6th International Conference on Recent Innovations in Science, Engineering and Management
IIMT College of Engineering (Approved by AICTE, New Delhi), Knowledge Park III, plot no. 20-A, Greater Noida, Uttar Pradesh (India) (ICRISEM)
20th August 2016, www.conferenceworld.in ISBN: 978-93-86171-03-0

MESH BASED MULTICAST ROUTING SCHEME FOR ENHANCING QOS AND SECURITY WHILE ROUTING IN MOBILE AD HOC NETWORK

[1] Gautam M Borkar, [2] A. R. Mahajan

[1]Assistant Professor, Rajiv Gandhi Institute of Technology, Versova, Andheri West, Mumbai,(India)

[2]Head, Department of Information Technology, Government Polytechnic College, Nagpur, Maharashtra (India)

ABSTRACT

A Mobile Ad hoc network (MANET) is a self-configurable network connected by wireless links. This type of network is only suitable for temporary communication links as it is infrastructure-less and there is no centralized control. Providing QoS and security aware routing is a challenging task in this type of network due to dynamic topology and limited resources. The main purpose of QoS aware routing is to find a feasible path from source to destination which will satisfy two or more end to end QoS constrains. A mesh based multicast routing scheme will proposed in this work. The proposed multicast routing scheme (MRS) finds stable multicast path for multimedia transmission in MANET. The shortest path is find by the ant colony optimization algorithm (ACO).Performance of the proposed scheme is compared with existing multicast routing protocols. It is observed that the proposed scheme produces better packet delivery ratio, reduced packet delay, reduced overheads (such as control, memory, computation, and message overheads) and provide security against vulnerabilities and attacks with low resource consumption.

Keywords: mobile ad hoc network (MANET), multicast routing scheme (MRS), quality of service (QoS), ant colony optimization algorithm (ACO).

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internet worked in areas without a pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension [1]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges [2] [11]; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other [14]. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network [3]. Routing protocols for ad hoc networks must deal with limitations such as high error rates, scalability, security, quality of service, energy efficiency, multicast, aggregation and node cooperation etc. [12]. Here, qualitative properties like security and quality of service are taken into account.

 ISBN: 978-93-86171-03-0

While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multi hop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment [4]. A MANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to watch network traffic, replay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security provisions [5]. The primary goal of a MANET routing protocol is to establish a correct and efficient route between a pair of nodes so that messages may be delivered in a timely manner. If routing can be misdirected, the entire network can be paralyzed. Thus, routing security plays an important role in the security of the whole network [6].

Quality of Service (QoS) is usually defined as a set of service requirements that needs to be met by the network while transporting a packet stream from a source to its destination [9]. QoS routing requires not only finding a route from a source to a destination, but a route that satisfies the end to-end QoS requirement, in terms of bandwidth or delay. The role of a QoS routing strategy is to compute paths that are suitable for different type of traffic generated by various applications while maximizing the utilizations of network resources. To find a path from source to destination satisfying user's requirements, to optimize network resource usage and to degrade the network performance when unwanted things like congestion, path breaks appear in the network [10] are the main objectives of QoS.

Routing is critical to QoS support, while its performance is vulnerable to changes in network topologies. In mobile wireless networks, such changes are mainly caused by node mobility [13]. Also security can be considered a QoS attribute. Without adequate security, unauthorized access and usage may violate QoS negotiations. The nature of broadcasts in wireless networks potentially results in more security exposure [9]. The physical medium of communication is inherently insecure, so we need to design security-aware routing algorithms for MANETs. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection across the entire protocol stack [15].

II. RELATED WORK

B. Paramasivan*et al.* [16] have used the dynamic Bayesian signaling game to analyze the strategy profile for regular and malicious nodes in MANET for Routing. This game also revealed the best actions of individual strategies for each node. Perfect Bayesian equilibrium (PBE) provides a prominent solution for signaling games to solve incomplete information by combining strategies and payoff of players that constitute equilibrium. This game can also furnish secure and reliable communication that makes effective cooperation among nodes. Using PBE strategies of nodes are private information of regular and malicious nodes. Regular nodes should be cooperative during routing and update their payoff, while malicious nodes take sophisticated risks by evaluating their risk of being identified to decide when to decline. The cluster based routing protocol (CBRP) efficiently minimizes the flooding traffic during route discovery. It is suitable for a small network. In large networks, it provides more overlapping cluster structures which increase the routing overhead so in this Paper, they proposed

 ISBN: 978-93-86171-03-0

Ad hoc On demand Distance Vector (AODV) provides reliable data transmission in MANETs. In AODV, there was a requested source and destination sequence number, which is the essential reason for the routing loop problem and for privacy. This approach minimizes the utility of malicious nodes and it motivates better cooperation between nodes by using the reputation system. Regular nodes monitor continuously to evaluate their neighbors using belief updating systems of the Bayes rule. Even though the regular nodes are follow the PBE strategy to reduce the malicious node utilities for improving throughput in the entire networks. The performance analysis concludes that the PBE strategy was the best strategy for regular nodes to reduce malicious nodes utility. In this analysis, throughput and routing latency are about 91% respectively, than other protocols that improve the networks performance.

