Detecting and Dealing with Malicious Nodes Problem in MANET

[1] Anil Kumar Gupta
[1]Amity University,Noida, India
anil24048@gmail.com

[2]Deepti Mehrotra
[2]Amity School of Computer Science, Noida, India
dmehrotra@amity.edu

Abstract--The objective of this research paper is to detect malicious behaviour of nodes so that a route via malicious node is never used to transmit an application packet to its destination. When a malicious node receives an application packet from a node destined for some other node then instead of forwarding that packet, it simply drops that packet. This data loss may become severe when number of malicious nodes present in network is high. In proposed work, we overcome this problem by identifying such malicious behaviour of nodes and then a route via such a node is never chosen by its neighbour to forward an application packet in the network.

Keywords-- AODV, MANET, Malicious Nodes in MANET.

1 INTRODUCTION

Routing is the process of choosing paths through which network traffic flows. Routing is implemented in different sort of networks, for instance telephone network, electronic data networks and internet network. In electronic data networks routing uses packet switching technology. In packet switching networks, routing makes the path for packet forwarding, and also supports for the transportation of addressed packets from source to destination through intermediate nodes by using hardware devices like routers, bridges, gateways, firewalls or switches. Ordinary computers with multiple network cards may forward packets and activate routing, regardless of limited performance. The objectives of this research paper in Computer science and engineering are to

- Acquire deep understanding of AODV routing protocol in MANET
- To detect malicious behaviour of nodes so that a route via malicious node is never used to transmit an application packet to its destination.

2 RELATED WORKS

Internet Engineering Task Force (IETF) introduced MANETs to create such type of network in which there is no central entity. The main purpose of MANETs is to improve IP routing protocol used for both static and dynamic techniques.[1] There are lots of routing protocols which are working under this category, but few of them are listed below.

- AODV (Ad-hoc on-Demand Distance Vector)
- TORA (Temporally Ordered Routing Algorithm)
- DSR (Dynamic source Routing)
- OLSR (Optimized Link State Routing Protocol)
- DSDV(Destination Sequenced Distance Vector Routing

The proactive routing protocols use shortest path algorithms. The proactive protocols include OLSR (Optimized Link State Routing Protocol), DSDV and WRP (wireless Routing Protocol). The main drawback of these routing is that the information used by these routing protocols cannot be used. The other major drawback is the broadcasting of information utilizes bandwidth and energy in terms of control packets. On the other hand the routing which represents on demand policy is referred as reactive routing. In contrast with proactive routing there is no pre computed routing here to the target, but on demand, when necessary.

Dynamic Source Routing Protocol represents source route which is implemented on demand basis. Every node should control its route cache. The node regularly updates the route cache if there is a better route, and then it can adopt new routes. In dynamic source routing process every packet has to know about the route direction, to avoid periodic route findings. DSR has the quality to find out the route and control the path for routing.M8AC layer helps DSR to detect link failures [2].

Basically proactive protocols depend on periodically link state updates and control packets delivery. There is a large traffic which ultimately effects original traffic. Messages are being updated and disseminated by flooding. Optimized Link State Protocol is considered to be proactive protocol [3].

The idea for destination sequenced distance vector routing depends on Bellman-Ford Routing algorithm with some updates to make it efficient for wireless networks. In this scheme every node has to create a consistent path towards routing table to the destination, also maintains hops to reach target and the sequence numbers allocated to destination nodes. The function of sequence numbers is to create the difference between old and new routes [4].

Basically TORA lies in the category of distributed routing protocol. The basic idea used in this algorithm is link reverse process. This routing algorithm is being developed by IETF to control the effects of topological changes. It makes it sure that loop free environment is developed and various routes

should be created for source to the destination. Its specific quality is to develop routing mechanism and rely on Internet MANET Encapsulation Protocol (IMEP) for other different functions. The route mechanism defined by TORA has three preliminary key functions Route detection plus deletion, Route generation and route maintenance [40].

