ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

OPTIMIZED MULTICAST ROUTING SCHEME FOR MOBILE AD HOC NETWORKS

[1]DR.A.RAJARAM, [2]S.GOPINATH,

[1]Associate Professor, Department of Electronics and Communication Engineering,
Karpagam College of Engineering, Coimbatore, India.
[2]Research Scholar, Anna University, Chennai, India
E-mail: [1]gct143@gmail.com , [2]gopi.vasudev@gmail.com

ABSTRACT

Mobile Ad hoc Network is the indivisible part of wireless network. In the past few years, the popularity of MANET grows unlimitedly. Due to the presence of mobility and infrastructure less topology, the vulnerability of ad hoc networks is introduced unconditionally. So the failures of link, path and node may occur which leads to lack of communication between the users. Sometimes the malicious attackers arise to make more damage to network connectivity and produce false information among the mobile nodes. To overcome this issue, several approaches are developed to make more efficient routing. But they have not focused on failures of node, link and path as well as malicious activities at a time. We proposed Optimized Multicast Routing Scheme (OMRS) to attain balance between the above said issues. In first phase of this scheme, we develop the detection and avoidance of malicious attacks is implemented with the predetermined trust value of node characteristics. We have also introduced the characteristics of malicious attacks in linear network systems. In second phase, stability ratio of link, path and node is determined to maintain threshold value which ensures the resilience to the path failures. By implementing these solutions, we have achieved better stability and node connectivity towards the ultimate goal of multicast routing scheme. We implement our proposed scheme within Network Simulator (NS2.34) tool environment. By using the extensive simulation results, the proposed scheme achieves better delivery ratio, detection ratio, probability of failure occurrence and less communication overhead, end to end delay than the ODMRP, BDP.

Keywords: *Multicast, Stability Ratio, Malicious Attackers, Detection Ratio, Delivery Ratio, Communication Overhead, End To End Delay, Threshold Value, Node Familiarity And Node Proposal.*

1. INTRODUCTION

In recent years, thanks to the propagation of wireless devices, the usage of the mobile networks is raising very fast. In particular, the recent studies and research are focussing on Mobile Ad hoc Networks (MANETs) [1]. A MANET is a self configuring and Infrastructure less networks, in which each and every node can act as a router. The performance of mobile ad hoc network depends on the routing scheme deployed and some of the traditional routing protocols do not work properly. In this type of dynamic network, nodes are moving randomly and the radio propagation conditions change rapidly.

In MANET, multicast routing protocols deliver the data from source to many destinations organized in a multicast group community. A major issue and challenge in a network is to ensure the heftiness to path failures and resilience to the malicious attackers. Multicasting can efficiently support a wide variety of applications that are characterized by a close degree of collaboration. Due to the presence of the mobile nodes, the path, link and node failures occurs or sometimes the malicious intruders may arise in the network to damage whole network connectivity. To ensure the robustness and resilience to these failures and attackers, there is a need of optimized multicast routing protocol in MANET.

In this work, we focus on the detection of malicious attackers and providing the astonishing stability to the link, path and node. For that we propose to introduce trust parameters like node familiarity and node proposal. If we follow the trustable multicast routing scheme, the data integrity will be high. As discussed in [2], the objectives and potential stability metrics are enumerated to find the stable routes.

- **Minimize the number of unstable link**
  The main objective is to reduce the number of unstable links.
- **Maximize the expected residual lifetime**
  The residual path lifetime is equal to the lifetime of its more critical link. The expected residual lifetime of a link can be calculated from collected statistical data.
- **Maximize the persistence probability**
  The estimation of the persistence probability of a link is proposed based on statistical data. This metric directly aims at minimizing the number of interruptions during a certain time span.
- **Maximize a residual lifetime quantile**
  The minimum residual lifetime that a path will reach with a given probability can be calculated from the path persistence probabilities.
- **Avoid Instable Links**
  The weakest link is deployed. Mostly, the path avoiding the instable links is wanted.

In MANET, uncooperative node is malicious node. The nodes belonging to the first category are either faulty and therefore cannot follow a protocol, or are intentionally malicious and try to attack the system. Malicious node causes packet dropping, false routing and etc. Effects of malicious nodes are given below:

- Malicious node reduces the network connectivity in MANETs.
- The result is defragmented networks, isolated nodes, and drastically reduced network performance.
- No intention for energy-saving.
- Launch all kinds of denial-of-service (DoS) attacks by replaying, reordering or/and dropping packets from time to time, and even by sending fake routing messages.