HaiyingShen*et al.* [17] have proposed a QoS-Oriented Distributed routing protocol (QOD) to enhance the QoS support capability of hybrid networks. Taking advantage of fewer transmission hops and any cast transmission features of the hybrid networks, QOD transforms the packet routing problem to a resource scheduling problem. QOD incorporates five algorithms:- QoS-guaranteed neighbor selection algorithm to meet the transmission delay requirement, Distributed packet scheduling algorithm to further reduce transmission delay, A mobility-based segment resizing algorithm that adaptively adjusts segment size according to node mobility in order to reduce transmission time, A traffic redundant elimination algorithm to increase the transmission throughput, A data redundancy elimination based transmission algorithm to eliminate the redundant data to further improve the transmission QoS. A number of queuing scheduling algorithms have proposed for Differentiated Service (DiffServ) to further minimize packet droppings and bandwidth consumption. Analytical results based on the random way-point model and the real human mobility model show that QOD can provide high QoS performance in terms of overhead, transmission delay, mobility-resilience and scalability. The traffic redundant elimination based transmission algorithm can further increase the transmission throughput. In the future they placed to evaluate the performance of QOD based on the real testbed.

Wei Liu *et al.* [18] have proposed a new routing protocol is Authenticated Anonymous Secure Routing (AASR), to satisfy the requirement and defend the attacks. More specifically, the route request packets are authenticated by a group signature to defend the potential active attacks without unveiling the node identities. The key encrypted onion routing with a route secret verification message, was designed to prevent intermediate nodes from inferring a real destination and also check whether AASR can achieve the anonymity goals by three anonymities namely identity anonymity, route anonymity, and location anonymity. To develop the anonymous protocols, a direct method is to anonymize the commonly used on-demand ad hoc routing protocols, such as AODV and ANODR. These results were used to compare the performance of AASR to that of ANODR, in a representative on-demand anonymous routing protocol. The results show that, it provides more throughput than ANODR under the packet-dropping attacks, although AASR experiences more cryptographic operation delay. Compared to ANODR, AASR provides higher throughput and lower packets loss ratio in different mobile scenarios in the presence of adversary attacks. It also provides better support for the secure communications that are sensitive to packet loss ratio. In future, they will improve AASR to reduce the packet delay. A possible method was to combine it with a trust based routing. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks.

 ISBN: 978-93-86171-03-0

Yang Qin *et al.* [19] have proposed a novel statistical traffic pattern discovery system (STARS). STARS aims to derive the source and destination probability distribution, i.e., the probability for each node to be a message source and destination, and the end-to-end link probability distribution, which is the probability for each pair of nodes to be an end-to-end communication pair. To achieve its goals, STARS includes two major steps one is to Construct point-to-point traffic matrices using the time-slicing technique, and then derive the end-to-end traffic matrix with a set of traffic filtering rules, and next one is Apply a heuristic approach to identify the actual source and destination nodes, and then correlate the source nodes with their corresponding destinations, which use the probability distributions produced by STARS are good indicators of the actual traffic patterns, i.e., actual sources, destinations, and end-to-end links. and which reveals most of the actual end-to end links by slightly sacrificing the false-positive rate. Specifically, in most cases, more than 80 percent of the actual end-to-end links are revealed (i.e., the false-negative rate was less than 0.2), while the false-positive rate was not more than 0.16.
Xu Li *et al.* [20] analyze the impact of network load on MAODV protocol, and proposed an optimized protocol MAODV-BB (Multicast Ad hoc On-demand Vector with Backup Branches), which improves robustness of the MAODV protocol by combining advantages of the tree structure and the mesh structure. The extension of MAODV protocol was to construct a multicast tree with backup branches from two aspects. One is the process of backup branches selection and addition, the other is the mechanism of multicast tree maintenance. It not only can update shorter tree branches but also construct a multicast tree with backup branches. As a tree based multicast routing protocol, MAODV-BB shows an excellent performance in light weight ad hoc networks. Mathematical analysis and this result both demonstrate that the MAODV-BB protocol improves the network performance over conventional MAODV in heavy load ad hoc networks. MAODV-BB's packet delivery was always maintained at a high level even when the network load is heavy also obvious to see that the delay of MAODV-BB is always lower than MAODV's.In MAODV-BB, the existence of backup branches reduces the frequency of tree reconstruction and ensures high packet delivery ratio in heavy load ad hoc networks.

