International Journal of Recent Trends in Engineering & Research
ISSN (ONLINE) : 2455 – 1457
IMPACT FACTOR : 4.101

Performance Evaluation of Secure AODV Routing Protocol for MANET

Nitin Pandit[1], Ravi Khatri[2]
[1]*Cyber security, Vikrant Institute of Technology and Management, Indore(Madhya Pradesh),India*
[2]*Vikrant Institute of Technology and Management, Indore(Madhya Pradesh),India*

Abstract— In mobile ad hoc networks (MANETs), the provision of quality of service (QoS) guarantees is much more challenging than in wire line networks, mainly due to node mobility, multi hop communications, contention for channel access, and a lack of central coordination. The difficulties in the provision of such guarantees have limited the usefulness of MANETs. In the last decade, much research attention has focused on providing QoS assurances in MANET protocols. In this paper we have analysed different types of routing protocols and QoS metrics in MANETS. Secure AODV (SAODV) routing protocol modify the effect of AODV routing protocol. In SAODV is preferred to achieve best result in terms of end-to-end delay, energy packet delivery ratio and throughput**.**

Keywords— MANETS, Qos, unicast rouing protocols, multicast Routing protocols.

I. INTRODUCTION

Wireless communication technology have been developed with two primary models one is fix infrastructure based model in which much of the nodes are mobile and connected through fixed backbone nodes using wireless medium. Another model is Mobile Ad-hoc network .Mobile Ad-Hoc Networks (MANETs) are comprised of mobile nodes (MNs) that are self-organizing and cooperative to ensure efficient and accurate packet routing between nodes (and, potentially, base stations). There are no specific routers, servers, access points for MANETs. Because of its fast and easy of deployment, robustness, and low cost, Typical MANETs applications could be find in the following areas like Military applications (i.e. a temporary network in the battlefield), Search and rescue operations, Temporary networks within meeting rooms, airports, Vehicle-to-vehicle communication in smart transportation, Personal Area Networks connecting mobile devices like mobile phones, laptops, smart watches, and other wearable computers etc. Design issue for developing a routing protocol for wireless environment with mobility is very different and more complex than those for wired network with static nodes [1]. Main problem in mobile ad-hoc network are limited bandwidth and frequent changes in the topology.

II. ROUTING PROTOCOLS IN MANETS

Routing protocols In [3], QoS routing protocols are classified chiefly by their: First one is uni-cast Routing Protocol, second one is multicast Routing Protocol. Different routing protocols try to solve the problem of routing in mobile ad hoc network in one way or the other. Unicast routing protocols and the multicast routing protocol are divided into proactive, reactive and hybrid routing protocol. Figure 1 gives a classification on routing protocol is based on uni-cast and multicast routing protocol.

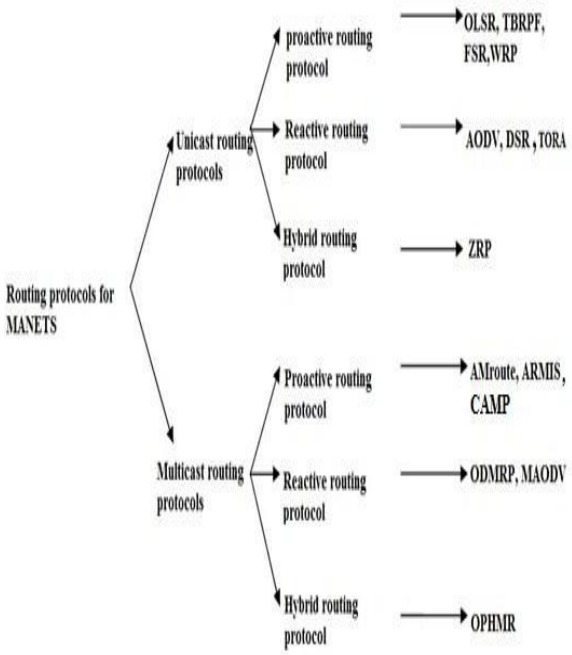

Fig 1: Classification of routing protocols for MANET

The Ad Hoc On-demand Distance Vector Routing (AODV) protocol [15] is a reactive unicast routing protocol for mobile ad hoc networks. As a reactive routing protocol, AODV only needs to maintain the routing information about the active paths. In AODV, routing information is maintained in routing tables at nodes. Every mobile node keeps a next-hop routing table, which contains the destinations to which it currently has a route. A routing table entry expires if it has not been used or reactivated for a pre-specified expiration time. Moreover, AODV adopts the destination sequence number technique used by DSDV in an on-demand way.

