-03-2015
Paper Accepted:20-03-2015
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

PREVENTING GRAY HOLE ATTACK USING TRUST BASED MODIFIED AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL

[1]N.RAJENDRAN, [2]M.KARTHIK
Department of Information Technology , B.S Abdur Rahman University,Chennai, India.
[1]*rajendran.n81@gmail.com*, [2]*karthikvsi367@gmail.com*

ABSTRACT

MANETs are autonomous and decentralized networks. So, they can operate no matter which nodes are connected or not connected to the network. Since, MANETs don't have any centralization; operations are done distributed, so each node has to have sufficient information about the network and have to operate independently. MANETs are very vulnerable to various attacks from malicious nodes, some classical malicious attacks (e.g., fractions of modification, DoS attacks, gray-hole and black-hole attacks). In Existing System, a trust prediction model is created to evaluate the trust dependability of nodes; it is based on the nodes past behaviors and fuzzy logic rules prediction method. Trust value is calculated using decision factors such as direct trust and recommendation trust. In the proposed work, we focus on further improvement of routing trust using Modified Ad-hoc On-demand Distance Vector Routing (AODV) protocol and to incorporate other decision factors (Incentive function and Active degree) to improve the trust. By enhancing the trust gray hole attacks will also be eliminated.

Keywords —Gray hole Attack, MANET, Trust

INTRODUCTION

A mobile ad hoc network is a collection of wireless mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. There are some unique characteristics of mobile ad hoc networks .First, the connections between network nodes are wireless, and the communication medium is broadcast. The wireless connection provides the nodes with freedom to move, so the mobile nodes may come together as needed and shape a network, not unavoidably with any assistance from the cable connections .Second, unlike traditional wireless networks, mobile ad hoc networks do not have any fixed infrastructure. It is only a collection of self-organized mobile nodes, which are connected through high-variable quality links. Thus, the network topology is always changing; the execution context is extremely dynamic .The interconnections between mobile ad hoc network nodes are not permanent; they are capable of changing on a continual basis to adapt this dynamically and arbitrarily pattern. Third, the membership is always changing. The mobile nodes are free to move anywhere, leave at any time and new nodes can enter unexpected. There is no mechanism to administrate or manage the membership. Fourth, the execution environment is insecure and unfriendly. Due to the lack of fixed infrastructure and administration, there are increased chances malicious nodes can mount attacks. Also, nodes may behave selfishly and result a degradation of the performance or even disable the functionality. Finally, the nodes in a mobile ad hoc network are usually portable mobile devices with constrained resources, such as power, computation ability and storage capacity. The remains of the paper are organized as follows. Section II discuss about the related work. Section III gives the proposed works of Trust Model. Section IV illustrates the simulation results and analysis using NS2 simulation and result analysis. Section V gives the conclusion and future work.

II.RELATED WORK

A. Gray hole Attack

There are various types of denial-of-service (DoS) attacks. One of them is gray hole attack. Gray hole

attack[5] is an attack in which some selective data packets are dropped by the malicious node. Gray hole attack is harder to find because of some data packets reached the destination and destination thinks that it is getting the complete data. In Gray hole attack [6,7] in routing protocol occur at the time of routing the data packet. In mobile ad hoc network this type of attack easily occurs due to dynamic nature of MANET. One of the major issue about the gray hole attacks is that it misguides the source by advertizing that there is a valid and shortest path to the destination. Thus the malicious node could do harm the network by degrading the network performance, disturbing route discover process etc.

B. AODV Protocol

The AODV[8] Routing protocol is a reactive protocol uses an on-demand approach for identifying routes, a route is establish only when it is required by a source node for transmitting data packets and then employs destination sequence numbers to identifying the shortest path. The major difference between AODV and Dynamic Source Routing (DSR) is that DSR uses source routing in which a data packet carries the complete path to be passed over. The message types defined by the AODV protocol are Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs). However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. In an on-demand routing protocol and then source node overflow the RREQ packet in the network .When a route is not available for the long for destination. It may obtain various routes to dissimilar destinations from a single Route Request. In major difference between AODV and other on-demand routing protocols is that it uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination. In a node updates to its track information only if the DestSeqNum of the current packet received is greater than the last DestSeqNum stored at the node.

