An Enhancement scenario of routing protocol scheme using TAODV protocol and fuzzy logic

[1]Prof. Ashish Khare, [2]Anubhav Sharma, [3]Rajeev Kumar Singh

[1]Professor & Head, Department of Information Technology, RITS, Bhopal (M.P.), India

[2]Department of Computer Science, RITS, Bhopal (M.P.), India

[3]Assistant Professor, Department of Computer Science, AITR, Bhopal (M.P.), India

[1]prof_ashish@rediffmail.com,[2]anubhav_sharma0025@yahoo.com,[3]rajeev_pratap@hotmail.com

Abstract- **An ad hoc network is a peer-to-peer network without centralized server. Mobile Ad- Hoc Network (MANETs) is a promising new wireless communications standard in which network device may move around and end hosts may function as a router. It is a key of success of being deployed to properly address the security problems. There are several researches focused on delivering packets from node to node and its security that will sure us for authentication delivery. Some nodes may behave maliciously, resulting in degradation of the performance of the network or even disruption of its operation altogether. Towards a solution of secure routing on MANETs, in this paper, we propose an enhanced algorithm for to reducing packet dropped rate. The feasibility of the proposed scheme of secure routing will be demonstrated by using OPNET simulator. In this paper we enhance AODV protocol and implement it in a 15 node scenario.**

INDEX ITEM- MANET, AODV, malicious nodes, Packet dropped rate, OPNET

1. Introduction-

Now a day's wireless ad-hoc network is getting more popularity as compared to wired networks. A wireless ad hoc network is a decentralized type of wireless network. The network is ad-hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. Ad-hoc networks demand a protocol completely different from those used for wired and infrastructure wireless networks. Ad-hoc networks have their own requirements and constraints and require a protocol that takes into account these issues and provide reliable communication under such constraints. The operation of Ad-hoc networks depends on the cooperation among nodes to provide connectivity and communication routes. However, such an ideal situation may not always be achievable in practice. Some nodes may behave maliciously, resulting in degradation of the performance of the network or even disruption of its operation altogether. To lessen the effect of such nodes and to achieve higher levels of security and reliability, this technology expands on relevant fuzzy logic concepts to propose an algorithm to establish quantifiable trust levels between the nodes of Ad-hoc networks. These trust levels are then used in the routing decision making process. Routing may be considered as two distinct processes: route discovery and packet forwarding. In wired networks, bandwidth is high and network topology is relatively static, compared to MANETs; as a result, wired networks typically employ proactive protocols such as OSPF [15] that strive to maintain a consistent picture of network connectivity throughout the routers in the network so that the next hop for an arriving packet can be computed quickly at each router. A mobile ad hoc network is an independent group of mobile users which communicate over unstable wireless links. Because of mobility of nodes, the network topology may change rapidly and unpredictably over time. All network activity, including delivering messages and discovering the topology must be executed by the nodes themselves. Therefore routing functionality, the act of moving information from source to a destination, will have to be incorporated into the mobile nodes .Hence routing is one of the most important issue in MANET.