III. MESH BASED MULTICAST ROUTING IN MOBILE ADHOC NETWORK

The group-oriented services are one of the primary application by Mobile Ad hoc Networks (MANETs) in recent years. To support such services, multicast routing is used. Thus, there is a need to design stable, reliable and secured multicast routing protocols for MANETs to ensure better packet delivery ratio, lower delays, reduce overheads and security mechanism handles misbehaviors and avoid various attacks. To overcome the above problems occurred in MANET, A mesh based multicast routing scheme will proposed in this work.The proposed multicast routing scheme (MRS) finds stable multicast path for multimedia transmission in MANET. A multicast mesh is constructed and the transmission route will discover in two stages. In first stage to maintain the quality of routing the physical parameter analysis will done by analyzing Transmit Energy, Distance, channel load, buffer occupancy, bandwidth and bit error rate (BER). Then in second stage the security of route will analyze by using route request, Erroneous Report Detection (ERD) scheme and route reply packets. One of the most stable paths with better quality for routing in the secure environment is discovered by employing ant colony optimization (ACO) technique. Then the Route maintenance will process to maintain the routing in case of any link failure happened. The proposed scheme is simulated over a large number of MANET nodes with

wide range of mobility and the performance is evaluated. The performance of the proposed scheme is compared with the existing routing protocols.

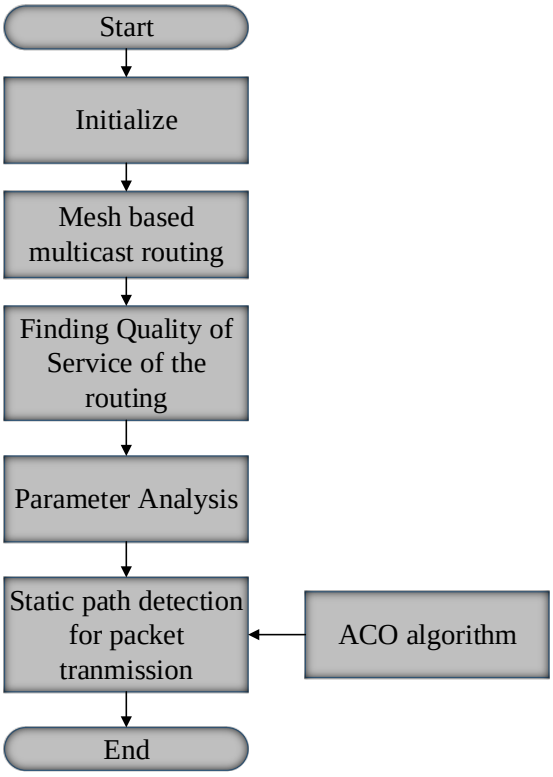

Fig.1 Proposed Flow Diagram

3.1. Mesh Based Multicast Routing

A multicast mesh is created with stable links when a source node needs to send data to receiver nodes. Mesh-based multicast protocols should have multiple paths between any source and destination pair. Request phase invokes a route discovery process to find routes to the multicast group. Different routes to the multicast group are setup during the reply phase. There are two types of nodes defined based on whether they are multicast group members or non-group members. Group members include all multicast sources, receivers and that of non-group members include intermediate nodes that help to create multicast routes from source to receivers. Non-group members help in forwarding the data packets. Both group members and non-group members help in recovery of failed links due to mobility of nodes and other interferences in route maintenance phase.

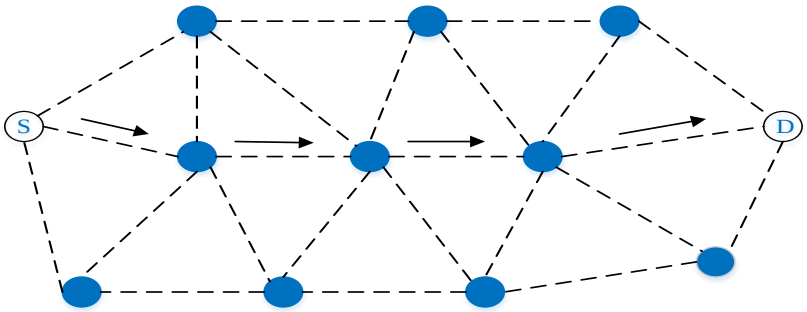

Fig.2. Mesh based multicast routing S- Source D-Destination

This protocol establishes multicast routes and group memberships which are added to the source on- demand. If the node realizes it is in the path to the source and a segment of the forwarding group then it set the FG flag and it broadcast its own Join Reply. The Join Reply causes by every forwarding group member unless it reaches multicast source through the shortest path. In the forwarding group this process builds or adding the routes from sources to receivers and constructs amesh. Forwarding group is set of nodes which are in charge of forwarding multicast packets and also it supports shortest paths between any member pairs. All nodes inside the multicast are members and also forwarding group nodes, forwarding group nodes forwards multicast data packets. If a multicast receiver is on the path between a multicast source and another receiver then it is said to be a forwarding group node. The mesh provides richer connectivity between multicast members as compared to multicast trees. Flooding redundancy among forwarding group helps to overcome node displacements and channel fading. Hence frequent reconfigurations are not required. Mesh-based multicast protocols may have multiple paths between any source and receiver pairs.