2. RELATED WORK

The mesh based routing scheme [3] is proposed in this work which is used to find the stable multicast path from the source to destination node. This path is built with the help of multicast route information cache and link stability database. Stable forwarding nodes with high stability of link connectivity had been chosen for computing the stable path. The proposed scheme consists of mesh creation, finding stable routes and mesh maintenance while handling link failures. Here better quality of link as well as possibility of reducing link failures also provided.

In the author Al-Sakib Pathan et.al [4], they mainly focused on robustness of the network. For that, it has been introduced that Neighbor Aware Multicast Routing Protocol to achieve reliable routing and robustness. The proposed protocol is a tree based protocol where it is constructed and maintained using traditional RREQ and RREP messages. It uses neighbor information of two hops away for both transmission and reception of the packets. The scheme called dominant pruning is used to flood the packets and create the route. The protocol also ensures robustness in the network by employing the Secondary Forwarder List (SFL) method. Totally in this work, it totally attains the balance between delivery of packets and robustness.

M. Rajendiran and S.K. Srivatsa [5] proposed link stability based on demand multicast routing protocol. This protocol finds the stable route with minimum delay and overhead. Here, multicast mesh of alternate routes between every source-destination pair is established in mesh creation segment. Link stability is also established by choosing link quality among its neighbors. Additionally link failure conditions are notified to the source node with bit error ratio to start the route detection of new path establishments. Here the simulation is performed in terms of control overhead and throughput.

In this work [6], the novel attacks are identified against high throughput multicast routing protocols in wireless mesh networks. The aggressive path selection procedure is found to maximize the throughput and attack effectiveness. The proposed mechanism is integrated with measurement based detection and accusation based reaction techniques. With the help of these schemes, manipulation attacks are detected which are damaging the network. The defense mechanism also copes with transient network variations and malicious attempts. The main goal of this proposed multicast routing is to achieve high throughput.

A MAC layer level clogging detection is projected in this paper [7]. The clogging system is integrated with two-step cross layer clogging control routing topology. Generally, the packet drops mainly occurs due to link crash and clogging. So it is explored that a cross layered model of clogging recognition an control mechanism that include energy efficient clogging detection, Multicast Group Level Clogging Evaluation and Handling Algorithm [MGLCEH] and Multicast Group Level Load Balancing Algorithm [MGLLBA], which is a hierarchical cross layered base clogging recognition and avoidance model in short can refer as Qos Optimization by cross layered clogging handling

(MGLCEH). The scheme achieved the better store utilization, congestion control and energy efficiency in clogging detection.

To maintain the efficiency of multicast routing, a new protocol called KHIP [8] (Keyed Hierarchical Multicast Routing Protocol) is developed. It also provides the authentication services and secure routing. It adds an authentication service that issues certificates to entities who are allowed access and who authenticate themselves with a known public key. These certificates are included in signed control messages to prove that the sender has the authority to alter the tree. The tree itself is divided into sub-branches, and messages within each sub-branch also carry nonces to prevent forgery or replay attacks that could build a branch of the tree to an unauthorized router. Each sub-branch can also use a shared key for data transmission, thus obviating the need for a single key shared across the entire tree. The headers of data packets are re-processed for transmission between sub-branches. The proposed KHIP attains the needs of security while providing the delivery of data across many receivers.

Sreedhar and Damodaram [9] proposed a new multicast routing protocol for MANET to handle congestion and improve the Quality of Service (QoS). The protocol makes use of reduced resource utilization and to adapt a mesh or tree structure with enhanced resilience against mobility. It also utilizes the group level multicasting to reduce the routing overhead, improve route efficiency and reduce data transmissions. In this regard, it first tries to control at hop level outflow load balancing , if failed then attempts to control by group level outflow load balancing, if still not succeed then finally attempts to control the congestion with outflow load balancing between groups.

A route driven gossip protocol is developed by Jun Luo et.al [10], to meet a more practical specification of probabilistic reliability in ad hoc networks. The main idea of this protocol is to explore the feasibility of such a probabilistic approach along with a prediction of its performance in a highly dynamic setting, useful for many critical applications such as security services like distributed key management services, or certificate distribution and revocation for self-organ ized public-key infrastructures.