Routing protocols in MANETs are generally classified as proactive and reactive [16]. Reactive routing protocols [4, 5, 6, 7, 8, 9], which also called on demand routing protocols, start to establish routes when required. These kinds of protocols are based on broadcasting RREQ and RREP messages. The duty of RREQ message is to discover a route from source to destination node .When the destination node gets a RREQ message, it sends RREP message along the established path. On demand protocols minimize the whole number of hops of the selected path and also they are usually very good on single rate networks. There are many reactive routing protocols, such as ad hoc on-demand distance vector (AODV) [17], dynamic source routing (DSR) [18], temporally order routing algorithm (TORA)[19], associatively-based routing (ABR) [20], signal stability-based adaptive (SSA) [21], and relative distance micro discovery ad hoc routing (RDMAR) [22]. In contrast , in table-driven or pro-active routing protocols [10,11,12,13,14], each node maintains one or more routing information table of all the participating nodes and updates their routing information frequently to maintain latest view of the network. In proactive routing protocols when there is no actual routing request, control messages transmit to all the nodes to update their routing information. Hence proactive routing protocols bandwidths become deficient. The major disadvantage of pro-active protocols is the heavy load caused from the need to broadcast control messages in the network. There are many proactive routing protocols, such as destination sequenced distance vector (DSDV), wireless routing protocol (WRP), cluster head gateway switch routing (CGSR), fisheye state routing (FSR), and optimized link state routing (OLSR) [10]. Many of the work reported on routing protocols have focused only on shortest path, power aware and minimum cost. However much less attention has been paid in making the routing protocol to choose a more reliable route. The open structure, lack of existing infrastructure and inaccessibility to trusted servers make traditional security methods and systems insufficient for Ad-hoc networks. This problem, faced with the presence of malicious nodes in Ad-hoc networks, requires the existence of a trust level based algorithm to alleviate the effect of such nodes. To address this problem an approach arising utilizing fuzzy logic concepts to establish trust relationships between nodes is proposed. To facilitate the quantification of trust levels for a node, information about the behavior history of this node is collected. Incorporating the concept of trust in Ad-hoc routing protocols and thereby mimicking human behavior, can further improve the performance and the reliability of Ad-hoc networks. It is expected that the establishment and quantification of trust levels can be used to detect nodes that misuse the trust placed in them. The detection of misbehaving nodes can be used to apply trust based route selection strategies to Ad-hoc routing protocols and thereby increase the effectiveness of the network. Four types of misbehaving nodes are considered in this paper. These include nodes that drop packets randomly, forward packets to the wrong destination, fabricate and transmit falsified routing messages, and launch replay attacks. Combining information related to these attacks by monitoring the neighboring nodes can facilitate the quantification of trust levels. Thus, a model utilizing fuzzy logic concepts is developed. To assign trust levels to nodes of Ad-hoc networks, a fuzzy trust evaluation application is developed using MATLAB [23]. This application receives information about the behavior history of Ad-hoc network nodes. The trust levels are then used by the routing protocol in an attempt to choose the most reliable route between the source and the destination nodes.

Using OPNET simulator, the proposed algorithm is validated and further studied. The findings show that when the proposed algorithm is utilized, the overall performance of the Ad-hoc network is significantly improved.

2. Proposed work-

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 behavior of nodes and then a route via such a node is never chosen by its neighbor to forward an application packet in the network.

3. Proposed algorithm-

Algorithm to identify malicious behavior of a neighbor node-

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

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

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

3. 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.

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

3.2 If the half-trusted node does not show malicious behavior 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:

3.3 No further RREP messages from this node will be entertained.

3.4 The application packets will not be forwarded to this node.

3.5 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.

Case-1:

- Total number of mobile nodes=15
- Number of malicious nodes=0

- Routing protocol used by nodes=AODV

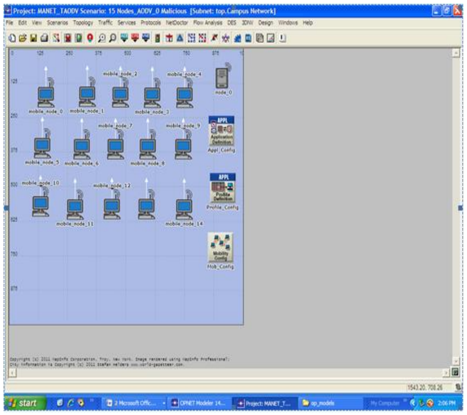
Project: MANET_TAODV Scenario: 15 Nodes_AODV_0 Malicious [Subnet: top.Campus Network]
File Edit View Scenarios Topology Traffic Services Protocols NetDoctor Flow Analysis DES 3DNV Design Windows Help
mobile_node_0
mobile_node_1
mobile_node_2
mobile_node_3
mobile_node_4
node_0
mobile_node_7
mobile_node_9
APPL
start

Figure (a) - Simulation Scenario (case 1)

Case-2:

- Total number of mobile nodes=15
- Number of malicious nodes=5
- Routing protocol used by nodes=AODV