III. IMPLEMENTATION

Reputation Management

Modified AODV is a Secure ad-hoc on demand vector routing (SAODV), is a protected routing protocol based on trust model for Mobile ad-hoc network. SAODV has several features as nodes perform trusted routing behaviors, mainly according to the trust dependency among them.

AODV routing protocol is implemented along with the trust function. The communication between the nodes in the mobile ad-hoc network depends on the cooperation and the trust level with its neighbors. Based on the security with a neighbor, an appropriate value of the node can classified as:

1. *Unreliable:* The Unreliable is the non-trusted node. Unreliable node is a node with minimum trust level. Originally, when any node joins, in the networks the trust relationships with its neighbors are low then that nodes are treated as Unreliable.

2. *Reliable:* These are the nodes, which have the trust level between the Most Reliable and Unreliable. A node is considered as Reliable only if it has received some packets from its neighboring node.

3. *Most Reliable:* Most Reliable are the most trusted nodes with highest trust level. Here the higher trust level means neighbors had received or send many packets successfully through this particular node. At the route discovery phase of the Ad hoc On Demand Distance Vector Routing protocol, the trust value is calculated for all the neighbors of any node.

The following flow of steps is the detailed description of the SAODV algorithm.

Step 1: Nodes are connected with each other for relaying messages in mobile ad-hoc network. Every node is initialized with Trust index=0.7.

Step 2: Source node transmits the route request packet to its neighbor nodes for relaying messages to the destination.

Step 3: Neighbor node first checks the route in its cache memory, if it exists, then it sends a route reply to the source node.
Otherwise, intermediate nodes send same route request to its neighbors and further to other intermediate nodes until the destination is found.
Step 4: When a route reply message is received from the neighbor nodes. Source node first checks sequence number and trust index of replying nodes, and select the highest reputed node for relaying messages.
Step 5: Source node transfers the message through the selected neighbor nodes.
Step 6: If a message is delivered correctly then the trust value of the neighbor is increased If not delivered then the trust value is decreased.
Step 7: All the nodes having trust index less than 0.7 are termed as black hole nodes and these nodes are black listed.

Table: Basis for deciding Trustworthiness of the Node

Most Reliable	Unreliable	Reliable	Action
		≥0.7	Request and check again
	<0.7		Disbelief the node
>0.7			Trusted node

