ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Improved Network Performance by Avoiding Attack on Routing Path Using Shortest Path Routing

B.Vinod, D.Balaji

Assistant Professor, Dept. of ECE, Ganesh College of Engineering, Salem, India

Assistant Professor, Dept. of ECE, Mahendra College of Engineering, Salem, India

ABSTRACT: MANET routing protocols are designed to scale up to thousands of routers with frequent changes of the topology. MANETs require a reliable, efficient, and scalable and most importantly, a secure protocol as they are highly secure, self-organizing, rapidly deployed and they use dynamic routing. In preference, MANET routing protocols should also support constrained low-power devices. AODV is flat to attacks like modification of sequence numbers, modification of hop counts, source route and production of error messages. AODV does not specify any special security measures. The proposed scheme we have to using a shortest path used to avoiding any type of attacking model on the network. Route Request and Route Reply from the data transmission on the source to destination on network process. Mainly to focus on compare the AODV with proposed secure routing to reduce the packet delay and improve network performance and then saving an energy level of the network.

KEYWORDS: AODV, S-AODV, Throughput, Packet loss, End Delay

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a dynamic wireless network with or without fixed infrastructure. Nodes may move freely and arrange themselves randomly. The contacts between nodes in the network do not occur very frequently. As a result, the network graph is rarely, if ever, connected and message delivery required a mechanism to deal with this environment Routing in MANET using the shortest-path metric is not a sufficient condition to construct high-quality paths, because minimum hop count routing often chooses routes that have significantly less capacity than the best paths that exist in the network [1,2]. Due to the frequently change in the network topology there is a significant change in the status of trust among different nodes which adds the complexity to routing among the various mobile nodes. The self-organization of nodes in ad hoc networks may to deny providing services for the advantage of other nodes in order to keep their own resources acquaint new security that are not addressed in the infrastructure-based networks in MANET. Routing protocols for MANETs are usually classified into proactive and reactive protocols, and hybrid protocols based on how routing information is acquired and maintained by mobile nodes.

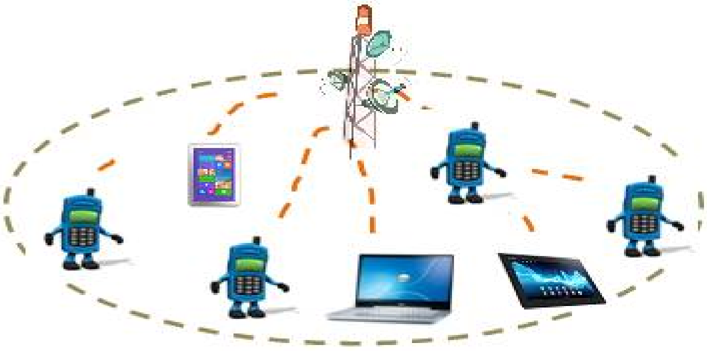


Fig.1 MANET

DOI: 10.15680/IJIRCCE.2016. 0402169

AODV is another routing algorithm used in ad hoc networks, it does not use source routing, but it is on-demand. In S-AODV, each node maintains a routing table which is used to store destination and next hop IP addresses as well as destination sequence numbers. Each entry in the direction-finding table has a destination talk to, next hop, procedural nodes list, lifetime, and distance to destination. We defined a console as the set of sensors that will be required to route high priority packets from the data sources to the sink [4]. Our solution does not require active queue organization, maintenance of multiple queues or preparation algorithms, or the use of specialized MAC protocols of the network[3]. Our wide simulations show that as compared to AODV with secure AODV.

An efficient network Traffic control has to prevent the packets losses, which are caused by unexpected traffic bursts. Thus, it has to estimate the dynamic behavior of the traffic in the nodes buffers and to send sources the congestion notifications early enough. Therefore, due to the dynamic nature of buffer occupancy and congestion at a node, it is expected that by applying traffic aware routing and to find the shortest path Routing (SPR) model on the network performance system [6]. We have to using a shortest path route finding on a model that have to using a best route find determination on the mobile ad hoc network.

II. RELATED WORK

The Performance metrics that are used to evaluate routing protocols are Routing Overhead, Throughput and Average End to End Delay, Packet loss ratio. Shortest path algorithm is a simple and easy to understand method [8]. In basic design of this technique is to construct a graph of the subnet, with each node of the graph in place of a router and each arch of the graph representing a message line using link. For result a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph. The length of a path can be measured in a number of ways as on the basis of the number of hops, or on the basis of area distance. They have more using the routing method to implementing for a data transmission on the system [5].

