SecurityManagement to Eliminate GrayHole Attack using Trust Based Ad-hoc On-demand Multi-path Distance Vector Routing protocol in MANET

D. AmuthaPandiyan
Assistant Professor
Department of CSE
MahaBharathi Engineering College
ChinnaSalem, India
Email: amuthancse@gmail.com

Punitha. R
PG Scholar
Department of CSE
MahaBharathi Engineering College
ChinnaSalem, India
Email: punithabtech@yahoo.com

***Abstract*-MANETs are autonomous and decentralized networks. It has no clear line of defense. It is accessible to both genuine users and malicious attackers. In the network services, confidentiality and integrity of the data is affected due to security issues. MANETs are very vulnerable to various attacks from malicious nodes, some classical malicious attacks (eg.,DoS attacks, warm-hole attack, gray-hole attack and black-hole attack). In this paper, we are calculating the trust value of nodes using decision factors such as direct trust and recommendation trust.We focus on further improvement of routing, trust based Ad-hoc On-demand Multi-path Distance Vector Routing (AOTMDV) protocol is used, which is an extension form of Ad-hoc On-demand Multi-path Distance Vector Routing (AOMDV) protocol. AOTMDV protocol is to incorporate other decision factors (Incentive function and Active degree) to improve the trust. By enhancing the trust, gray hole attacks will be eliminated and the performance of network throughput, packet delivery ratio and malicious attack resistance also improved effectively.**

***Keywords*- Ad-hoc, Gray hole attack, Trust, MANET, Security, AOTMDV routing**

I. INTRODUCTION

A Mobile Ad-hoc NETwork(MANET) is a self-configuring, infrastructure-less network of mobile devices connected without wires.There are some unique characteristics of mobile ad-hoc networks.First,the connection between network nodes are wireless and the communication medium is broadcast. The wireless connection provides the nodes with free to move, so the mobile nodes may come together as needed and shape a network. Second, mobile ad hoc network do not have any fixed infrastructure. Thus, the network topology is always changing, it is extremely dynamic. The intercomnections 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 discuss about the proposed works of Trust model. Section IV illustrates the simulation results and analysis using NS2 simulation and resultanalysis. 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 data packets are dropped by the malicious node. Gray hole attack is difficult 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. One of the major issue about the gray hole attacks is that it misguide the source by advertising 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. AOTMDV Protocol

The Trust based Ad-hoc On-demand Multi path Distance Vector (AOTMDV) [8] Routing protocol is an extension to AOMDV routing protocol for computing multiple loop-free and link disjoint paths using trust values. The routing entries for each destination contain a list of the next-hop counts and path trust. All the next hops have the same sequence number and all the nodes have path trust value. This helps in keeping track of a route. For each destination, a node maintains the advertised hop count and path trust, which is defined as the maximum hop count for all the paths, which is used for sending route advertisements of the destination.Each duplicate route advertisement received by a node defines an alternate path to the destination.Loop freedom is assured for a node by accepting alternate paths to destination if it has a less hop count than the advertised hop count for that destination. Because the maximum hop count is used, the advertised hop count therefore does not change for the same sequence number. When a route advertisement is received for a destination with a greater sequence number, the next-hop list and the advertised hop count are reinitialize.

AOTMDV can be used to find node-disjoint or link-disjoint routes. To find node-disjoint routes, each node does not immediately reject duplicate RREQs. Each RREQs arriving via a different neighbor of the source defines a node-disjoint path. This is because nodes cannot be broadcast duplicate RREQs, so any two RREQs arriving at an intermediate node via different neighbor of the source could not have traversed the same node.In an attempt to get multiple link-disjoint routes, the destination replies to duplicate RREQs, the destination only replies to RREQs arriving via unique neighbors. After the first hop, the RREPs follow the reverse paths, which are node disjoint and thus link-disjoint. The trajectories of each RREP may intersect at an intermediate node, but each takes a different reverse path to the source to ensure link disjoint ness. The advantage of using AOTMDV is that it allows intermediate nodes to reply to RREQs, while still selecting disjoint paths.

Destination
Sequence Number
Advertised Hop count
Expiration Timeout
Route List {(NextHop$_1$, HopCount$_1$), (NextHop$_2$, HopCount$_2$), ….. }

Destination
Sequence Number
Advertised Hop count
Expiration Timeout
Route List {(NextHop$_1$,HopCount$_1$, pathTrust$_1$), (NextHop$_2$,HopCount$_2$, pathTrust$_2$), …… }

(a) AOMDV (b) AOTMDV

Fig 1. Difference between AOMDV and AOTMDV

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 nodes.

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.

P_S

$$DT_{xy} = \frac{P_S}{P_R}$$

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. Recommendation Trust

In [2,3] recommendation 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 punishment to the cooperative entities. This function is denoted by which is calculated with the 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.

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

Where,

$$\Phi(n) = \frac{N_T - M_T}{N_T} \quad (0<\Phi<1)$$

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:

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

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 AOTMDV protocol the simulation is performed in NS2. The work is carried 50-100 nodes. During the simulation some parameters are defined which are stated in the using NS2 simulator.