By concerning the benefits of using multiple paths, Jamal et.al [11] proposed the Mobile Multipath Multicast Routing Protocol (M3RP) provide multiple routes among the multicast group members. Besides the sequence number of each packet and the source ID, M3RP consider the number of hops between the source and destination in route construction. Group membership and multicast routes are established and updated by the source on demand. This technique makes the protocol robust to mobility and increases the packet delivery ratio. Demand multicast route construction and membership maintenance, and it is based on mesh forwarding. M3RP obtain multiple multicast routes, which provides alternate paths for packets to travel in the event that some of the paths become disconnected. Packets travel down each one of the routes in the set of multiple routes obtained increasing the likelihood that a receiver receives the packet sent from the sender node as the topology of the network changes. M3RP attempts to ensure that the reliability due to redundancy is high, yet the amount of extra network traffic is not overly burdensome.

A QoS based Clustering technique is proposed for multicast security in MANET by Vennila et.al [12]. Here the author justify the node with maximum available bandwidth and residual energy. This node is elected as the Cluster Heads (CH) as well as multicast group leaders in cluster region. Each CH computes trust value based on success ratio and routing control packets. In this scheme several advantages have been listed out i.e. Since nodes trust values are evaluated only by the cluster head, the delay and overhead is less and Only trusted nodes are admitted in the multicast group, thus restricting outside malicious nodes etc.

The author in [13], analyzed that impact of mobility pattern on multicast routing performance of MANET. It is observed that the strengths and weaknesses of the individual multicast routing protocols, the mobility patterns does also have influence on the performance of the routing protocols The connectivity of the mobile nodes, route setup and repair time are the major factors that affect protocol performance. Several other parameters such as traffic patterns, node density and initial placement pattern of nodes may affect the routing performance of the network.

The author developed [14] a persistent Range Detection Multicast Protocol (RDMP) for MANET. Here, leadership track node is the in-charge of exchanging control messages for efficient group membership management. The data packets and control packets are transmitted along efficient end-to end tree-like paths without the need of explicitly creating and maintaining a tree structure. A special exclusive hand over mechanism is integrated to elect the best group leader for multicasting. The proposed protocol is a table driven reactive multicasting protocol, a member joining the group is carried out only on demand request made by the participant node. Group Leader is taken here to handover the leadership to the other member by means of voluntary handover mechanism.

Rajashekhar and Sunilkumar [15] proposed Bandwidth Delay Product (BDP) based multicast routing scheme with the help of ring mesh backbone. Reliable node pairs are computed based on mobility, remaining battery power and differential signal strength. The node pairs are used to compute BDP between them. BDP of a reliability pair is assessed using available bandwidth and delay experienced by a packet between them. Backbone ring mesh is constructed using reliable pair nodes and convex hull algorithm. Reliable ring mesh is constructed at an arbitrary distance from the centroid of the MANET area. Multicast paths are created by discovering a path from source to each destination of the group with concatenated set of reliability pairs that satisfy the BDP requirement. In case of node mobility and failures occurs, the ring mesh can be able to maintain high BDP on ring links and also it can be recovered.

To withstand the insider attacks from colluding adversaries, the author proposed [16] novel secure multicast routing protocol. The protocol also ensures data delivery to the group of multicast group members even in the presence of Byzantine attacks. Here the byzantine attacks are black hole attack, worm hole attack, flood rush attacks are avoided by using the proposed scheme. It also identifies and avoids adversarial links based on a reliability metric associated with each link and capturing adversarial behavior. Our aim in this paper is to arrive at a multicast protocol which strikes a balance between defending against Malicious Nodes and path, link and node failures.

3. OVERVIEW OF OPTIMIZED MULTICAST ROUTING SCHEME

The optimized multicast routing scheme consists of two phases i.e. detection of malicious nodes and handling link failure and path failure by choosing the stability ratio of link and path. In the first phase of the scheme, the malicious node is detected by means of trust threshold which contains the values of node familiarity and node proposal. In second phase of the scheme, estimation of stability ratio for link, node and path is proposed.