A. Route Request, Route Reply and Route Error Packets to create a multicast mesh and a stable route in a mesh from source to destination, various control packets such as route request, route reply and route error (RE) packets are used. In this section, we describe some of the fields of the control packets required for multicast mesh creation, stable path establishment and handling link failure situations. The fields of RR packet are as follows.

• Source address: It is the address of the node originating the packet.

• Multicast group address: It is the address of the multicast group.

• Sequence number: The sequence number assigned to every packet delivered by the source that uniquely identify the packet.

• Route request flag (RR flag): This flag is set for the duration of forward travel of RR packet from source to destination.

• Previous node address: It is the address of previous node that RR packet has visited during its forward movement. In the route request phase, a node receiving RR packet stores this address with multicast address in its MRIC as next hop node to send the packets to RR packet source. This field is updated after every movement to the next node until it reaches the receiver with multicast address.

• Power: This is the power at which a node has transmitted the packet to neighbor.

• Antenna gain: This is gain of antenna at the forwarding node to forward RR packet to its neighbor. RP packet format for multicast mesh creation is almost similar to RR packet with few changes in RR packet. They are as follows: RR flag value will be made 0, previous node address is removed, and source address is replaced by receiver address. RP packet moves on path traversed by RR packet by using MRIC and also updates the MRIC towards receiver /multicast address by adding one more next hop(node address from where RP packet has come) to multicast address. In general, next hop at every node to reach a source is set by using RR packets whereas RP packets set next hop at every node to reach receivers from the source. RE packet is generated when a node is unable to send the packets. Some of the fields of this packet are source address, destination address, sequence number, and route error flag (RE flag).Whenever a node identifies link failures, it generates RE packet with

 ISBN: 978-93-86171-03-0

route error flag set and sends the packet to either source or receiver. If link failure occurs in forward journey of a RR packet from source to multicast receiver, RE packet is sent to the source and if link failure occurs for reverse journey of the RP packet from receiver to the source, RE packet is sent to the multicast receiver.

3.2. Parameter Analysis

To maintain the quality of routing the physical parameter analysis will done by analyzing Transmit Energy, Distance, channel load, buffer occupancy, bandwidth and bit error rate (BER).

3.3. Transmit Energy

We assume that the data transmission between the nodes with power P the corresponding transmit energy is PT_s. Let the variable $E_{s,t}$ be the minimal energy required to transmit one data packet from the source node at (0, 0) to the destination node at (D, 0), and where *Z* is in decibels over a path with exactly t hops

$$G_t = \frac{E_{st}}{E_{hop}} \qquad \rightarrow(1)$$

The normalized minimal transmit energy over a single hop is

$$F_{G1}(g) = P\{E_{s,1} \le g_{hop}\} = P\{10^{-Z/10} \le g\} \qquad \rightarrow(2)$$

$$= P\left(Z \ge -\frac{10}{in\,10} In\, g\right) = 1 - Q\left(\frac{In\, g}{h\sigma}\right) \qquad \rightarrow(3)$$

Distance

The weight function is the parameter P_{ij} that allows nodes to select the best path. This parameter is defined by:

$$P_{ij} = \alpha * \frac{D_{ij}}{T_{r_i}} + \beta * \frac{E_{ij}}{T_{r_j}} \qquad \rightarrow(4)$$

Where

α and β are the weights satisfied the nodes

D_{ij} is the distance between node i and node j.

T_{r_i} transmission range of node i

T_{r_j} transmission range of node j

E_{ij} is the maximum energy between node i and node j.

Channel load:

This channel load focuses on analyzing the variation of channel load measurements for the nodes. The channel load functionality was implemented by several scenarios were configured for testing. This variation leads us and a usefulness of a single channel load measurement. This channel load measurement can significantly improve the network performance both in network latency and throughput.

Bandwidth:

 ISBN: 978-93-86171-03-0

Bandwidth is the rate of data transfer, bit rate or throughput, measured in bits per second. The amount of data that can be carried from one node to another in a given time period is known as bandwidth in MANET. It measures how much data can be sent over a specific connection in a given amount of time. Now days modern networks typically have speeds measured in the millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second, or Gbps).However, this estimate indicates how much bandwidth an application or device in the wireless network can expect when sending or receiving network traffic. This bandwidth variation as on low or high frequency.