Security attacks in MANET routing can be divided in network performance model on intention of a attack is typically to listen and retrieve vital information inside data packets, for example by launching a traffic monitoring attack. In such an attack, a malicious node tries to identify communication parties and functionality which can provide information to launch further attacks. The attack type is called passive since the normal functionality of the network is not altered. That time to identify the attack model, so we have using the secure and efficient routing protocol and then avoiding model of their process[7,9]. The route discovery begins with the flooding of Route Request (RREQ) messages by a source node. RREQ is broadcast from source S, received by the neighbor nodes of S, and then is rebroadcast.

This Multihop transmission allows the RREQ to reach the expected destination D. In response to the RREQ, D unicast Route Reply (RREP) messages toward S. This RREP will eventually reach the source node through the Multihop path. In this way, the route from S to D is established. It should be noted that this path is the shortest path out among possible routes, and is best route performance on their network. Hybrid routing protocols aggregates a set of nodes into zones in the network topology.

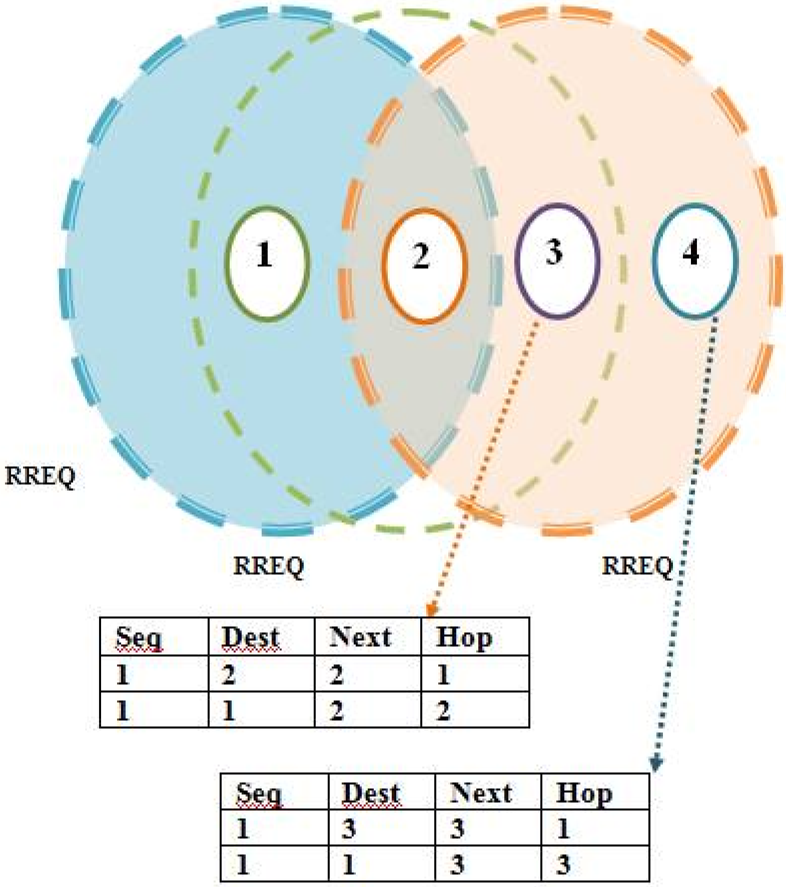
Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information [11]. To route packets between different zones, the reactive approach is used [10]. Consequently, in hybrid schemes, a route destination that is in the same zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones. The routing protocol provide a compromise on scalability issue in relation to the frequency of end-to-end connection, the total number of nodes, and the frequency of topology change.

A. PROPOSED APPROACH

The nodes in MANETs perform the routing functions in addition to the inbuilt function of being the network. The limitation on wireless transmission range requires the routing in multiple hops. So the nodes depend on one another for transmission of packets from source nodes to destination nodes via the routing nodes [12]. So we have to take hybrid pro active and reactive routing and to data transmission for all the network nodes. Most routing protocols have been designed without taking security into account. It has been assumed that all nodes in a MANET are trusted.