3.1 Optimized Multicast Backbone Construction

Optimized multicast route acts as a backbone for multicast routing in MANET. In order to create an optimized multicast backbone, it is needed to have a complete topological knowledge. The MANET boundary area is determined by using the jarvi's convex hull algorithm [17] from computational complexity. If the boundary is known, the area and centroid can be determined which helps in the construction of optimized multicast backbone. In fig.1, the convex hull creation is illustrated. The angles P, Q correspond to two extreme neighbors on negative x-axis. An angle is supposed to calculate at node *A*(u_0, v_0) that is assumed to be a starting node to initiate convex hull formation on all the boundary nodes. The angle at A(u_0, v_0) selects a neighbor node *B*(u_1, v_1) as it makes minimum angle *P* rather than neighbor node *C*(u_2, v_2) which makes an angle *Q* with the condition that $P < Q$ once if traced in clockwise direction. This procedure is repeated at node *B* and its next boundary node (tracing all the boundary nodes) till it reaches to the original node *A*(u_0, v_0) through opposite direction. Thus, the convex hull is created. Once the convex hull is created, optimized multicast back bone is constructed that serves as a backbone for multicast routing.

The creation of optimized multicast backbone is shown in fig.2. Optimized multicast creation is initiated based on two assumptions, (i) establishing a trustable loop that should be located at 4/6 th of an average radius from the centroid so as to be reached by all the nodes with least hop distance whether they are either towards the centroid or towards the boundary nodes on the convex hull, (ii) this loop is established by connecting links formed by trustable factors of node familiarity, node proposal, link stability and path stability.

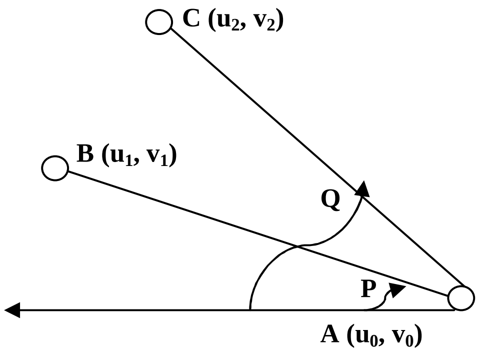

Fig.1. Accepted Angle To Create Convex Hull

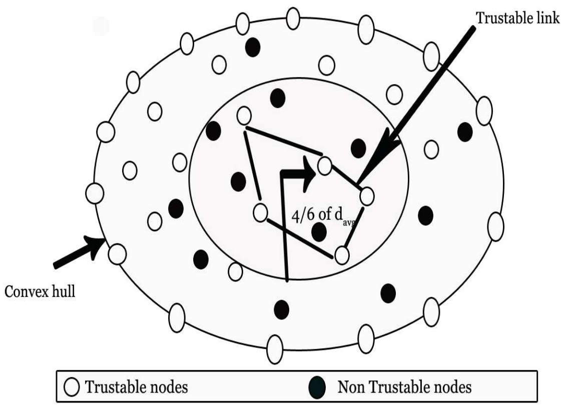

Fig.2. Optimized Multicast Backbone Creation

Average radius is obtained by,

$$d_{averradius} = \frac{1}{N}\sum_{i=1}^{N}\sqrt{(u_i - u_i^{'})^2 + (v_j - v_j^{'})^2} \quad (1)$$

Where N = number of nodes and u_i and v_i are the convex polynomial created by nodes. The optimized multicast routing is constructed at an arbitrary distance $d_{averradius}$ measured from centroid of the convex hull. It is given by $d_{avg} = \frac{4}{6} \times d_{averradius}$. All the nodes at d_{avg} are joined together to form an optimized backbone.

3.2 Detection of Misbehaviors in MANET

The main goal of our routing scheme is to identify and isolate the misbehaviors including like link failure, node failure and malicious node. In case of any malfunctions occurs in the network, our scheme efficiently detects the misbehavior in the given periodical time. Before finding the presence of malicious node in the network, we need to characterize the malicious behaviors. For a linear system and non empty set cases $U_1 \in U$, for an input b_{U1} (t) is unidentifiable if and only if,

$$F_j V^{t+1} \overline{y} = \sum_{\sigma=0}^{t} F_j V^{t-\sigma}(D_{U1} b_{U1}(\sigma) - D_{U2} b_{U2}(\sigma)) \quad (2)$$

for all $t \in \mathbb{N}$, and for some b_{U2} (t), with $U_1 \in U$, $U_1 \neq U_2$ *and* $\overline{y} \in \Re^n$. If the same holds with b_{U2} (t) is actually undetectable. F_j is function of presence of malicious behaviors.

The detection of the misbehaviors consists of two phases like

i) Identification of the malicious node.
ii) Isolation of the malicious activities.