Formula for the lower cutoff frequency

$$f_1 = f_0\left(\sqrt{1+\frac{1}{4Q^2}}-\frac{1}{2Q}\right) \qquad \rightarrow(5)$$

Formula for the upper cutoff frequency

$$f_2 = f_0\left(\sqrt{1+\frac{1}{4Q^2}}-\frac{1}{2Q}\right) \qquad \rightarrow(6)$$

Formula for the Q factor

$$Q=\frac{f_0}{f_2-f_1} \qquad \rightarrow(7)$$

Formula for the bandwidth

$$f_2-f_1=\frac{f_0}{Q} \qquad \rightarrow(8)$$

Where $f_0$is center frequency

f_1 is low cutoff frequency and

f_2 is high cut of frequency and

Q is the Quality factor

Bit Error Rate (BER)

Considering a multi hop route between source and destination, the BER at the end of a link between two neighboring nodes, denoted as BER link, depends on the signal-to-noise ratio (SNR) at the receiving node. Finally itis possible to show that the BER at the end of the n_h -th linkof the multi-hop route, denoted by BER^{n_k} , can be expressed as

$$BER^{n_h} \cong 1-\prod_{i=1}^{n_h}[1-BER_{link}(i)] \qquad \rightarrow(9)$$

Ant Colony Optimization:

The ant colony optimization (ACO) meta-heuristic is a generic problem representation and it is based on the behavior of ants. It adopts real ant's foraging behavior. Ants initially start random walk when multiple paths exist between nests to food. They lay a chemical substance called pheromone during their food searching trip as

 ISBN: 978-93-86171-03-0

well as their return trip to the nest. Pheromone serves as route mark, which the ants follow. Newer ants will take that path which has higher pheromone concentration and also the pheromone concentration of that path will increase by the time. This is an autocatalytic effect and this helps the solution to be emerging quickly. Some properties characterizes ACO instances for routing problems. In a network where the topology changes dynamically, highly adaptive routing is necessary. Also, in the network without any centralized control, due to node mobility the link can be broken any time and the communication may be lost. If multiple paths exist between source and the destination, one path lost cannot effect the communication, because anyone of the existing paths can be used for routing. ACO provides both the traffic-adaptive and the multipath routing.

b. It is necessary to choose a path for routing which satisfies both the required constraints for routing and for this, some previous information are needed and based on the newer and the previous information the path is chosen. In ACO, both the passive and active information are gathered and monitored.

c. ACO uses the stochastic components for routing.

d. ACO does not allow local search estimates to have global impact for the required solution. In ACO no routing information has to transmit to neighbor or all the nodes.

e. ACO does not set paths like other greedy shortest path schemes, at the time of path set up it also taken care of load balancing. So, it taken care of the link quality also.

f. Another important aspect is parameter setting. It is done by ACO in less sensitive way.

Figure.2 illustrates the behavior of ants. A set of ants moves along a straight line from their nests to a food source D. At a given moment, an obstacle is put across this way so that side. Now, the ants have to decide which direction they will take: either A or B. The first ones will choose a random direction and will deposit pheromone along their way. The ants taking the way SBD, will arrive at the end of the obstacle (depositing more pheromone on their way) before those that take the way SAD. So, pheromone intensity of route SBD becomes greater than that of route SAD. So, the ants choose the path SBD. The ants will then find the shortest way between their nest and the food source. The motion direction of the ant is given in Figure.

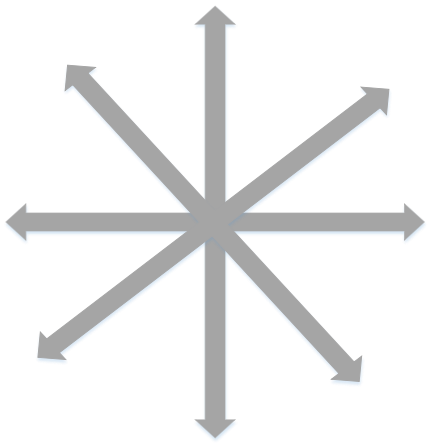

Fig.3 Motion Direction of an Ant

In most cases, an artificial ant will deposit a quantity of pheromone represented by $\Delta\tau_{i,j}$ only after completing their route and not in an incremental way during their advancement. This quantity of pheromone is a function of the found route quality. Pheromone is a volatile substance. An ant changes the amount of pheromone on the path (i, j)when moving from node i to node j as follows:

$$\tau_{i,j} = \sigma.\tau_{i,j} + \Delta\tau_{i,j} \qquad \rightarrow(10)$$

Where $0 < \rho < 1$and ρ is the pheromone evaporation factor which avoids infinite increment of pheromone which may leads to stagnation of the route. At one point i, an ant chooses the point j (i.e. to follow the path (i, j)) according to the following probability:

$$P_{i,j} = \frac{(\tau_{ij})^{\alpha}.(\eta_{ij})^{\beta}}{\sum_{i,k\in C}(\tau_{ik})^{\alpha}.(\eta_{ik})^{\beta}} \qquad \rightarrow(11)$$

Where $\tau_{i,j}$: is the pheromone intensity on path $(i.j)$.

$\eta_{i,j}$: is the ant's visibility field on path (i, j)(an ant assumes that there is food at the end of this path).