3 AD-HOC ON DEMAND DISTANCE VECTOR

The Ad-hoc on-demand is basically reactive protocol which supports multi routing between nodes which are playing their roles to form an Ad-hoc network. AODV is the improved version of DSDV protocol, but the main difference is that AODV is reactive whereas DSDV is proactive .[5][6] It has great advantages, for instance, for disseminating information through routes on demand basis requirement for maintenance is not necessary. One of the main qualities of AODV is that it is free from hops. The environment where AODV is activated, target sequence numbers confirm the route, to be refreshed properly. The algorithm use d in AODV considers two messages, one is route request, to establish the route request message is being activated by AODV, and the other is hello message. These messages support nodes to strengthen neighbour nodes. Without the presence of hello messages, the identification of nodes is difficult. AODV has the ability to provide lot of information about the following technical aspects [7][10].

- Target IP addresses, where the packets should be sending.
- Sequence numbers.
- Counting of hops, that packet has passed.
- Next hop, stability of routes
- Neighbor nodes activity
- Request, the request should be on at a time.

[1] Process to Find out Route

The node starts to find out the path, the path is necessary for determining and travelling of data. The source finds out the path and sends the message towards the destination. The request message is also activated to find out the appropriate route for sending the message [7].

[2] Route Management Policy

To manage the route, it is necessary to point out the route that lacks its validity, then the removal of route entry exists and link failure message is conveyed. This message is also transferred to nodes which are using the same route which has been suffering from breakage. The neighbour's nodes are properly updated. This process is repeated again and again. The main benefit of AODV is the limitation of routing messages as compared to ordinary protocols. This is all due to the reactive behaviour of AODV [7][8].

4 PROPOSED WORKS

When a malicious node receives an application packet from a node destined for some other node then instead of forwarding that packet, it simply drops that packet. This data loss may become severe when number of malicious nodes present in network is high. In proposed work, we overcome this problem by identifying such malicious behaviour of nodes and then a route via such a node is never chosen by its neighbour to forward an application packet in the network.

4.1 Proposed Algorithm

Algorithm to identify malicious behaviour of a neighbour node-

When a node wants to send an application packet to other node which is not its immediate neighbour then it sends an RREQ packet to all its neighbours. If a neighbour knows route to destination of this packet then it sends an RREP packet that contains the next hop address to which neighbour node will forward the packet. Let us call this next hop address as next to next hop address. The algorithm is described as follow:

i. Sender node forwards application packet to one of its immediate neighbour delegating the responsibility of further forwarding it to that neighbour. Sender also sets a timer (which is twice the network diameter) to receive acknowledgement from destination node.

ii. If acknowledgement is received before timer expires then the route is considered to be trusted and no further action is needed.

iii. If timer expires and acknowledgement is not received then the route is not considered to be trusted. Now sender sends an application packet to next to next hop address node and again sets a timer to receive an acknowledgement.

- If acknowledgement is received before timer expires then the neighbour node is considered to be trusted and no further action is needed, otherwise the neighbour node is considered as half-trusted. In this situation, this half-trusted node will be under observation until it shows same malicious behaviour again when an application packet is forwarded to it next time.

iv. If the half-trusted node does not show malicious behaviour when the application packet is forwarded to it next time then it will be considered as trusted-node, otherwise this half-trusted node will be considered as malicious and following actions will be performed:

- No further RREP messages from this node will be entertained.
- The application packets will not be forwarded to this node.
- New routes will be discovered to forward application packets to those destinations that have this un-trusted (malicious) node as next hop address in route table.

5 EXPERIMENTAL SETUP

In this paper we have discussed the simulation results and the analysis that we have obtained after doing the simulation in OPNET 14.0. We simulated MANET with three different networking scenarios and checked the performance in terms of number of packets dropped. During our simulation we have used Global Statistics by choosing individual DES statistics in a workspace window of OPNET and the results are displayed in the form of graphs, where all the graphs are displayed as sample sum. The FTP was used as traffic in our simulation for all kinds of scenarios in equal amount.

