MISBEHAVING ATTACK MITIGATION TECHNIQUE FOR MULTICAST SECURITY IN MOBILE AD HOC NETWORKS (MANET)

[1]C.RAJAN, [2]N.SHANTHI

[1]Assistant Professor, Department of Information Technology
KSR College of Technology
[2]Professor & HOD, Department of Information Technology
KSR College of Technology
E-mail: [1]crajanphd@gmail.com

ABSTRACT

Node misbehavior problems have received increased attention in multicasting in Mobile ad hoc networks (MANET). The misbehaving nodes can be either selfish or malicious nodes. The main goal of the malicious nodes is to intentionally interrupt the network using various attacks. Hence it is essential to develop a mitigation technique against misbehaving attacks. In this paper, we propose a misbehaving attack mitigation technique for multicast security in MANET. Initially the nodes are categorized into strong and weak nodes according to their stability index which is estimated based on the link availability and mobility. Among the selected strong nodes, the nodes with high reputation index are chosen as initiator nodes which assist in attack detection. The initiator node detects the misbehaving nodes based on their packet delivery ratio. Upon misbehaving node detection, initiators employ recrimination based attack isolation technique to isolate the attacker node during data transmission. By simulation results we show that the proposed technique enhances security in MANET.

Keywords: *Mobile Ad Hoc Networks (MANET), Misbehaving Attack Mitigation Technique (MAMT), Security.*

1. INTRODUCTION

1.1 Mobile Ad Hoc Networks

A multi-hop wireless networks with adaptive, self-configurable, self-organizing nature with exclusion of the infrastructure along with erratic active topologies is termed as mobile ad hoc networks. The adaptive, self-configurable and self-organizing nature reveals that the ad hoc network can be either combined or split into networks based on the requirements of the network. As it is devoid of infrastructure, it can be deployed without any base stations. The multi-hop wireless networks defines that the route between end users holds the multi-hop wireless links. Also the nodes in this network can move independently and forward the packets to other nodes [1].

By multi-hop wireless, means, in an ad hoc network the routes between end users may consist of multi-hop wireless links. In addition, each node in a mobile ad hoc network is capable of moving independently and forwarding packets to other nodes [1].

1.2 Multicasting in MANET

The process of broadcasting the packets to a group of zero or more hosts recognized a single destination address is termed as multicasting [2]. This implies that the message is transmitted from one sender to several receivers or from multiple senders to multiple receivers. The merit of multicast technique is that it offers services to multiple users exclusive of networks and resources overloading in the server [3]. The multicast technique is utilized by the application such as routing, neighbor discovery, key distribution and topology control. This technique is also used by the ad hoc network application that desires identical data transmission from a single sender to several receivers which minimizes the network traffic and energy consumption. [5]

The multicasting approach can enhance the efficiency of the wireless links for transmitting the multiple copies of messages in order to utilize the inbuilt broadcast nature of wireless transmission. Thus multicast takes a major responsibility in MANET. The major aim of multicast routing protocol is to reduce the control overhead and processing overhead, enhancing the potentiality of multicast routing protocol, upholding the dynamic topology and avoids network loops and so on.

1.3 Attacks on Multicast in MANET

Owing to the complications and exclusivity in MANETs, they are more susceptible to security threats in contrast to their wired counterparts. The categories of attacks in ad hoc network include passive and active attacks [4].

Passive attacks: During this attack, normal network function is not disturbed but the data swapped in the network is intruded by the attacker without any changes.

Active attacks: During this attack, the attacker tries to modify or destroy the data that is swapped in the network which interrupts the regular network operation.

Resource Consumption Attack: In this attack, the malicious node intentionally consumes the network resources.

Rushing Attack: This attack prevails in on-demand routing protocol that utilizes the route discovery process. When an attacker node receives a “route request” packet from the source, it rapidly floods the packet all through the network. Thus the other node that receives the same “route request” will not be able to respond.

Black Hole Attack: During this attack, the malicious node wrongly publicizes the best route to the destination node while executing the route discovery process.

Gray Hole attack: This category of attack includes two phases. During the first phase, the malicious node utilizes the AODV protocol to publicize itself since it possess suitable route to the destination node. During the second phase, seized packets are dropped by the node.