α And β : are the parameters which control the relative importance of the pheromone intensity compared to ant's visibility field. C: represents the set of possible paths starting from point $(i(i,k))$is a path of C).Like real pheromone the artificial pheromone decreases over time for fast convergence of pheromone on the edges. This happen in ACO according to the following formula:

$$\tau_{i,j} = (1-q).\tau_{i,j} \qquad q \in (0,1) \qquad \rightarrow(12)$$

Calculating Stability of A Route:

Each node in the network estimates the stability of its one-hop neighbors. We define stability based on the number of HELLO packets received by a node. To explain this more clearly, let us assume that nodes Band C are the one hop neighbors of A. If in a particular interval, A receives x HELLO packets from Band y packets from C, and x < y then from the view point of A, C is more stable than B. In addition, each node also takes into account the stability history of its neighbor when estimating its stability. Formally, let every node calculate the number of HELLO packets received from its neighbors periodically for every WMESH STABILITY INTERVAL seconds. We define Current Stability as the percentage of HELLO packets received with respect to the expected number of HELLO packets in the last WMESH STABILITY INTERVAL. Let α be the weight factor for calculation of a neighbor's stability. Stability of a neighbor is calculated as follows:

Stability = (α) Current Stability+ (1−α) Stability →(13)

Every node maintains the Stability of its neighbors in its NEIGHBOR TABLE. To calculate, the stability of the route, control packets are piggybacked with stability information which are updated by intermediate nodes along the route. To explain further, let source S needs to find a route to destination D. During the route discovery phase, S initializes Stability to 0 and piggybacks this information on the RREQ packets. When a node I receives a RREQ packet from previous hop P, it adds the Stability of P to the stability field of the RREQ packet. Thus Reverse Route Stability (RRS) is the sum of stabilities of all the nodes along the path. Analogously, we

calculate the Forward Route Stability (RRS) by piggy backing stability info on RREP packets and updating it along the route. To negate the effect of higher stabilities for longer routes, we take the hop count of the route into account. Formally, Route Stability is calculated as follows:

$$Route\ Stability = (FRS + RRS)\ 2 \times Hop\ Count \quad \rightarrow (14)$$

This is the formula for finding the stability of the route using ACO algorithm. Performance of the proposed scheme is compared with existing multicast routing protocols. It is observed that the proposed scheme produces better packet delivery ratio, reduced packet delay, reduced overheads (such as control, memory, computation, and message overheads) and provide security against vulnerabilities and attacks with low resource consumption.

IV. RESULTS AND COMPARSION

In this section we have presented a comparison between existing routing protocols with MMR. We illustrate the results of comparison in terms of dynamic source routing and the results for MMR in MANET. The parameters like throughput, transmit energy, channel load, buffer occupancy, transmit distance and bit error rate are improved as previously noted. The MMR protocol embeds the complete sequence of the routing path in data packets, which increases the throughput in MANET. This performances is refers to the ratio of the number of packets successfully transferred by the network to that of the packets injected into the network. We measure throughput by the total number of packets received at the destination per unit time. We have compared the throughput of MMR with dynamic source routing in Table.1. We found that the throughput of MMR is highest among the protocols due to the availability of automatic alternate node paths and higher bandwidth than other protocols used in MANET. Following formula was used to calculate the throughput.

$$Throughput = \frac{No\ of\ \ packets\ sent}{Total\ time\ taken}$$

Using our technique mesh based multicast routing (MMR) protocol the quality of service and security has been improved for the smaller and larger networks, respectively.

No of nodes	DSR			MMR		
	BER	QoS	Throughput	BER	QoS	Throughput
20	0.798	7	9021	0.967	26	17251
40	0.808	9	10863	0.97	28	20621
60	0.818	12	11311	0.97	31	20909
80	0.819	13	12064	0.973	38	21554
100	0.819	14	12205	0.974	44	23819

Table .1. Comparison Table for BER, Qos and Throughput of DSR and MMR.

 ISBN: 978-93-86171-03-0

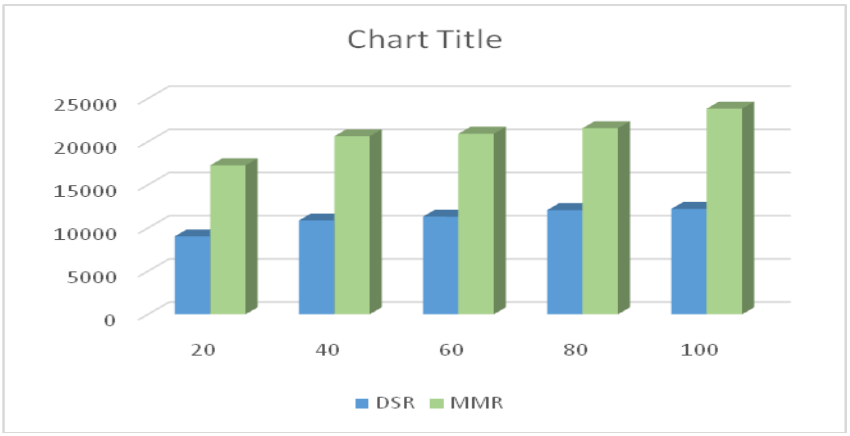

Figure .6. Chart of Bit error Rate

Figure .6. shows that the bit error rate of network using DSR and our proposed MMR. The calculation of above graph of bit error rate is based on the received and generated packets. Observe that MMR protocol maintenance the bit error rate while compared to the dynamic source routing.