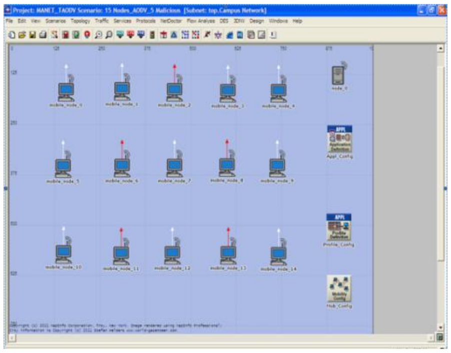
Project: MANET_TAODV Scenario: 15 Nodes_AODV_5 Malicious [Subnet: top.Campus Network]
File Edit View Scenarios Topology Traffic Services Protocols NetDoctor Flow Analysis DES 3DNV Design Windows Help
APPL

Figure (b) - Simulation Scenario (case 2)

Case-3:

- Total number of mobile nodes=15
- Number of malicious nodes=5
- Routing protocol used by nodes=Trust Based AODV (TAODV)

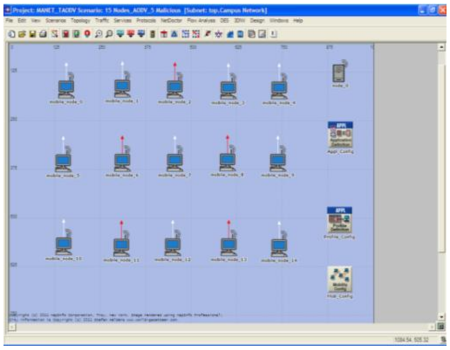
Project: MANET_TAODV Scenario: 15 Nodes_AODV_5 Malicious [Subnet: top.Campus Network]
File Edit View Scenarios Topology Traffic Services Protocols NetDoctor Flow Analysis DES 3DNV Design Windows Help
APPL

Figure (c) - Simulation Scenario (case 3)

4. Simulation results and analysis-

In this section, we have discussed the simulation results and the analysis that we have obtained after doing the simulation in OPNET Modeler 14.0. We simulated MANET with different cases 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. We are proposing a scenario using 15 nodes. This scenario is tested separately and separate graphs are obtained which are shown further. We made a scenario in which we used 15 mobile nodes from the object palette window of OPNET Modeler 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. After making scenario in OPNET Modeler 14.0, we run the simulation and check results of scenarios. We performed the simulation for 10 minutes (600 seconds) and graphs were saved in jpeg images. These graphs were found very helpful for statistical analysis as they are showing reasonable variations in the graphs.

(1)AODV 15 Nodes, No Malicious node-

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.

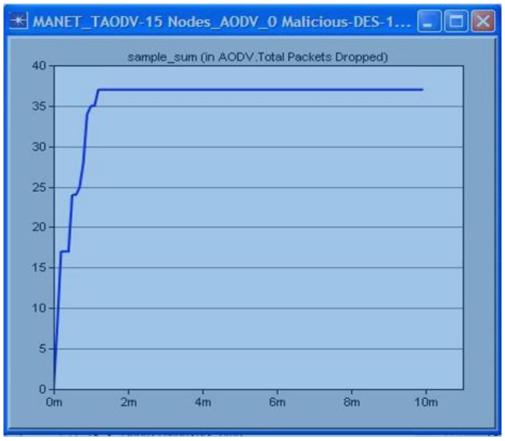

Figure- Graph representation of case (1)

(2) AODV 15 Nodes, 5 malicious nodes-

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.

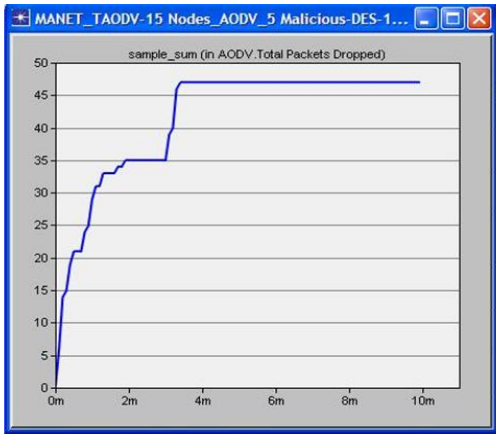

Figure- Graph representation of case (2)

(3)TAODV 15 Nodes, 5 malicious nodes-

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.