3.2.1 Identification of Malicious Node

Due to the presence of the malicious node, the whole network is heavily damaged and network connectivity is unavailable. To avoid such cases, the each node carries trust counter value. This value is calculated from the node proposal, node familiarity which is stored in the neighbor node routing table. The status of this above information is being sent to source node.

In Route discovery phase, the source node sends S_RREQ message to group of destination nodes via intermediate nodes. Once the information received via multicast routing $R_1, R_2, \ldots R_N$, the destination nodes send back D_RREP($D_1, D_2 \ldots D_N$). If the malicious node presents in the any route, the message D_RREP cannot be reached the source node. If successful, the message is delivered to the source node. Each node carries the sequence number in its packet which is used to identify the authorized node or not.

For an example in R_1 route, source node sends S_RREQ message to destination node D_1 via intermediate nodes like $IN_1, IN_2, \ldots IN_n$ where IN_1 is Neighbor node 1 in the R_1 route. The same procedure follows for $IN_2 \ldots IN_n$. Each neighbor nodes carries node trust counter value (T_{CV}) which is derived as

$$T_{cv} = MN_f + MN_p \quad (3)$$

Where,
MN_F = Mobility of Node familiarity
MN_P = Mobility of Node Proposal

In Mobile Node familiarity, consider two nodes like S and D. To determine better relationship between the two nodes is to identify how much incoming and outgoing packet can be sent or received. In such cases, the node familiarity provides well connectivity between the nodes. This relationship is extended towards the whole network. Mobility of Node familiarity is given as,

$$MN_f = (1 - P^*_{E,F}) \times (1 - P^*_{F,E}) \quad (3)$$

$P^*_{E,F}$ is probability of packet sent from node E to F.

$P^*_{F,E}$ is probability of packet sent from node F to E.

In Mobile Node proposal case, the recommendations about the neighbor nodes are collected. This recommendation is sent towards the source node. Once the source node receives recommendations, it identifies trustable node. One of the main parameter to identify the malicious node is node proposal [19]. Here we take nodes like

E, F and G. The Mobility of node proposal is given by MN_P

$$MN_P = \frac{\sum_{v \in \gamma} V|E \rightarrow F| * V|G \rightarrow F|}{V|E \rightarrow G|} \qquad (4)$$

γ is a group of recommenders.

$V|E \rightarrow G|$ is trust vector of node E to G.

$V|G \rightarrow F|$ is trust vector of node G to F.

Source node maintains trust threshold count vector value to find the presence of any malicious node in the network. If any trust count value is below the trust threshold count vector value, that node is considered as malicious node.

3.2.2 Isolation of the malicious activities

Once the malicious activities are found, the alternative route will be chosen for forwarding the packet to the destination node. The data is aggregated before sending data to the destined user. The alternative path is chosen for collecting malicious activity information and sends it back to the sender. So the vulnerability of the attackers will be totally avoided.

4. PERFORMANCE EVALUATION

The performance of the proposed approach is evaluated in this section. The simulation model is discussed in Section 6.1 and the simulated results are presented and described in Section 6.2.

4.1. Network Model

In the proposed network model, it is assumed that K+1 mobile nodes are present in the network while taking the source node is K and destination node is (K+1). The packets are received in a queuing order from the rest of K nodes. The proposed model is symmetric and synthetic model. Here the mobile node may in the transmission range or out of the range. The packets are transmitted in a fixed size and the route discovery time is deterministic. Packets are arrived to the destination according to the Markovian Arrival Process in discrete time (DBMAP/D/1/N). Here, N is the buffer size of the destination mobile node. So, the process is in the queuing condition. Mobility nodes are randomly chosen while considering the packet loss probability which involves transition matrix is (K+1)(N+1) x (K+1)(N+1).

4.2 Mobility Model

Mobility model we have chosen for our proposed scheme is Random Waypoint Mobility model. The node pause time is changed between in direction or speed i.e. node starts by staying in one location for certain period of time. If the pause time is expired, the mobile node will choose a random destination and speed which are uniformly distributed between 0 and MAXSPEED. After that the node moves towards the destination at the selected period.

4.3 Simulation Model and Parameters

We have simulated our results using NS2.34 simulator. It is an object oriented discrete event simulator to identify the performance of proposed scheme. The Backend language of NS2.34 is C++ and front end is Tool command language (Tcl). NS2 is user friendly and easy to fabricate our own protocol. Tcl is a string-based command language. The language has only a few fundamental constructs and relatively little syntax, which makes it easy to learn. The syntax is meant to be simple. Tcl is designed to be a glue that assembles software building blocks into applications. Here we made the assumption that adopted for simulation is all nodes are moving dynamically including the direction and speed of nodes. Mobility scenario is generated by using random way point model with 300 nodes in an area of 1000 m × 1000 m. Our simulation settings and parameters are summarized in table 1.