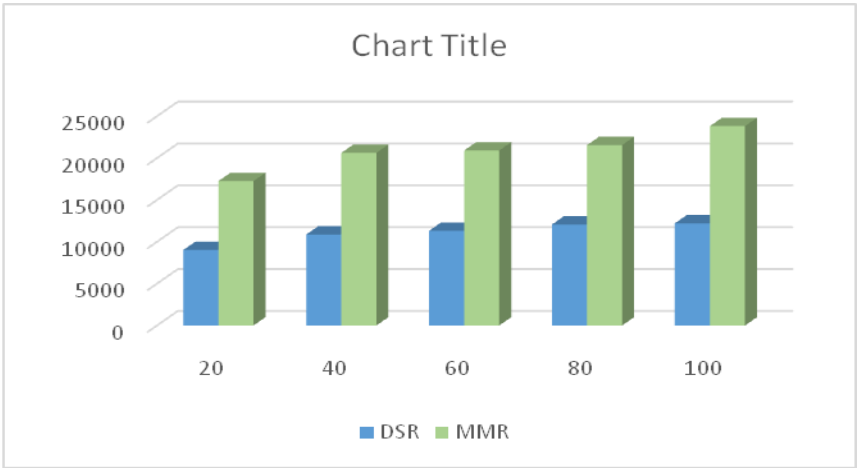

Figure .7. Chart of Qos

Figure .7. shows that quality of service the of network using DSR and our proposed MMR. Observe that MMR protocol maintenance the low delay while compared to the dynamic source routing.

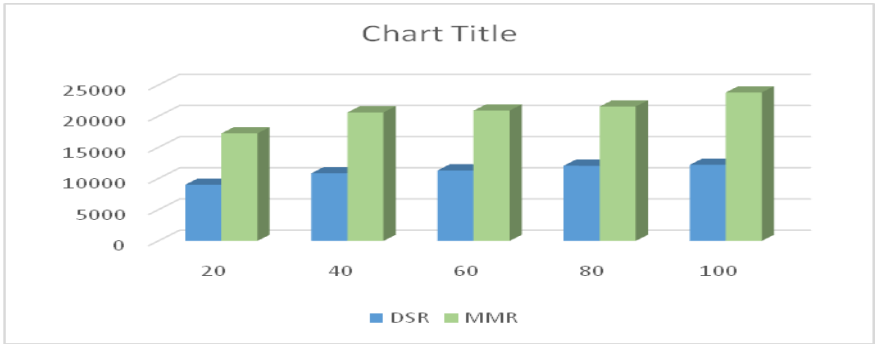

Figure .8. Chart of Throughput

Figure .8. shows that the throughput of network using DSR and our proposed MMR. The proposed MMR protocol maintenance the high throughput while compared to the dynamic source routing.

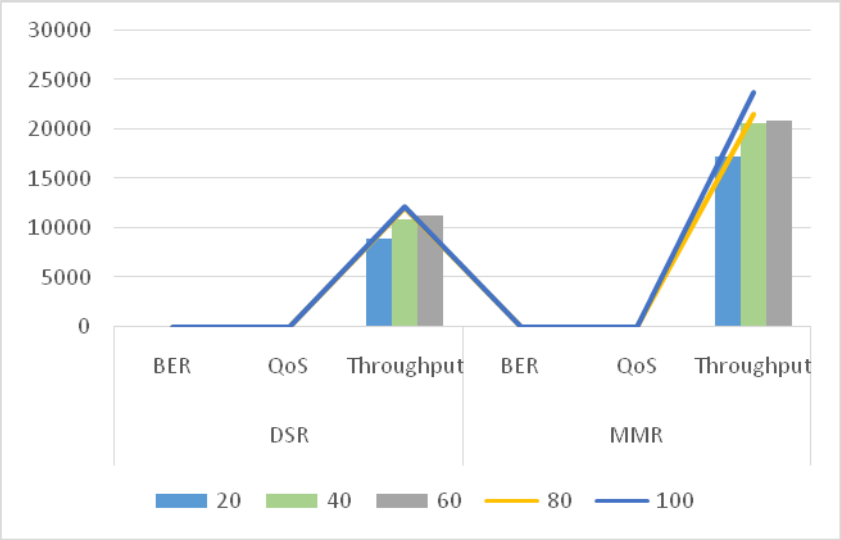

Figure. 9. Overall Comparison Chart

The overall comparison diagram of DSR and MMR has been shown in figure.9. Hence our proposed method shows high performance among all other existing methods.