Wormhole Attack: The packets that are received at one point by the attacker are tunneled to another point in the network. Then the attacker repeats the process of tunneling the packet from that point into the network.

Anonymity, non-repudiation, access control, trust issues, upholding service availability for safeguarding the network from clogging attacks etc. are certain other security issues in MANET [4].

1.4 Security in Multicasting in MANET

The basic features of security in MANET include confidentiality, integrity, authentication and non-repudiation.

Confidentiality:

This aspect guarantees that the network information cannot be revealed to the illegal unit.

The leakage of tactical military decisions or location information can result in serious effects and thus confidentiality is very much necessary.

Integrity:

The malicious nodes have a capability to modify the data in the network due to benign malfunction that includes the radio propagation harm or due to the hardware glitches in the network. This integrity is essential that maintains data transmitted between nodes without any change or degradation.

Availability:

Availability means that despite the presence of the potential issues in the system, the services that are demanded are available in a timely manner. The packet drop and weakening of resources alleviates the network availability.

Authenticity:

The lack of authentication can cause the attacker masquerade any node and rules over the whole network.

Non-repudiation:

Non-repudiation guarantees that the message forwarded cannot be refused by the message instigator. It is very helpful for recognizing and separation of compromised nodes. [4]

1.5 Problem Identification

The existing techniques [6, 7, 8, 9, 10, 11] described in section 2 do not provide efficient counter measures against attacks. As per thorough observation, we understand that only limited techniques has arrived in recent times for handling misbehaving attacks related to multicast security in MANET. Hence, we propose a defensive mechanism against misbehaving attacks in MANET to enhance multicast security.

2. RELATED WORKS

Aishwarya.K et al [6] have proposed an enhanced on-demand multicast routing protocol (E-ODMRP) in MANET. This protocol is mesh based multicast routing protocol that has a high packet delivery ration under high mobility and high throughput. They utilized the waiting time variable and route reply table of the protocol for suspecting the malicious nodes. The drawback is that the proposed approach is not tested for reactive protocols.

Shang-Ming Jen et al [7] have proposed a multipath hop-count analysis (MHA) in order to avoid wormhole attacks based on a hop-count analysis scheme. MHA is designed to use split multipath routes, so the transmitted data are naturally split into separate route. This scheme does not require additional hardware or impractical assumptions of the networks. Hence, it can be directly used in MANET. Though this approach offers a solution to wormhole attack problems, the dynamic information of the packets could still be modified.

V. Palanisamy et al [8] they studied the impact of rushing attacks in multicast session in MANET. They drew a graph based on the rushing attack position in the network. With respect to the attack positions, the best position to launch rushing attacks is at the near receiver, have the highest success rates. The rushing attack near sender have the low success rate and final attack position is likely to take place anywhere in the network, have the least success rate.

Mr. A. Amuthan et al [9] they worked towards securing multicast routing protocol for ad hoc networks. Initially they examined the vulnerabilities of PUMA (Protocol for Unified Multicasting through Announcements) which is a representative of mesh based routing protocol and proposed a trust based approach where in which the secure route is selected for the receivers not only based on current trust values of its neighbor nodes but also its past experience is considered for black hole and wormhole attack.

Mrs. N.Shanthi et al [10] have proposed a secure scheme for multicast ad-hoc on-demand distance vector routing protocol in MANET. In order to guarantee the integrity in ad hoc networks, secure hash algorithm-1(SHA-1) is used. The drawback of this approach is that certain attacks such as tunneling attacks, selectively drop packets persisting in ad hoc network is not handled.

S.Vijayalakshmi et al [11] have proposed a two novel techniques such as limiting packet propagation parameter (LP3) and neighbor aware wormhole adversary axing (NAWA2) which sustainably maintains the network performance parameter like multicast packet delivery (MPDR) at a constant level despite the severity of the attack. LP3 is embedded with the multicast packet just like time to live (TTL) field. NAWA2 helps to instantly prune the misbehaving wormhole perpetuators culminating in cordoning off the attack infected zone.