Table1. Simulation And Settings Parameters Of OMRS

No. of Nodes	300
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Initial energy	75
Transmitted power	0.879
Received Power	0.08
Pause time	150 s
Communication range	540m

4.4 Performance Metrics

We evaluate mainly the performance according to the following metrics.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully to the total number of packets transmitted.

Communication Overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets. It suppresses the communication between the source and destination nodes.

End-to-end delay: It depends on the routing discovery latency, additional delays at each hop and number of hops.

Detection Ratio: It is the ratio of detection of link, path and node failure as well as malicious node to the total number of nodes during transmission phase.

E. Results

We compared our proposed scheme OMRS with Bandwidth Delay Product based Multicast routing Scheme [15] and On Demand Multicast Routing Protocol [19]. The results are examined by using performance metrics end-to-end delay, packet delivery ratio, malicious node detection ratio, network lifetime, end to end delay and overhead.

Fig.3 shows the analysis of nodes Vs Packet Delivery Ratio. From the results, our proposed scheme achieves high packet delivery ratio than the existing schemes like ODMRP and RMRBDP because of stability deployed in the optimized routing.

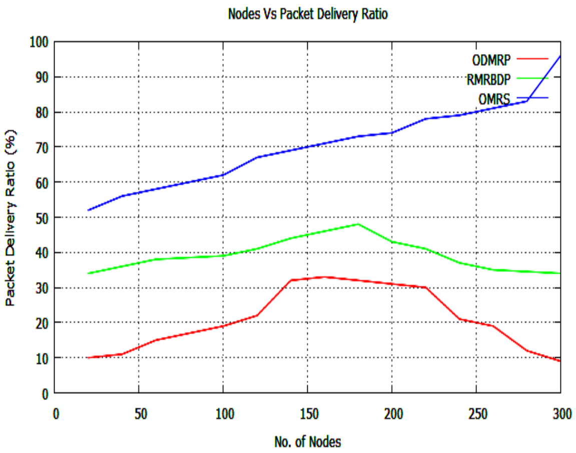

Fig.3. Nodes Vs Packet Delivery Ratio

In Fig.4, we vary the mobility from 10 to 100. While increasing the mobility, the communication overhead of proposed algorithm OMRS has low than the ODMRP and RMRBDP. This is achieved by employing the trustable packet loss ratio in the transmission process.

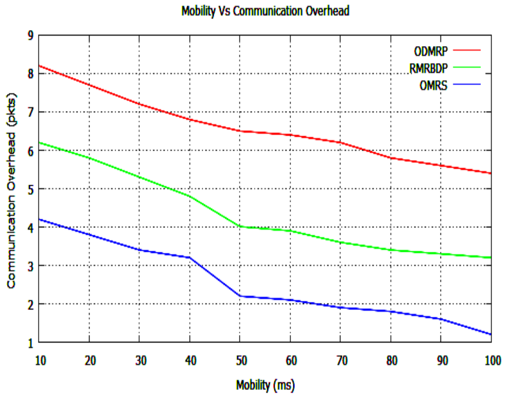

Fig 4. Mobility Vs Communication Overhead

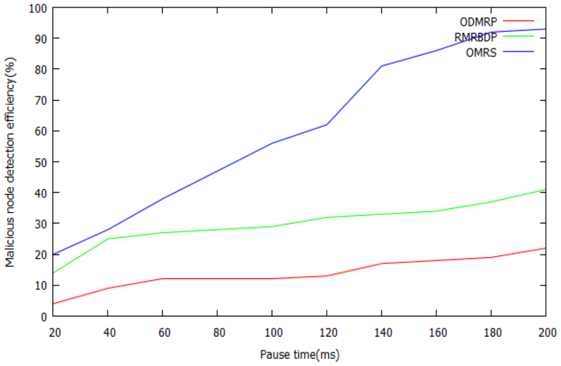

Fig.5 . Pause Time Vs Malicious Node Detection Efficiency

In Fig 5, Pause time is varied from 20 to 200 ms. The malicious detection efficiency of proposed scheme OMRS achieves high than the ODMRP and RMRBDP because of using node proposal and node familiarity parameters.