V. CONCLUSION

In this paper, a novel mesh based multicast routing scheme is presented to enhance the quality of service and security of the routes in MANET. Firstly, the paths are found to be connected between the source and destination pair. The main purpose of QoS aware routing is to find a feasible path from source to destination which will satisfy two or more end to end QoS constrains. The ant colony optimization algorithm is used to find the shortest and best path for routing. The proposed scheme is compared to the existing routing protocols. The result shows that our proposed technique enhanced the quality of routing and had find the best path by the optimization algorithm.

REFERENCE

[1] M. Scott Corson, Joseph P. Macker, and Gregory H. Cirincione, "Internet-based mobile ad hoc networking", Internet Computing, IEEE Vol.3, no.4, pp.63-70, August 1999.

[2] Devesh Kumar Pal and Dr. Pallavi Murghai Goel, "Survey on Security Issues in Mobile Ad Hoc Networks", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5, No.3, pp.3732-3735, 2014.

[3] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey", Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County, pp.1-23, 2008.

[4] Hao Yang, HaiyunLuo, Fan Ye, Songwu Lu and Lixia Zhang, "Security In Mobile Ad Hoc Networks: Challenges And Solutions", Wireless Communications, IEEE Vol.11, No.1, pp. 38-47, February 2004.

[5] NishuGarg and R.P.Mahapatra, "MANET Security Issues", IJCSNS International Journal of Computer Science and Network Security, Vol.9, No.8, pp. 241-246, August 2009.

[6] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", Communications Magazine, IEEE Vol.40, No.10, pp. 70-75, October 2002.

[7] Mohammed Saghir, Tat-Chee Wan and Rahmat Budiarto, "QoS Multicast Routing Based on Bandwidth Estimation in Mobile Ad Hoc Networks", In Proceedings of the Int. Conf. on Computer and Communication Engineering, ICCCE, Vol. 6, No. I, 9-11 May 2006.

[8] Agha K and Pujolle G., "QoS for Ad hoc networking based on multiple metrics: bandwidth and delay." In Proceedings of the 5th IEEE International Conference on Mobile and Wireless Communications Networks, pp. 15 -18, 2003.

[9] PrasantMohapatra, Jian Li, and Chao Gui, "QoS In Mobile Ad Hoc Networks", IEEE Wireless Communications , Vol.10, No.3, pp. 44-53, June 2003.

[10] Chunxue Wu, Fengna Zhang and Hongming Yang, "A Novel QoS Multipath Path Routing in MANET", International Journal of Digital Content Technology and its Applications, Vol. 4, No. 3, pp.132-136, June 2010.

[11] Jared Cordasco and Susanne Wetzel, "Cryptographic Versus Trust-based Methods for MANET Routing Security", Electronic Notes in Theoretical Computer Science, Vol. 197, No. 2 pp.131-140, 2008.

[12] Akshai Aggarwal, Savita Gandhi and Nirbhay Chaubey, "Performance Analysis Of Aodv, Dsdv And Dsr In Manets", International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, pp. 167-177, November 2011.

[13] Shengming Jiang, Yaoda Liu, Yuming Jiang and Qinghe Yin, "Provisioning of Adaptability to Variable Topologies for Routing Schemes in MANETs", IEEE Journal on Selected Areas In Communications, Vol. 22, No. 7, pp. 1347-1356, 2004.

[14] Azzedine Boukerchea,b, Khalil El-Khatiba, Li Xua and Larry Korbab, "An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks", Computer Communications, Vol. 28, No.10, pp. 1193-1203, 2005.

[15] Parul Tomar, Prof. P.K. Suri and Dr. M. K. Soni, "A Comparative Study for Secure Routing in MANET", International Journal of Computer Applications, Vol.4, No.5, pp. 17-22, July 2010.

[16] B. Paramasivan, M.J.V. Prakash, and M. Kaliappan, "Development of a secure routing protocol using game theory model in mobile ad hoc networks", IEEE Journal of Communications and Networks, Vol. 17, No. 1, pp. 75-83, 2015.

[17] Haiying Shen and Ze Li, "A QoS-Oriented Distributed Routing Protocol for Hybrid Wireless Networks,", IEEE Transactions on Mobile Computing, Vol. 13, No. 3, pp.693-708, 2014.

[18] Wei Liu and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, Vol. 63, No. 9, pp.4585-4593, 2014

[19] Yang Qin, Dijiang Huang and Bing Li, "STARS: A Statistical Traffic Pattern Discovery System for MANETs", IEEE Transactions on Dependable and Secure Computing, Vol. 11, No. 2, pp.181-192, 2014

[20] Xu Li, Tianjiao Liu, Ying Liu and Yan Tang, "Optimized multicast routing algorithm based on tree structure in MANETs", China Communications, Vol. 11, No. 2, pp.90-99, 2014.