B. Simulation Result

The performance of AOTMDV 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 fig 2, fig 3 and fig 4 represent the variation of increase in the packet delivery ratio, packet loss and overhead vs. number of packets.

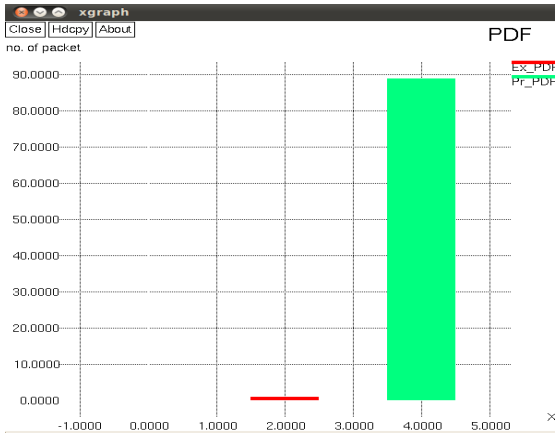

Fig 2. Packet delivery ratio vs. number of packet

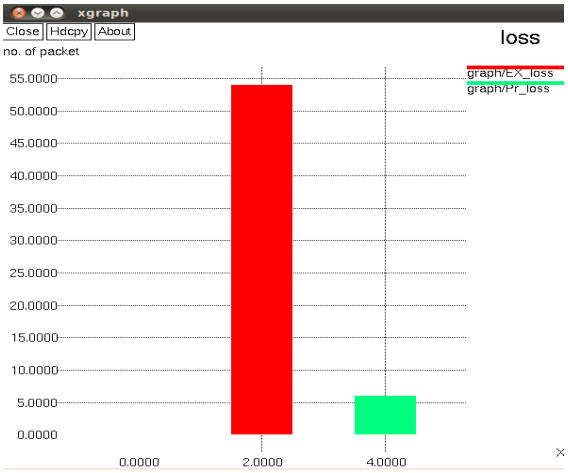

Fig 3. Packet loss vs number of packet

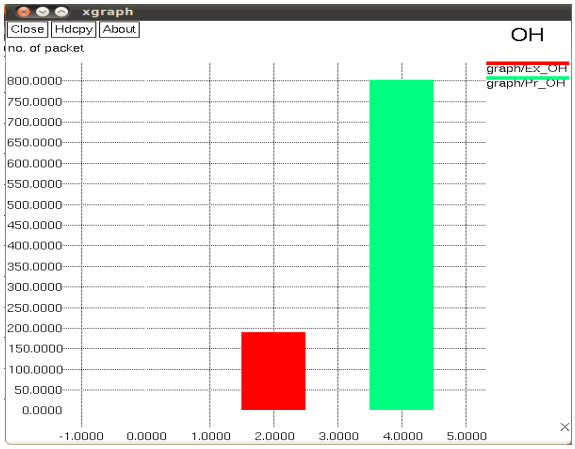

Fig 4. Overhead vs number of packet

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 eliminate gray hole attack using trust model. By combining the direct trust value and recommendation trust value, in our proposed work to incorporate the new decision factors of trust model such as incentive function and active degree to evaluate the accurate trust value. Using the trust values in AOTMDV routing protocol, the secure and shortest path is discovered in one route discovery and gray hole attack is identified and eliminated. In future work using some other decision factors of trust models using various protocols.

REFERENCES

[1] Zhexiongwei, Helen tang, F.richard Yu, Maoyu Wang,"Security enhancements for Mobile Ad hoc Networks with Trust Management using Uncertain Reasoning" IEEE Transactions in Vehicular Technology(2014).

[2] Hui Xia, ZhpingJia, 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, ZhipingJia, 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, ZhipingJia, 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", InternationalJournal of Emerging Technology and Advanced Engineering Volume 2, Issue 1, January 2012.

[6] AmanpreetKaur, ManjotKaurSidhu," Mitigation of Black Hole and Gray 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, " An Efficient Way to Minimize the Impact of Gray Hole Attack in Ad hoc 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] ParthaSarathi Banerjee, J. Paulchoudhury, S. R. BhadraChaudhuri," Fuzzy Membership Function in a Trust based AODV for MANET", International journal of Computer Network and Information Security, 2013, 12, 27-34.

[10] JiGuo, Alan Marshall, Bosheng Zhou, " A New Trust Management Framewwork for Detecting Malicious and Selfish Behaviour for Mobile Ad hoc Networks", 2011 International Joint Conference of IEEE.

AUTHOR'S PROFILE

PUNITHA R was born on Sep 13 1990. She received B.Tech Degree in Information Technology from B.S. AbdurRahman Crescent Engineering College, Chennai in the year 2012. She is pursuing her M.E CSE in Mahabarathi Engineering College, chinnasalem. Her research interests in the areas of wireless networks and computer networks.