III.PROPOSED WORK

A. Direct Trust

In [1] direct trust calculation comes under direct observation of neighbor's one hop to another .In every mobile node in the network monitors the behavior of its neighbor's node, and if any abnormal activity is detected, to evaluate trust value. In this module to monitors the neighbor's nodes by tractable listening to their communication for detecting dropped, delayed, and forwarded packet. In every mobile node in the network monitors the behavior of every other neighbor's node really forwards the packet or drop them by default all the mobile nodes while communicating with other nodes the direct trust value of all the communicating nodes are calculated and stored in the trust table of corresponding node with field name using index of node, direct trust value and one more total trust value of the corresponding mobile node and otherwise by default all the mobile nodes while communicating with other mobile nodes, the direct trust value of all of the communicating nodes are calculated and stored in the trust table of corresponding node with field name using index of node, direct trust value and one more total trust value of the corresponding node. After some time the neighbor's nodes may move out of the range of a particular node due to their mobility and again they come back to the transmission range then again trust value is calculated and the corresponding entry in the table is updated.

$$DT_{xy}= \frac{P_s}{P_R} \qquad (10)$$

Where,

DT_{xy} =the final direct trust value of x and y.
P_s= the successful packet sent from the node x.
P_R = the successful packet receive from the node y.

B. Indirect Trust

In [2, 3] indirect trust monitor is to collect or request the trust related information of target mobile node from the neighboring nodes. The neighbor nodes collecting the trust information while requesting the trust information of the target node from neighbors, the direct trust value of that neighbor node should be considered. This information generally called as Recommendation trust. In the task of recommendation trust agent is to collect or request the trust related information of target node from the neighboring nodes. The source node will broadcast the recommendation request packet to all its neighboring nodes and the reply packets. In [9] fuzzy logic method is applied to the direct trust value of all the replied neighbors. The node with maximum trust value is considered for evaluation of recommendation trust value.

C. Incentive Function

In [4] this function reflects the incentive function for cooperative entities. Because of the cooperative entities often have fewer bad interactions and less interaction failure rates, while malicious nodes or uncooperative entities often refuse to the interrupt service. This function also reflects that the system would make some punishment to the uncooperative entities. This function is denoted by which is calculated with following equation. It is used to indicate that the node does not fulfill its responsibility, and do harm to evaluating a node's trust value.

$$IF_{ij}=1-\Phi(n) \qquad (4)$$

Where

$$\Phi(n) = \Phi^{\frac{N_T - M_T}{N_T}} \qquad (\Phi < 1)$$

N_T=Total Number of Interaction
M_T=Total Number of Malicious Interaction

D. Active Degree

In[4] active degree decision factor that reflects the level of activity of an entity in a network. This is used to represent the credibility of evaluated entity. If an (evaluated) entity has a higher active degree, other (evaluating) entities is willing to interact with it due to its expected higher trust level. An evaluating node V_i records the cumulative number of entities interacting with an evaluated node V_j and calculates the active degree of the evaluated node as follows:

$$AD_{ij} = 1 - \frac{\eta}{L-1} \qquad (L \geq 0) \quad (4)$$

Where
L=Cumulative number of entities interacted with the evaluated node V_j.
η = Black-list trust threshold

IV.SIMULATION AND ANALYSIS

A. Simulation Parameter

For the performance evaluation in the AODV protocol the simulation is performed inNS2. The work is carried 50-100 nodes. During the simulation some parameters are defined which are stated in the using NS-2 Simulator.

B. Simulation Result

The performance of AODV is analyzed. Based on the parameter such Packet delivery ratio, Overhead and Packet loss. X-graphs are plotted for these parameters. Finally, the results obtained from this module X-graphs are plotted. In Fig1, Fig2 and Fig3 represent the variation of increase in the packet delivery ratio, Packet loss and Overhead vs. Number of packet