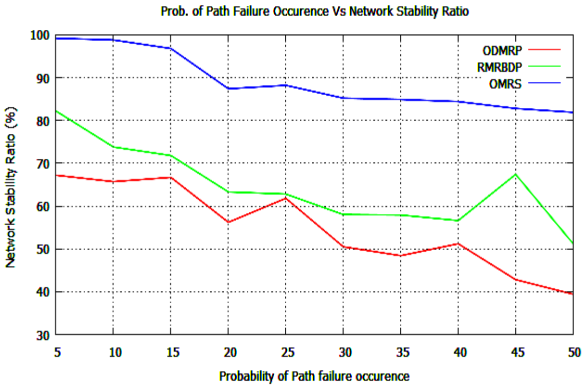

Fig 6. Probability Of Path Failure Occurrence Vs Network Stability Ratio

In Fig 6, we vary the probability value of path failure occurrence like 5, 10,…50. The network stability ratio of OMRS achieves higher than the RMRBDP and ODMRP.

In Fig 7, speed is varied as 10, 20….100. When we increase the speed, the mobility is also getting increasing. The proposed algorithm OMRS has low end to end delay per packet than the existing routing schemes like ODMRP and RMRBDP.

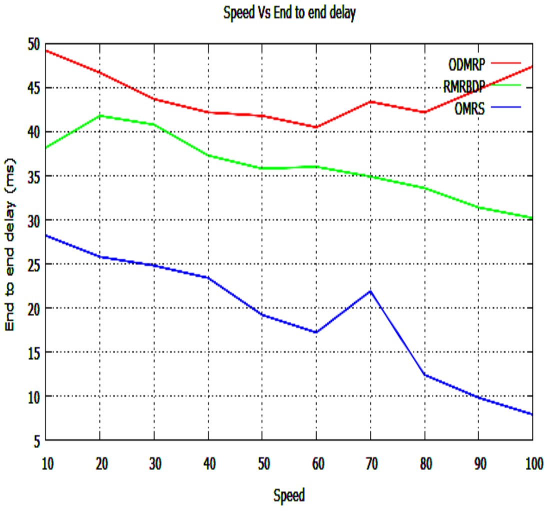

Fig 7. Speed Vs End To End Delay

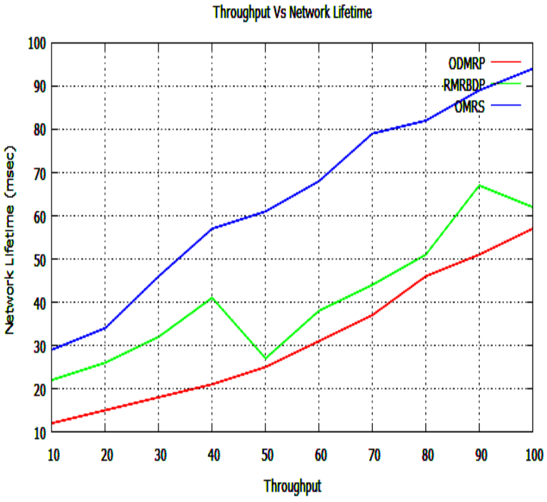

Fig 8. Throughput Vs Network Lifetime

In Fig. 8, throughput is varied as 10,20….100. The network lifetime of the proposed algorithm OMRS has high Network lifetime than the existing routing schemes like ODMRP and RMRBDP. This parameter is getting larger because of isolating the malicious activities.

5. CONCLUSION

In this research work, an optimized multicast routing scheme is proposed for handling link, node path failures and malicious attackers in ad hoc networks. The proposed scheme is based on threshold value to maintain the reliable multicast routing which enhances the stability and connectivity of the network. The vulnerability of the intruders is totally reduced by means of deploying our multicast routing scheme. By simulation results, the OMRS is better than BGP and ODMRP in the presence of malicious nodes. The proposed work can be a suggestive approach for a real life approach such as military search and rescue operations. Future studies can be extended to implement the authentication and security in the optimized multicast routing scheme to make more integrity that the information is carried out among the mobile nodes. We plan to choose the cryptographic schemes to make network more secure.

REFERENCES:

[1] Internet Engineering Task Force, "Manet working group charter', http://www.ietf.org/html charters/manetcharter.html.