3. PROPOSED WORK

3.1 Overview

In this paper, we propose a misbehaving attack mitigation technique for multicast security in MANET. Initially the nodes are categorized into strong and weak nodes according to their stability index. The stability index is estimated based on the link availability and mobility. Among the selected strong nodes, the nodes with high reputation index are chosen as initiator nodes which assist in attack detection. The initiator node estimates the predicted and recognized packet delivery ratio of their neighbor nodes. The predicted packet delivery ratio is estimated from the success probability product metric (SPP) at the concerned route. The recognized packet delivery ratio is determined by testing the continuity of the sequence number in received data packets. If the difference of both the packet delivery ratio exceeds threshold, then nodes are detected as misbehaving. Upon detecting misbehaving nodes, initiators employ the recrimination based attack isolation technique to isolate the attacker node during data transmission. Through this technique, the valid paths can be utilized in spite of false recrimination of the strong nodes.

3.1.1 Estimating Received Signal Strength

The received signal strength (RSS) is computed using the following formula

$$RSS = \alpha * \theta * S_{tx} \qquad (1)$$

where α = constant that relies on the wavelength and the antennas.

θ = channel gain.
S_{tx} = Signal power of the transmitter.

RSS can be expressed in terms of the dB and dBm (dB milliWatts) as follows.

$$RSS\,[dBm] = 10 \log_{10} \alpha + \theta\,[dB] + S_{tx}\,[dBm] \qquad (2)$$

3.1.2 Estimating Mobility

The mobility is estimated based on power level detected at the receiving node (N_{rx}) [15].

In the ideal background, the Friis free space propagation model uses an inverse-square dependence of the ratio of received and transmit power on the physical distance between the transmitter and receiver.

i.e. $$\frac{RSS}{S_{tx}} \propto \frac{1}{dist^2} \qquad (3)$$

But, in the real environment, calculating distance among the transmitter and receiver from the computed signal strength is not possible owing to complications in accuracy of channel modeling.

From the ratio of RSS among the two consecutive packet transmissions from a neighbor node, the information concerned with mobility among the two nodes can be obtained. Through this information, the mobility metric $M_j(i)$ at a node j with respect to i is calculated as follows.

$$M_j(i) = 10 \log_{10} \frac{RSS_{i \to j}^{new}}{RSS_{i \to j}^{old}} \qquad (4)$$

3.1.3 Link Quality

Link Quality (LQ) is estimated by ratio of the number of bits in error to the number of bits received (bit error rate) [16].

$$LQ = b_{error} / b_{rx} \qquad (5)$$

This value gets updated for every packet received at a node over a certain period. It depends on parameters such as the interference effect of the wireless channel, additive white Gaussian noise, and signal transmission range.

3.1.4 Stability Index

Stability index (SI_{ij}) is computed for a link to a neighbor based on the received signal strength, mobility and link quality (Using the section 3.1.1, 3.1.2, and 3.1.3)[16]. SI_{ij} of a link between node i and node j is defined as follows

$$SI_{ij} = \frac{RSS * LQ}{M_j(i)} \qquad (6)$$

3.1.5 Estimation of Reputation of Nodes

Consider the nodes i and j.

The recent satisfaction index (P_{ij}) for node i about node j is computed as follows.

$$P_{ij} = f(i, j) – e(i, j) \qquad (7)$$

where f (i, j) = percentage of packets originating from i that were forwarded by node j over the total number of packets offered to node j.

e (i, j) = percentage of packets that were expired over the total number of packets offered to node j.

Thus P_{ij} can be considered as the direct reputation of node j

$$Rep_{ij} = Rep_{ij\text{-}pr} * W_{hist} + P_{ij} * (1- W_{hist}) \qquad (8)$$

where $Rep_{ij\text{-}prev}$ is reputation value that node i had for node j before incorporating the most recent satisfaction index.

W_{hist} is a constant that reflects the level of confidence that node i has in the past observed reputation for its neighbor j.

REP_{ij} is normalized using the following equation

$$REP_{ij} = \frac{REP_{ij}}{\max_t(REP_{ij})} \qquad (9)$$

$\max_t$ is the function that reports the maximum observation of REP_{ij} over time [17].

3.1.6 Success Probability Product Metric (SPP_i)

Let S and D represent the source and destination respectively.

Let N1 and N2 represent the two intermediate nodes respectively.