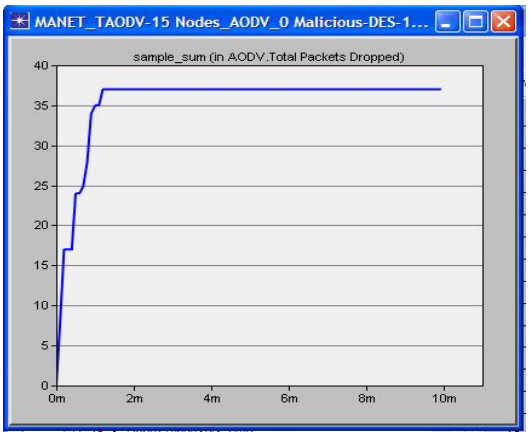
5.1 Simulation Results and Analysis

There were three scenarios used in our simulation i.e. 15 nodes, 30 nodes and the third one was 45 nodes. All scenarios were tested separately and separate graphs were obtained.

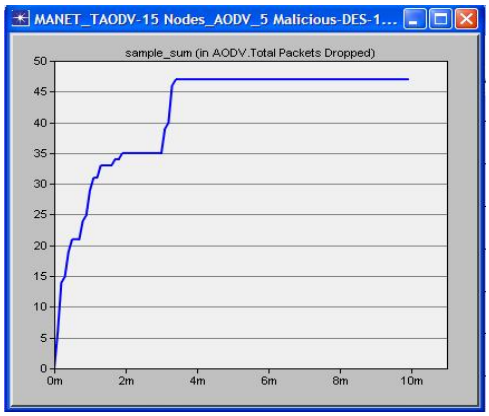
5.1.1 First Scenario

We made first scenario in which we used 15 mobile nodes from the object palette window of OPNET 14.0 and pasted all of them in the workspace window. For these 15 mobiles there had to be one server, so we took one fixed wlan_server from the object palette. These nodes were pasted in the campus network size of 1000 x 1000 meters. Once all the mobile nodes and fixed node server have been pasted on a workspace window, IPv4 addressing was assigned automatically to all nodes. After this we drag application_config and profile_config from object palette to workspace window. All the attributes of these two config(s) contain mostly the number of rows, speed in meters/seconds and pause time in seconds. So these settings must be done according to the requirement. The FTP was selected as traffic and FTP was set to High Load FTP traffic. After doing all the configurations to a network now it's time to deploy the configured profile which can be done by clicking Protocol tab in OPNET workspace window and selecting the Deploy Defined Application. Mobility_Config was also dragged into workspace window, all its necessary attributes had been set and then random mobility was set to MANET as a profile. Before running simulation, individual statistics had been selected from where we can choose protocols and wireless LAN etc. The figure of this first scenario is shown as follows in which all the three cases were compared in terms of number of packets dropped.

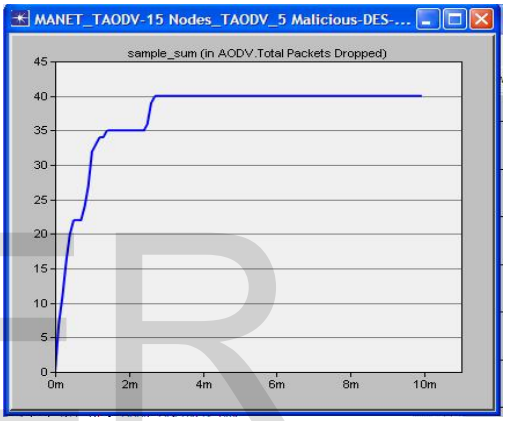
Case-1- This figure was taken after simulating case-1 of first scenario where we have 15 mobile nodes and 1 fixed node server. The protocol used is AODV with no malicious nodes. Number of packets dropped is shown in sample_sum graphical format. X-axis shows time in minutes and Y-axis shows number of packets dropped.



Case-2: This figure was taken after simulating case-2 of first scenario where we have 15 mobile nodes and 1 fixed node server. The protocol used is AODV with 5 malicious nodes. Number of packets dropped is shown in sample_sum graphical format. X-axis shows time in minutes and Y-axis shows number of packets dropped.