[2] Gerharz, M., Waal, C. d., Martini, P. & James, P., " Strategies for Finding Stable Paths in Mobile Wireless Ad-Hoc Networks, LCN '03: *Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks*, IEEE Computer Society, Washington, DC, USA, 2003, pp. 130-136.

[3] Rajashekhar Biradar, Sunilkumar Manvi & Mylara Reddy, "Mesh Based Multicast Routing in MANET: Stable Link Based Approach", *International Journal of Computer and Electrical Engineering*, Vol. 2, No. 2, 2010, pp.1793-8163.

[4] Al-Sakib Pathan, Muhammad Monowar, Md. Rabbi, Muhammad Alam and Choong Hong, "NAMP: Neighbor Aware Multicast Routing Protocol for Mobile Ad Hoc Networks", The *International Arab Journal of Information Technology*, Vol. 5, No. 1, 2008, pp.102-107.

[5] M. Rajendiran and S.K. Srivatsa, "Route efficient on demand multicast routing protocol with stability link for MANETs", *Indian Journal of Science and Technology*, Vol. 5, No. 6, 2012, pp.2866-2871.

[6] Jing Dong Reza Curtmola Cristina Nita-Rotaru, "Secure High-Throughput Multicast Routing in Wireless Mesh Networks", *Proceedings of SECON*, 2008, pp.1-16.

[7] N. Nagaraju & M.L.Ravichandra, "Ordered Cross Layer Approach for Multicast Routing in Mobile Ad hoc Networks: Qos by Clogging Control", *Global Journal of Computer Science*

and Technology Network, Web & Security, Volume 12, Issue 16, 2012, pp.23-30.

[8] Clay Shields J.J. Garcia-Luna-Aceves, “KHIP : A Scalable Protocol for Secure Multicast Routing”, *Defense Advanced Research Projects Agency (DARPA)*, 1999, pp.1-13.

[9] G.S.Sreedhar and A.Damodaram, “ OLMRP: Hierarchical Outflow Load-balancing Multicast Routing Protocol for Congestion Control in Ad hoc Networks”, *International Journal of Computer Applications (IJCA)*, Volume 56, No.15, 2012, pp.12-17.

[10] Jun Luo, Patrick Th. Eugster and Jean-Pierre Hubaux, “Probabilistic reliable multicast in ad hoc networks”, *Elsevier, Ad Hoc Networks*, 2004, Vol.2, pp.369–386.

[11] Jamal N. Bani Salameh, Hani Q. Al-Zoubi and Yazeed A. Al-Sbou, “A Novel Multicast Routing Protocol for Ad Hoc Networks”, *European Journal of Scientific Research*, Vol.83, No.4, 2012, pp.475 – 492.

[12] R. Vennila and V. Duraisamy, “QoS Based Clustering Technique for Multicast Security in MANET”, *European Journal of Scientific Research*, Vol.81, No.1, 2012, pp.33-46.

[13] R. Manoharan and E. Ilavarasan, “Impact of Mobility on the performance of multicast routing protocols in MANET”, *International Journal of wireless and mobile networks*, Vol.2, No.2, 2010, pp.110-119.

[14] Velumani, R. and K. Duraiswamy , “Range Detection Multicast Routing Protocol for Mobile Ad-Hoc Networks”, *Journal of Computer Science*, Vol. 8, No.4, 2012, pp. 579-584.

[15] Rajashekhar C. Biradar & Sunilkumar S. Manvi (2012), “Ring Mesh Based Multicast Routing Scheme in MANET Using Bandwidth Delay Product”, *Springer, Wireless Personal Communication*, Vol.66, pp.117-146.

[16] Reza Curtmola and Cristina Nita-Rotaru, “BSMR: Byzantine-Resilient Secure Multicast Routing in Multi-hop Wireless Networks”, *Computer Science technical reports* , 2007, pp.1-22.

[17] Mulmuley, K., “Computational geometry: An introduction through randomized algorithms. *Englewood Cliffs: Prentice-Hall Inc*, 1999.

[18] S.Gopinath and Dr.A.Rajaram, “Improving Minimum Energy consumption in Mobile Ad hoc Networks under Different Scenarios”, *International Journal of Advanced and Innovative Research (IJAIR)*, Vol.1, Issue 4, 2012, pp.40-46.

[19] Sung-Ju Lee , Gerla, M. and Ching-Chuan Chiang, ““On Demand Multicast Routing Protocol”, *IEEE Conference on Wireless Communications and Networking*, 1999, pp.1298-1302.