The link quality (N1 → N2) as recognized by N_2 is given as:

$$SPP_i = Pr_{succ} \qquad (10)$$

where Pr_{succ} represent the probability that a packet is sent successfully from N1 to N2 in the forward direction. N_2 gets the Pr_{succ} by counting the probe packets received from N_1 over a fixed time interval.

For SPP, the probability of a packet distributed over a path from S to D is defined as the product of the probabilities that the packet is successfully delivered to each of the intermediate nodes on the path. When the intermediate node gets failed, then the entire route fails, as there are no re-transmissions.

Thus $SPP_{s \to D}$ (in fact 1/ $SPP_{s \to D}$) represents the predicted number of transmissions required at S to deliver a packet from S to D successfully.

SPP value ranges in the interval [0, 1].
Specifically, SPP = 1 $\Rightarrow$ perfect reliability
SPP = 0 $\Rightarrow$ complete unreliability. [12]

3.2 Classifying the Nodes

The nodes are categorized into two types namely strong and weak nodes. The steps involved in selecting the nodes are as follows.

1) Each node deployed in the network periodically exchanges a HELLO packet with its neighbor nodes.

2) By exchanging the hello packets, every node measures the received signal strength RSS, link quality and mobility $M_j(i)$ of its neighbor nodes. (explained in section 3.1.1-3.1.3)

3) Based on the measurement of RSS, link quality and $M_j(i)$, each node computes the stability index (SI) of its neighbor nodes (explained in section 3.1.4) and the values are stored in the neighbor table (NT).

4) The SI of each neighbor N_i is checked such that

```
If SI_i < SI_th (threshold of Stability Index)
Then
    The nodes are marked as weak nodes (N_wi) and
    stored in NT
Else
    The nodes are marked as strong nodes (N_si) and
    stored in NT
End if
```

For example consider the network in fig. 1. The nodes 7, 8, 15, and 16 are marked as strong nodes as their stability index is greater than the threshold value. Remaining nodes are marked as weak nodes as their stability index is less than the threshold value.

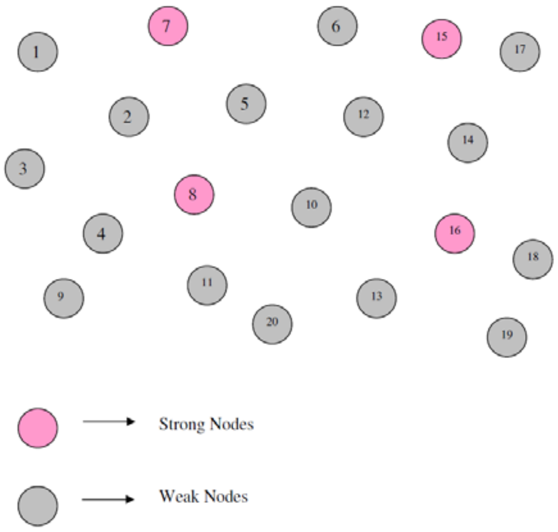


Fig 1 Selection of Strong and weak nodes

3.3 Selection of Initiator Nodes

Among the chosen Ns_j (explained in section 3.2), some nodes has to be designated as initiators which helps in detection of the misbehaving nodes. The initiators (I) are selected based on the reputation index (RI) of nodes (explained in section 3.1.5).

The direct reputation of node N_{sj} is given as.

$$Rep_{ws} = Rep_{ws\text{-}pr} * z + P_{ws} * (1- z) \qquad (11)$$

Where $Rep_{ws\text{-}pr}$ = reputation value of N_{sj} contained in N_{wi} prior to the addition of recent satisfaction index.

z = constant that replicates the level of confidence possessed by N_{wi} for its N_{sj}.

P_{ws} = recent satisfaction index for N_{wi} about N_{sj}

Thus N_{sj} with high Rep_{ws} values are selected as initiators (I).

The attacks do not affect the multicast protocol unless they cause a drop in the packet delivery ratio (PDR).

In the following section, we consider a reactive approach for detecting and isolating the attacker nodes.