A. Packet Delivery Ratio
It is the ratio of actual packets delivered to total packets sent.

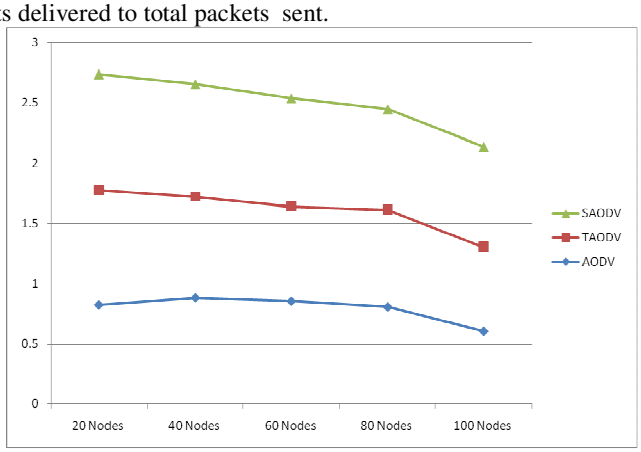

Figure 1 Packet Delivery Ratio

B. End to End delay
This is the average delay between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes.

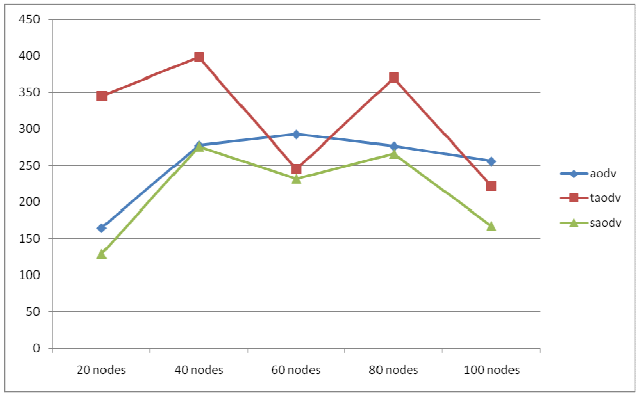

Figure 2 End to End Delay

C. Residual Energy

It is the total amount of remaining energy by the nodes after the completion of Communication or simulation. If a node is having 100% energy initially and having 70% energy after the simulation than the energy consumption by that node is 30%.The unit of it will be in Joules.

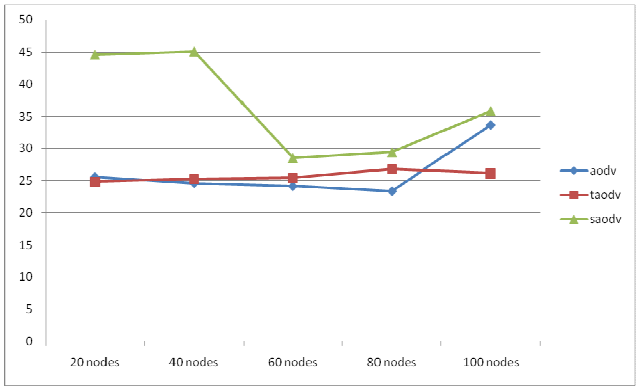

Figure 3 Energyy

D. Throughput

Throughput is the rate of successful message delivery over a communication channel. It is usually measured in kilobits (kilobit/s or kbps).

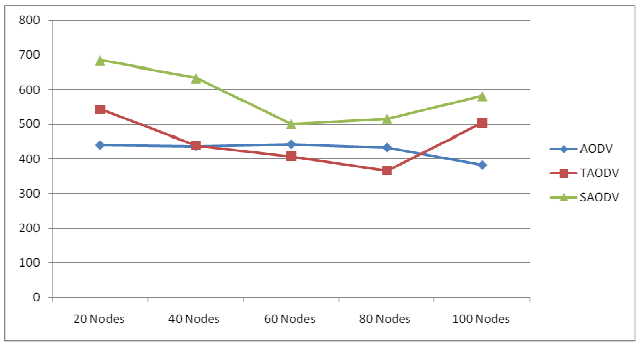

Figure 4 Generated Throughput

IV. CONCLUSION

In this paper, much research attention has focused on providing QoS assurances in MANET protocols. In this paper we have analyses different types of routing protocols and QoS metrics in MANETS. Secure AODV (SAODV) routing protocol modiffy the effect of AODV routing protocol. In SAODV is preferred to achieve best result in terms of end-to-end delay, energy packet delivery ratio and throughput**.**

REFERENCES

[1] X.Li, M.Lyu and J.Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks",in IEEE Proceedings of the Aerospace Conference,Vol.2,pp.1286-1295, March 2004.

[2] A.Pal, J.P.Singh and P. Dutta, "The Effect of speed variation on different Traffic Patterns in Mobile Ad Hoc Network",in the 2nd International Conference on Computer,Communication, Control and Information Technology, Vol.4, pp.743-748, February 2012.

[3] A.Sharma, D.Bhuriya, U.Singh and S.Singh, "Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing",in International Journal of Computer Science and Information Technologies, Vol.5,no.4, pp.5021-5025, August 2014.