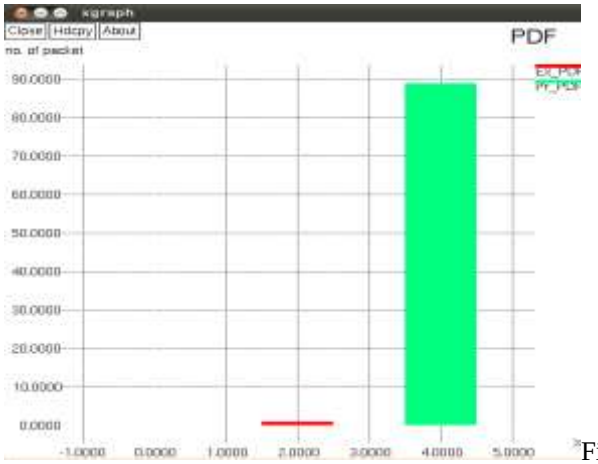

Fig 1 Packet Delivery Ratio vs. Number of packet

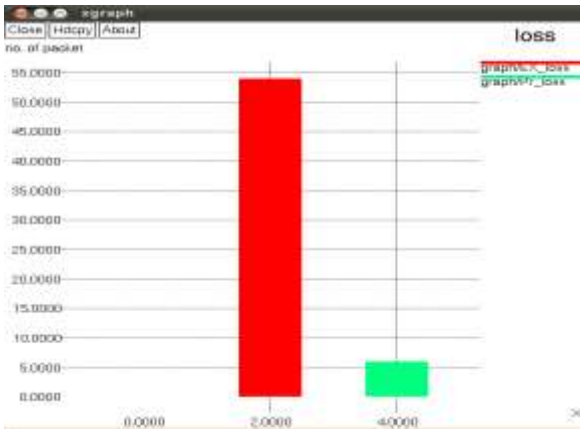

Fig 2 Packet loss vs. Number of packet

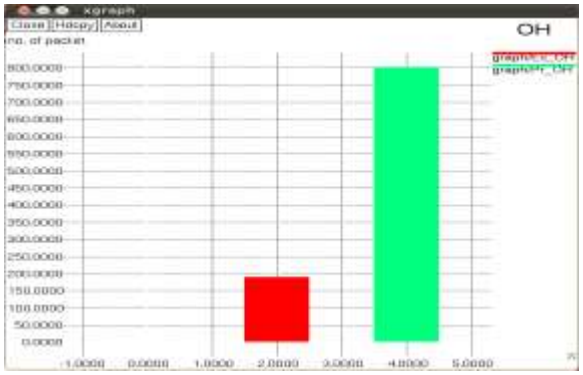

Fig 3 Overhead vs. Number of Packet

V.CONCLUSION AND FUTURE WORK

In this paper, we proposed a Trust model to measure trust level of nodes in MANET. Our aim is to prevent the Gray Hole Attack using Trust Model .In existing to combine the direct trust value and recommendation trust our

proposed work to incorporate the new decision factor of trust model such as Incentive Function and Active degree to evaluate the trust value. In future Work using some other decision factor of Trust model using various protocols.

REFERENCES

[1]Zhexiong wei,Helen Tang,F.Richard Yu,Maoyu Wang, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management using uncertain Reasoning" IEEE Transactions on Vehicular Technology(2014).
[2] Hui Xia, Zhiping Jia, Xin Li, Lei Ju,Edwin H. M. Sha "Trust prediction and trust-based source routing in mobile ad hoc networks", Journal of Ad Hoc Networks 11 (2013) 2096–2114.

[3] Hui Xia, Zhiping Jia, Xin Li, Lei Ju,Edwin H.-M. Sha "Impact of trust model on on-demand multi-path routing in Mobile ad hoc Network" Journal of Computer Communications 36 (2013) 1078–1093
.[4] Hui Xia, Zhiping Jia, Xin Li, Lei Ju,Edwin H.-M. Sha "A Subjective Trust Management Model with Multiple Decision Factors for MANET based on AHP and Fuzzy Logic Rules" 2011 IEEE/ACM International Conference on Green Computing and Communications
[5] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda " Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method" International Journal of Emerging Technology and Advanced Engineering Volume 2, Issue 1, January 2012.
[6] Amanpreet Kaur ,ManjotKaur Sidhu " Mitigation of Black Hole and Grey Hole Attack In Mobile Ad hoc Networks" International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.
[7] Mr.Chetan S.Dhamand , Prof. H.R.Deshmukh "A Efficient Way To Minimize the Impact of Gray Hole Attack in Adhoc Network" International Journal of Emerging Technology and Advanced Engineering Volume 2, Issue 2, February 2012.
[8] Onkar V. Chandure, Prof. V. T. Gaikwad "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV routing protocol in MANET International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011
***[9]** Partha Sarathi Banerjee, J. Paulchoudhury, S. R. Bhadra Chaudhuri " Fuzzy Membership Function in a Trust Based AODV for MANET" I. J. Computer Network and Information Security, 2013, 12, 27-34.*
[10] Ji Guo , Alan Marshall, Bosheng Zhou, "A New Trust Management Framework for Detecting Malicious and Selfish Behaviour for MobileAd hoc Networks", 2011 International Joint Conference of IEEE