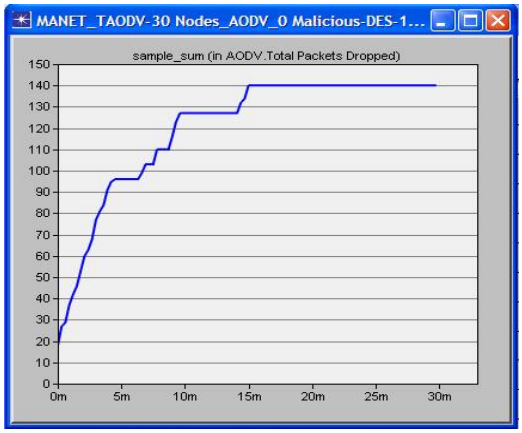


Case-3 This figure was taken after simulating case-3 of first scenario where we have 15 mobile nodes and 1 fixed node server. The protocol used is Trusted-AODV with 5 malicious nodes. Number of packets dropped is shown in sample_sum graphical format. X-axis shows time in minutes and Y-axis shows number of packets dropped.



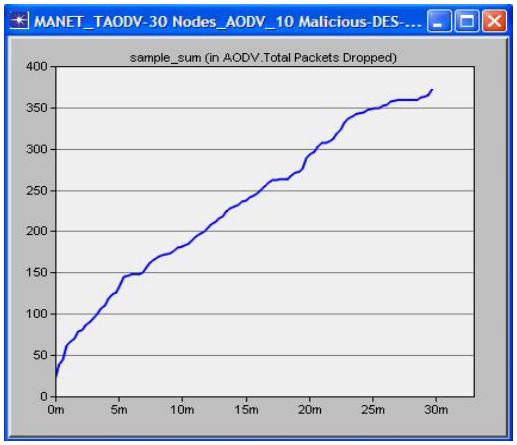
5.1.2 Second Scenario

Case-1: we have 30 mobile nodes and 1 fixed node server. The protocol used is AODV with no malicious nodes. Number of packets dropped is shown in sample sum graphical format. X-axis shows time in minutes and Y-axis shows number of packets dropped.

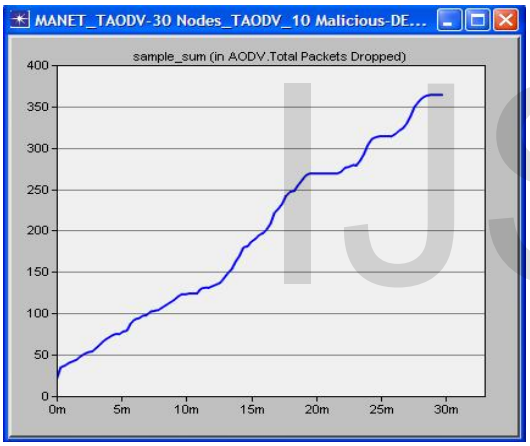


Case-2: This figure was taken after simulating case-2 of second scenario where we have 30 mobile nodes and 1 fixed node server. The protocol used is AODV with 10 malicious nodes. Number of packets dropped is shown in sample_sum

graphical format. X-axis shows time in minutes and Y-axis shows number of packets dropped.

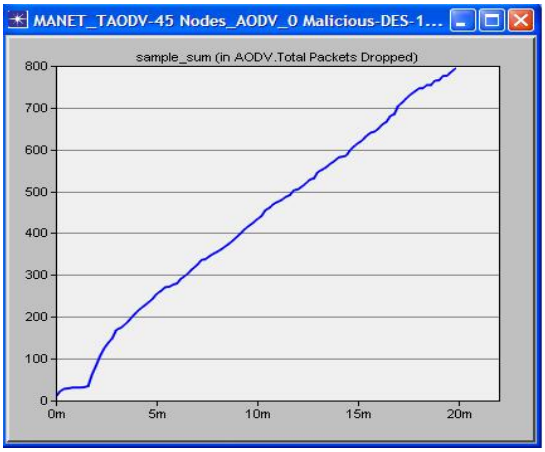


Case-3: This figure was taken after simulating case-3 of second scenario where we have 30 mobile nodes and 1 fixed node server. The protocol used is Trusted-AODV with 10 malicious nodes. Number of packets dropped is shown in sample_sum graphical format. X-axis shows time in minutes and Y-axis shows number of packets dropped.