3.4 Detection of Attacker Nodes

When the data is not delivered at a reliable rate and optimal path quality, it is predicted that attack is detected. The attack detection technique depends on the capacity of I to detect the difference among the predicted PDR (PrP) and recognized PDR (ReP). The estimation of PrP and ReP is as follows.

PrP can be estimated from the success probability product metric (SPP) at the concerned route (Explained in section 3.1.6).

SPP for a path of n links among S and D is given by Eq (12)

$$SPP_{S\to D} = \Pi_{i=1}^{n} SPP_i \qquad (12)$$

where the metric for each link i on the path is $SPP_i = Pr_{succ}$.

ReP of a route is determined by testing the continuity of the sequence number in received data packets. i.e by dividing the number of received packets by the number of packets sent by the source over an interval of time.

ReP in terms of performance of packet delivery is given by the following equation.

$$ReP = P_r / P_s \qquad (13)$$

where P_r is the average number of packets received by all receivers

P_s is the number of packets sent by the source.

Even if the attacker nodes drop all data packets, initiator nodes have capacity to determine the ReP with the inclusion of the backup data packet authenticated by the source.

```
If |PrP−ReP| > η
Then
The malicious behavior is detected by I since the particular route does not deliver the data at consistent level with optimal path quality.
End if
```

3.5 Isolation of Attacker Nodes

The steps involved in the isolation of attacker nodes are as follows

Step 1

When I detects the malicious behavior, it temporarily recriminates the suspicious node by flooding a failure notice in the network that includes ID of recriminated and recriminator nodes and the period of recrimination.

Step 2

Until the recrimination is valid, metrics broadcasted by the recriminated node will not be taken into account and will be discarded during routing process.

Step 3

In case of transient network variations, the temporary recrimination scheme is taken into consideration.

Step 4

In temporary recrimination strategy, initially the time period of recrimination is computed in relative to the observed difference among PrP and ReP. This is performed with the intention that the recriminations caused by increase in metric values as well as malicious data dropping rate retains for longer duration than the recriminations caused by the transient network variations.

Step 5

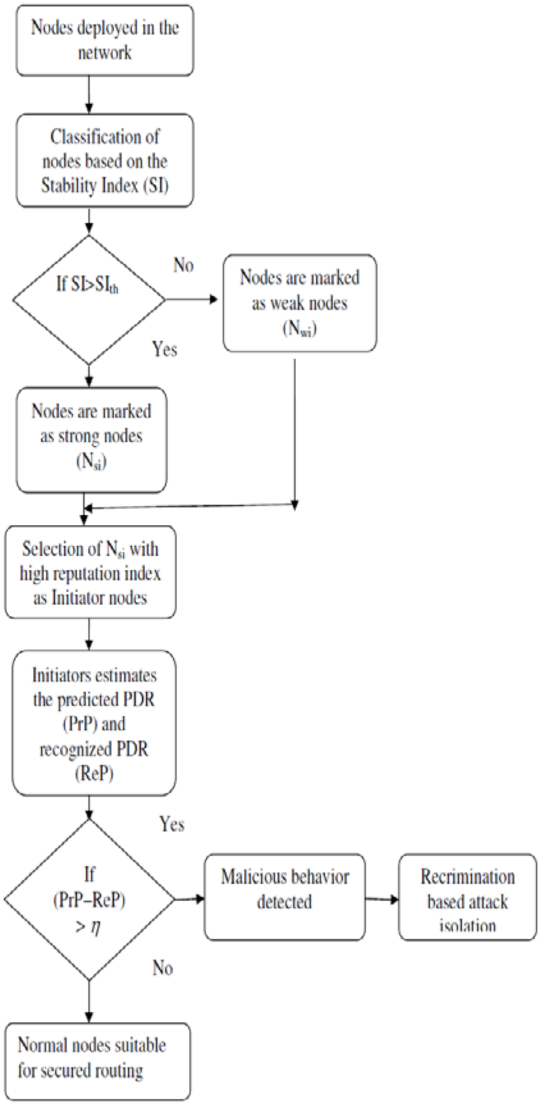
In order to avoid the recrimination caused by attackers, a node is not permitted to announce a new recrimination prior to the expiry of the already announced recrimination.

Step 6

If the best metric is broadcasted by an recriminated node
Then
The initiator node activates the recriminated node in addition to the best non-recriminated node.