B. EFFICIENT SECURE AD HOC ON-DEMAND DISTANCE VECTOR ROUTING

AODV is basically an improvement of DSDV which is a reactive routing protocol instead of proactive. AODV have to include Efficient Secure system improving a network performance model system. It minimizes the number of broadcasts by creating routes based on demand, if we have any source node wants to send a message to a destination, it broadcasts a route request (RREQ) message.



Seq	Dest	Next	Hop
1	2	2	1
1	1	2	2

Seq	Dest	Next	Hop
1	3	3	1
1	1	3	3

Fig 2. S-AODV routing

The neighboring nodes in turn broadcast the message to their nearest node and the process continues until the message reaches the destination. While the route request message is forwarded, intermediate nodes record the address of their neighboring nodes from which the first copy of the broadcast packet is received[14]. The messages are discarded if later the additional copies of the same RREQ messages are received.

C. SHORTEST PATH ROUTING

Shortest path routing (SPR) in which average conditional intermeeting times are used as link costs rather than standard intermeeting times and the messages are routed over the network. A comparison is made between SPR protocol with the existing system model based routing protocol through real trace- driven simulations. The results demonstrate that SPR achieves higher delivery rate and lower end-to-end delay compared to the shortest path based routing protocols [13]. This shows how well the conditional intermeeting time represents internodes link costs and helps making effective forwarding decisions while routing a message.

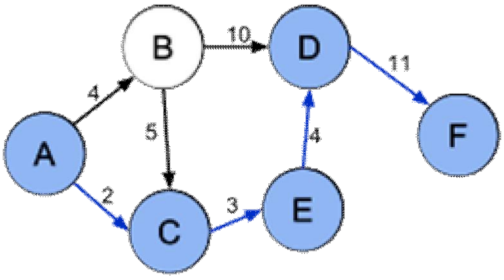


Fig.2. Shortest Path Routing

Routing algorithms utilize a paradigm called store-carry-and-forward. It generates the multiple messages from a random source node to a random destination node at each second.

Step 1: Source node broadcasts a RREQ
Step 2: Authenticate the RREQ
Step 3 : calculate its security level
Step 4: update the security level in the RREQ packet
Step 5: broadcast the RREQ to its neighbor nodes
Step 6: if network=traffic then Q queue check to D
Step 7: SPR -> D {Shortest path routing model}
Step 8: If network ≠ T Route SPR to D
Step 9: Dropped Packets Find another
Step 10: By SPR algorithm model S data send to D on network
Step 11: route path selection method process over

D. PERFORMANCE ANALYSIS

The goal of our simulation is to analyze the behavior of the ES-AODV by deploying mobile ad hoc Networks. The simulation environment is created in NS-2, a network simulator that provides support for simulating mesh wireless networks. NS-2 was written using C++ language and it uses the Object Oriented Tool Command Language (OTCL). It came as an extension of Tool Command Language (TCL).

The simulations were carried out using a mobile node environment consisting number of wireless mobile nodes roaming over a simulation area of 1000 meters x 1000 meters flat space operating for 10 seconds of simulation time. The radio and IEEE 802.11 MAC layer models were used. Nodes in our simulation move according to Random Waypoint mobility model, which is in random direction with maximum speed from 0 m/s to 20 m/s. A free space propagation channel is assumed for the simulation.

PARAMETER	VALUE
Simulator	Ns-2
Propagation Model	Two Ray Ground
MAC Layer	IEEE 802.11
Simulation Time	10 m sec
Average Delay	1ms
Simulation Area	1000*1000m
Transmission Range	50-300 m
Node Movement Model	Random Way Point
Traffic Model	CBR(UDP)
Transfer per Packet	512 Bytes

Table 1. Parameters for Simulation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Hence, the simulation experiments do not account for the overhead produced when a multicast members leaves a group. Multicast sources start and stop sending packets; each packet has a constant size of 512 bytes. Each mobile node in the network starts its journey from a random location to a random destination with a randomly chosen speed.

E. PERFORMANCE RESULTS

The simulation scenario is designed specifically to assess the impact of network concentration on the performance of the protocols. The impact of network density is assessed by deploying 80 nodes over a fixed square topology area of 1000m x 1000m using 5m/s node speed and 3 identical source-destination connections. S-AODV has a number of quantitative metrics that can be used for evaluating the performance of mobile ad hoc network. We have used the following metrics for evaluating the performance.