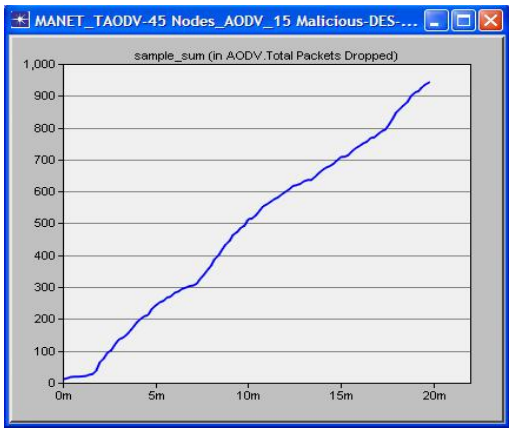


5.1.3 Third Scenario

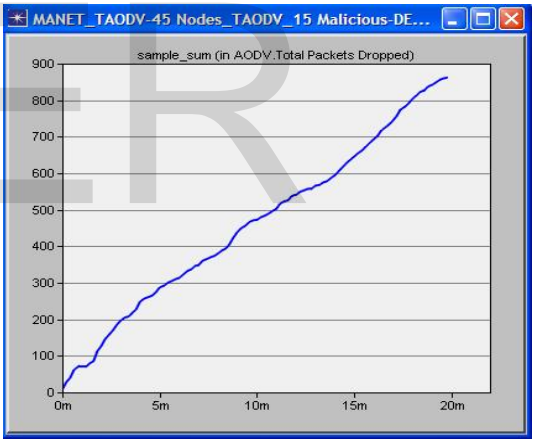
Case-1: This figure was taken after simulating case-1 of third scenario where we have 45 mobile nodes and 1 fixed node server. The protocol used is AODV with no malicious nodes. Number of packets dropped is shown in sample_sum graphical format. X-axis shows time in minutes and Y-axis shows number of packets dropped.



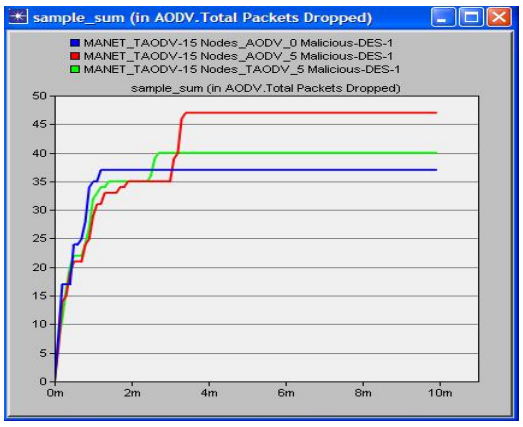
Case-2: This figure was taken after simulating case-2 of third scenario where we have 45 mobile nodes and 1 fixed node server. The protocol used is AODV with 15 malicious nodes. Number of packets dropped is shown in sample_sum graphical format. X-axis shows time in minutes and Y-axis shows number of packets dropped.



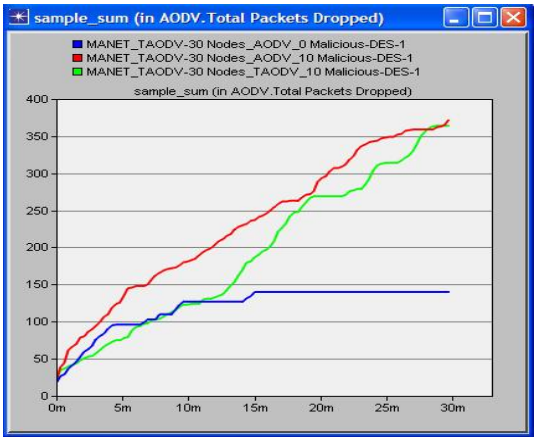
Case-3: This figure was taken after simulating case-3 of third scenario where we have 45 mobile nodes and 1 fixed node server. The protocol used is Trusted-AODV with 15 malicious nodes. Number of packets dropped is shown in sample_sum graphical format. X-axis shows time in minutes and Y-axis shows number of packets dropped.