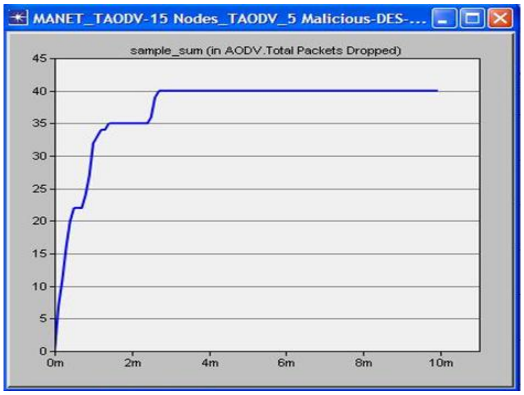

Figure- Graph representation of case (3)

Comparison of Scenario (Case I, II & III)-

In this section, we shown result through this graph and compare all three cases. And we find that TAODV i.e. enhancement of AODV Protocol, is performed better result/packet dropped rate.

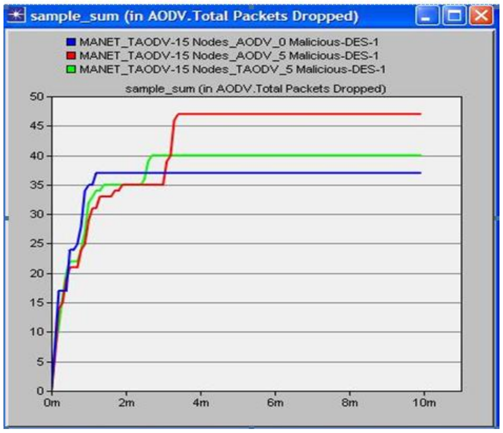

Figure- performance evaluation of both three cases

Total Nodes	Time (min)	Protocol	Malicious Nodes	Packets Dropped
15	2	AODV	0	37
		AODV	5	35
		TAODV	5	35
	4	AODV	0	37
		AODV	5	47
		TAODV	5	40
	6	AODV	0	37
		AODV	5	47
		TAODV	5	40
	8	AODV	0	37
		AODV	5	47
		TAODV	5	40
	10	AODV	0	37
		AODV	5	47
		TAODV	5	40

Figure- Comparison Evaluation of Scenario (all Three Cases)

5. Conclusions and future work-

This paper has highlighted, the effect of malicious nodes on the Performance of Ad-hoc networks is presented and importance of using trust levels to improve the reliability and performance of Ad-hoc networks. Evaluating trust levels between nodes of Ad-hoc networks poses a big challenge due to the lack of infrastructure in Ad-hoc networks. To overcome this limitation, a new approach based on fuzzy Trust Algorithm is proposed to facilitate the evaluation of trust levels between nodes of Ad-hoc networks. Simulation and experimental results collected after applying the TAODV approach show significant improvements in the performance and the reliability and Reduce the Packet dropped rate with reference to Time of Ad-hoc networks in the presence of malicious nodes.

However, a number of further investigations could be conducted to extend this approach. User make many trust-based decisions on a

Sub conscious level.

6. References-

1] H. Hallani , A. Hellany "Wireless Ad-Hoc Networks: Using Fuzzy Trust Approach to Improve Security between Nodes" Computer Engineering & Systems, 2009. ICCES 2009. International Conference on 14-16 Dec. 2009

2] H. Hallani, **Fuzzy Trust Approach for Wireless Ad-hoc Networks,** Communications of the IBIMA Volume 1, 2008

3] N.-C. Wang , Y.-F. Huang , J.-C. Chen, A stable weightbased on-demand routing protocol for mobile ad-hoc networks , Information Sciences 2007pp 5522–5537.

4] N.-C. Wang ,S.-W.Chang , A reliable on-demand routing protocol , Computer Communications 2005, pp 123–135 .