III. SIMULATION RESULTS

No	Protocol	Throughput	End-to-end Delay	Overhead	Packet loss Ratio
1	AODV	**90%**	**95%**	**98%**	**93%**
2	S-AODV	**98%**	**45%**	**80%**	**50%**

Table 2. Comparison Table of existing and proposed

F. THROUGHPUT PERFORMANCE

It is the ratio of throughput performance overall network performance improve network performance and packet delivery ratio and minimize packet delay.

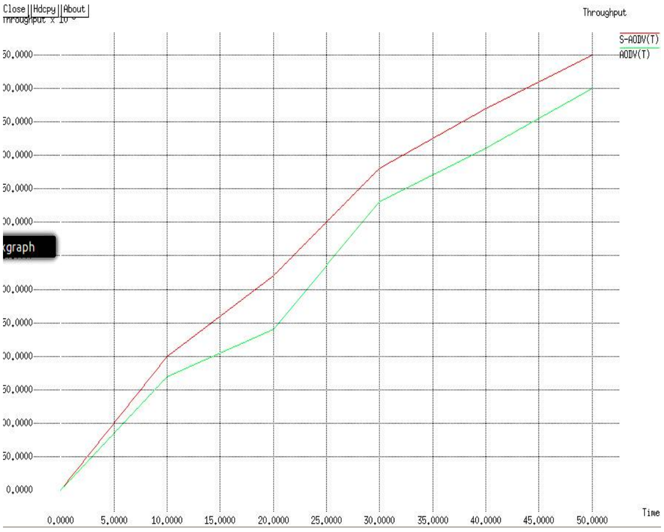


Fig. 3. Throughput of routing Protocols

G. AVERAGE END-TO-END DELAY

This includes all possible delay caused by buffering during route discovery latency, queuing at the interface queue, retransmission delay at the propagation and transfer time. It is defined as the time taken for a data packet to be transmitted across an MANET from source to destination.

$$D = (Tr - Ts)$$

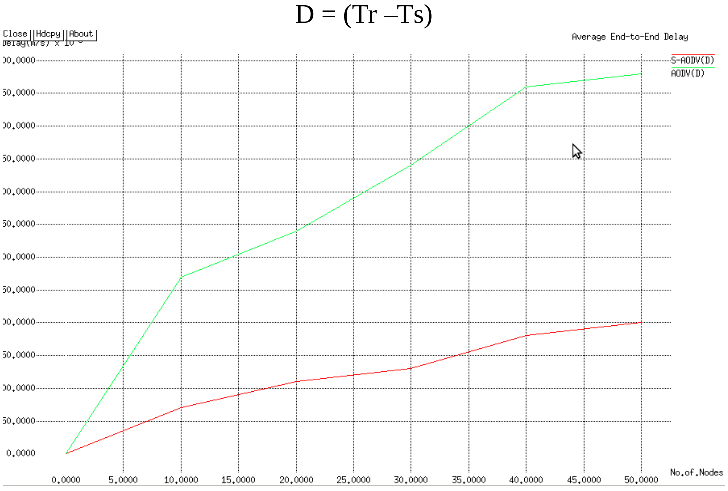


Fig 4. Average end-to-end delay

H. ROUTING OVERHEAD

Nodes often change their location within network. so, some stale routes are generated in the routing table which leads to unnecessary routing overhead. Since the graph describes the performance of the overhead ratio of the protocols.

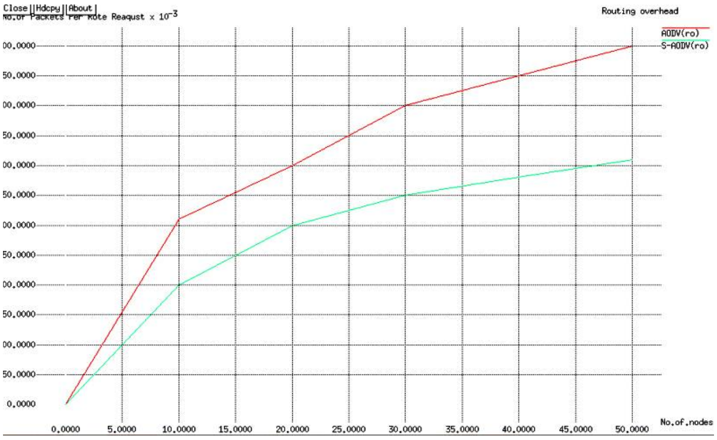


Fig 5. Routing overhead

I. PACKET LOSS RATIO

Packet loss is the failure of one or more transmitted packets to arrive at their destination. Since the packet loss ratio of the corresponding ratio of the routed packets are determined. The graph explains the comparison of ratio of loss regarding the delivery of the packets.