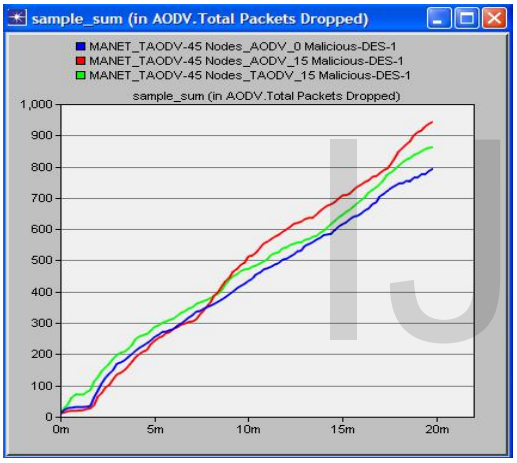
5.2 Comparison Of Case 1, 2 & 3 (Scenario-1)



5.3 Comparison Of Case 1, 2 & 3 (Scenario-2)



5.4 Comparison Of Case 1, 2 & 3 (Scenario-3)



6 CONCLUSIONS

This research paper improves the conventional AODV routing protocol in terms of packet loss, in presence of malacious nodes. If data is forwarded to these nodes then, this may lead to severe data loss, because they do not forward data packets. The proposed approach (Trusted-AODV) handles this problem. It guarantees that data is never forwarded to such nodes. Simulation results validate the approach in terms of decreased packet loss in presence of malicious nodes. Hence, using the proposed approach in presence of malicious nodes helps in reducing data loss.

REFERENCES

[1] C.E. Perkins, E. Beliding-Royer, S. Das, Ad hoc on-demand distance vector (AODV) routing, IETF Internet Draft, MANET working group, Jan. 2004.

[2] D.B. Johnson, D.A. Maltz, Y.-C. Hu, „„The Dynamic Source Routing Protocol for Mobile Ad-hoc Network (DSR)," IETF Internet Draft, July 2004.

[3] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, October 2003.

[4] Charles E. Perkins, Pravin Bhagwat, Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers, SIGCOMM (1994).

[5] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing," *Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps.*, New Orleans, LA, Feb. 1999, pp. 90–100.

[6] Akanksha Saini, and Harish Kumar, "Effect of Black Hole Attack on AODV Routing Protocol in MANET", International Journal of Computer Science and Technology, Vol.1, issue 2, Dec 2010

[7] Suman Deswal and Sukhbir Singh," Implementation of Routing Security Aspects in AODV", International Journal of Computer Theory and Engineering. Vol. 2, No. 1, February, 2010.

[8] Dr. Nakkeeran, B.Partibane, S.Sakthivel Murugan, N.Prabagarane." Detecting the malicious faults in MANET". International Journal of Computer Applications in Engineering, Technology and Sciences (IJ-CA-ETS), ISSN: 0974-3596, May"09-September"09.

[9] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy May/June 2004.

[10] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing," *Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps.*, New Orleans, LA, Feb. 1999, pp. 90–100.

[11] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, *"Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04*, April 2-3, 2004, Huntsville, AL, USA.

[12] Semih Dokurer, Y.M. Erten, Can Erkin Acar, „„Performance Analysis of Ad-hoc Networks under Black Hole Attacks", in: Proc. of the IEEE SoutheastCon, pp. 148–153, 2007.

[13] Ganesh Reddy, P.M. Khilar."Routing Misbehavior Detection and Reaction in MANETs", Proceedings of International Conference on Industrial and Information System, 2010,

[14] Frank Kargl, Andreas Klenk, Stefan Schlott, Michael Weber, "Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks", University of UIm, Dep. Of Multimedia Computing, UIm, Germany.

[15] Payal N Raj, Prashant B. Swadas, "DPRAODV: A Dynamic Larning System Against Blackhole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[16] Sunil kumar Senapati, Pabitra Mohan Khilar, "Securing FSR against data dropping by malicious nodes", International Journal of Applications in

Engineering, Technology and Sciences (IJ-CA-ETS), ISSN: 0974- 3596, April‟09-September‟09.