5] N.-C.Wang , C.-Y.Lee, A reliable QoS aware routing protocol with slot assignment for mobile ad hoc network , Journal of Network and Computer Applications Vol. 32, Issue 6, November 2009, Pages 1153-1166.

6] R. Patil and A.Damodaram, "Cost Based Power Aware Cross Layer Routing Protocol For Manet", IJCSNSInternational Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.

7] G. Nishant and D. Samir, "Energy-aware on-demand routing for mobile Ad Hoc networks," Lecture notes in computer science ISSN: 0302-743, Springer, International workshop in Distributed Computing, 2002.

8] M.Tamilarasi, T.G Palani Velu, "Integrated Energy-Aware Mechanism for MANETs using On-demand Routing", International Journal of Computer, information, and Systems Science, and Engineering 2;3 © www.waset.org Summer 2008.

9] M.Pushpalatha, Revathi Venkatraman, "Security in Ad Hoc Networks: An extension of Dynamic Source Routing", 10th IEEE Singapore International conference on Communication Systems Oct 2006,ISBN No:1-4244-0411-8,Pg1-5.

10] H. Wu1and C.n Shi1," A Trust Management Model for P2P File Sharing System", International Conference on Multimedia and Ubiquitous Engineering, IEEE Explore 78-0-7695-3134-2/08, 2008.

11] Arash Dana1, Golnoosh Ghalavand2, Azadeh Ghalavand 3 and Fardad Farokhi,": A Reliable routing algorithm for Mobile Adhoc Networks based on fuzzy logic" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011.

12] Suresh Kumar, Machha.Narender, and G.N.Ramesh "Security Provision For Mobile Ad-Hoc Networks Using Ntp & Fuzzy LogicTechniques", Global Journal of Computer Science and Technology Page |62 Vol. 10 Issue 8 Ver. 1.0 September 2010

13] H. Hallani, S. A. Shahrestani "Wireless Ad-hoc Networks: Employing Behaviour History to Combat Malicious Nodes"

14] V.Sumalatha and Dr P.C.Reddy "A Novel Approach for Misbehavior Detection in Ad hoc Networks " International Journal of Cryptography and Security Volume 2, Number 1, January 2009

15] 1. J. Moy, "OSPF Version 2," RFC 2328, April 1998.

16] D. Remondo, "Tutorial on wireless ad hoc networks", Second International Conference in Performance Modeling and Evaluation of heterogeneous networks, July 2004.

17] C.E. Perkins, E. Royer, Ad-hoc on-demand distance vector routing, Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, February, 1999 pp. 90–100

18] D.B. Johnson, D.A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, Kluwer, 1996.

19] V. Park, M.S. Corson, A highly adaptive distributed routing algorithm for mobile wireless networks, Proceedings of the 1997 IEEE INFOCOM, Kobe, Japan, April, 1997 pp. 1405–1413

20] C.K. Toh, A novel distributed routing protocol to support ad-hoc mobile computing, Proceedings of the fifteenth IEEE Annual International Phoenix Conference on Computers and Communications, March, 1996 pp. 480–486

21] R. Dube, C.D. Rais, K.Y. Wang, S.K. Tripathi, Signal stability-based adaptive routing (SSA) for ad hoc mobile networks, IEEE Personal Communications 4 (1997) 36–45.

22] G. Aggelou, R. Tafazolli, RDMAR: a bandwidth-efficient routing protocol for mobile ad hoc networks, Proceedings of the Second ACM International Workshop on Wireless Mobile Multimedia (WoWMoM), August, 1999 pp. 26–33.

23]Matlab,http://www.mathworks.com/products/matlab/.

24] X. Yang and N. Vaidya, "Priority Scheduling in Wireless Ad-hoc Networks," Wireless Networks, 2006, vol. 12, pp. 273-286.

25] L. Fanzhi, S. Xiyu, J. Sabah, and A. Christopher, "The effects of malicious nodes on performance of mobile Ad-hoc networks," In Proc. of the Mobile Multimedia/Image Processing for Military and Security Applications, 2006, pp. 1-6.