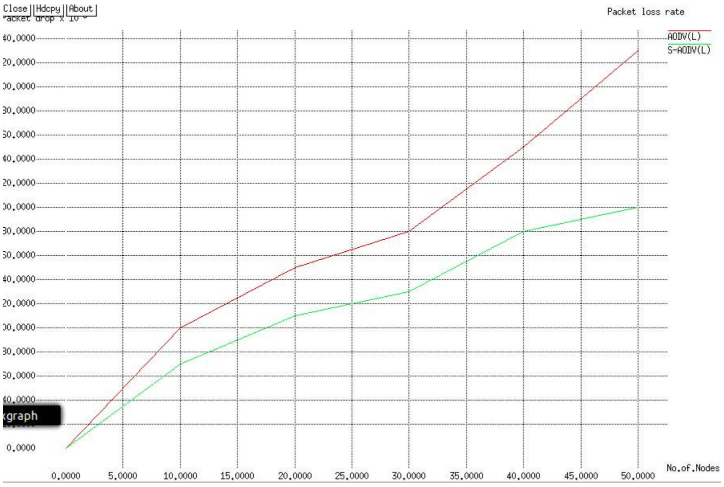


Fig 6. Packet loss ratio

IV. CONCLUSION AND FURTURE WORK

Hence we developed Secure AODV protocol to using the trust management architecture for security solutions based on intrusion detection system on network. It thus can easily be sending the data on routing method and then SPR algorithm to be implemented on the process. In this paper, a Shortest Path Routing algorithm model on packet optimization has been proposed to improving throughput. In our future work to take a different protocol comparison with for Secure method using the shortest path where further increase in the performance.

REFERENCES

[1]Arvind Dhaka, raghuveer Singh Dhaka, priyank hada" A security in zone routing protocol for Manet", IJREAS volume 2, issue 2 (February 2012).
[2]K. Thamizhmaran1, R. Santhosh Kumar Mahto, V. Sanjesh Kumar Tripathi," Performance Analysis of Secure Routing Protocols in MANET", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 9, November 2012
[3] Gaurav kadyan, sitender malik," comparative study of various hybrid routing protocols for mobile ad-hoc network", international journal of latest research in science and technology vol.1, issue 2: page no145- 148,July-august 2012.
[4] K. Sahadevaiah," Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks", Network Protocols and Algorithms ISSN 1943-3581 2011, Vol. 3, No. 4, 2010.
[5] Priyanka Goyal1, MANET: Vulnerabilities, Challenges, Attacks, Application, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.
[6] Attila A. YAVUZ, Faith ALAGOZ," A new multi-tier adaptive military MANET security protocol using hybrid cryptography and sign cryption", Turk J Elec Eng & Comp Sci, Vol.18, No.1, 2010.
[7] Augustan Caminero," Network-aware Peer-to-Peer Based Grid Inter-Domain Scheduling", at 2008.
[8] Ramesh, D. and A. Krishnan," An Optimal Load Sharing Technique for Grid Computing", American Journal of Applied Sciences.
[9] Ying Chen, Ataul Bari," Techniques for Designing Survivable Optical Grid Networks", JOURNAL OF COMMUNICATIONS, VOL. 7, NO. 5, MAY 2012.
[10] Takeshi Matsuda, Hidehisa Nakayama," Gateway Selection Protocol in Hybrid MANET Using DYMO Routing", 2010.
[11] S.Sriram, Sunther," Performance Evaluation of Route Securing Protocols in MANET", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.
[12] Celia Li, Zhuang Wang, and Cungang Yang," Secure Routing for Wireless Mesh Networks", International Journal of Network Security, Vol.13, No.2, PP.109–120, Sept. 2011.
[13] S. Prasad, Y.P.Singh, and C.S.Rai," Swarm Based Intelligent Routing for MANETs", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.
[14] Parul Tomar, Prof. P.K. Suri," A Comparative Study for Secure Routing in MANET", International Journal of Computer Applications (0975 – 8887) Volume 4 – No.5, July 2010.