[4] A.Mehta, R.Jain and V.Somani, "Comparison of different Radio Propagation Models with and without Black Hole Attack on AODV Routing Protocol in MANET", in Proceedings of the International Journal of Computer Applications, Vol.61, no.1, pp.20-24, January 2013.

[5] R.Bar , J.Mandal and M.Singh, "QoS of MANet Through Trust based AODV Routing Protocol by Exclusion of Black Hole Attack", in Proceedings of the 1stInternational Conference on Computational Intelligence,Modeling Techniques and Applications, Vol.10 ,pp.530- 537, December 2013.

[6] P.Singh and G.Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET",in IEEE Proceedings of the 11th International Conference on Trust,Security and Privacy in Computing and Communications, pp.902-906, June 2012.

[7] A.Sharma and U.Singh, "Performance Evolution for Mobile ad- hoc networks on black hole AODV and TAODV", in the 11th IRF International Conference, pp.169-173,June 2014.

[8] S.Singh, A.Dixit and K.Gupta, "Comparative Analysis of performance of black hole detection techniques",in Proceedings of the International Journal of Science Technology and Management,Vol.4, no.1,pp.648-653, February 2015.
[9] A.Bala, M.Bansal and P.Singh, "Performance Analysis of MANET under Black hole Attack",in Proceedings of the 1st International Conference on Networks and Communications(NETCOM), pp.141- 145, December 2009.
[10] C.E.Perkins and E.M.Royer, "Ad-hoc On Demand Distance Vector Routing",in IEEE Proceedings of the 2nd Workshop on Mobile Computing Systems and Applications, pp.90-100, Febuary 1999.
[11] Murthy, S. and J.J. Garcia-Luna-Aceves, ―An Efficient Routing Protocol for Wireless Networks‖, *ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks*, Oct. 1996, pp. 183-97.
[12] M. Ismail. ―Routing Protocols for Ad Hoc Wireless Networks‖, M.Sc. (ISS) project, Carleton University, Ontario, Canada, August 2001.
[13] J. N. Al-Karaki and A. E. Kamal, ―Quality of Service Routing in Mobile Ad Hoc Networks: Current and Future Trends,‖ Mobile Computing Handbook, I. Mahgoub and M. IIays, Eds., CRC Publishers,2004. http://www.csjournals.com/ IJITKM/Special1 / UNICAS T ANDMULTICAST.pdf
[14] C. R. Lin and J.-S. Liu, ―QoS Routing in Ad Hoc Wireless Networks,‖ *IEEE JSAC*, vol. 17, Aug. 1999, pp. 1426–38.
[15] S. Chen and K. Nahrstedt, ―Distributed Quality-of-Service Routing in Ad Hoc Networks,‖ *IEEE JSAC*, vol. 17, Aug. 1999,pp. 1488–505.
[16] A. R. Bashandy, E. K. P. Chong, and A. Ghafoor, ―Generalized Quality-of-Service Routing with Resource Allocation,‖ *IEEE JSAC*, vol. 23, Feb. 2005, pp. 450–63.
[17] M. Wang and G.-S. Kuo, ―An Application-Aware QoS Routing Scheme with Improved Stability for Multimedia Applications in Mobile Ad Hoc Networks,‖ *Proc. IEEE Vehic. Tech. Conf.*, Sept. 2005, pp. 1901–05.
[18] A. Abdrabou and W. Zhuang, ―A Position-Based QoS Routing Scheme for UWB Mobile Ad Hoc Networks,‖ *IEEE JSAC*, vol.24, Apr. 2006, pp. 850–56.
[19] P. Jacquet, P. Muhlethaler, and A. Qayyum, ―Optimized Link State Routing Protocol‖, *IETF MANET, Internet draft*, 1998.
[20] Mario Gerla, Xiaoyan Hong, and Guangyu Pei, ―Fisheye State Routing Protocol (FSR) for Ad Hoc Networks‖, *draft-ietf-manet-fsr- 03.txt,* June 2002.