The step 6 reveals that the valid paths can still be utilized in spite of false recrimination of the strong nodes.

3.6 Flowchart of Overall Technique


Nodes deployed in the network
Classification of nodes based on the Stability Index (SI)
If SI>SI$_{th}$
No
Nodes are marked as weak nodes (N$_{wi}$)
Yes
Nodes are marked as strong nodes (N$_{si}$)
Selection of N$_{si}$ with high reputation index as Initiator nodes
Initiators estimates the predicted PDR (PrP) and recognized PDR (ReP)
Yes
If (PrP–ReP) > η
Malicious behavior detected
Recrimination based attack isolation
No
Normal nodes suitable for secured routing

4. SIMULATION RESULTS

4.1. Simulation Model and Parameters

We use NS-2 [14] to simulate our proposed protocol. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. For multicasting, we have used multicast AODV (MAODV) [ ] routing protocol.

In our simulation, 50 mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in table 1.

Table1: Simulation Parameters

No. of Nodes	50
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Rate	250Kb
Mobility Model	Random Way Point
Receivers	10,20,…50
Attackers	1,2,3,4 and 5.

4.2. Performance Metrics

We compare our Misbehaving Attack Mitigation Technique (MAMT) with the traditional GKMP [13]. We evaluate mainly the performance according to the following metrics.

Average Packet Delivery Ratio: It is the ratio of the No. of packets received successfully and the total no. of packets sent.

Throughput: It is the average packets received at the destinations.

Drop Rate: It is the ratio of number of packets dropped at each receiver and the total no. of packets sent.

A. Based on Attackers

In the second experiment we vary the number of attackers as 1,2,3,4 and 5. with receivers as 20

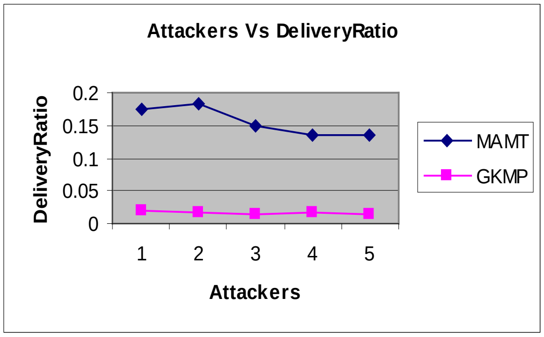


Fig 2: Attackers Vs Delivery Ratio

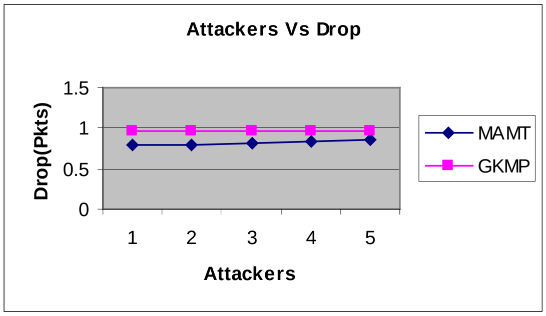


Fig 3: Attackers Vs Drop

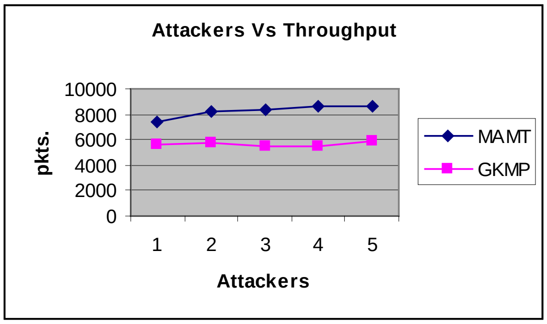


Fig 4: Attackers Vs Throughput

From fig. 2, we can see that our proposed MAMT protocol achieves high delivery ratio than the existing GKMP scheme.

From fig. 3, we can see that our proposed MAMT has less packet drop than the existing GKMP scheme.

From fig. 4, we can see that our proposed MAMT protocol has low Overhead than the existing GKMP scheme.

B. Based on Receivers

In our first experiment we vary the number of receivers as 10,20,30,40 and 50 with attackers as 5.

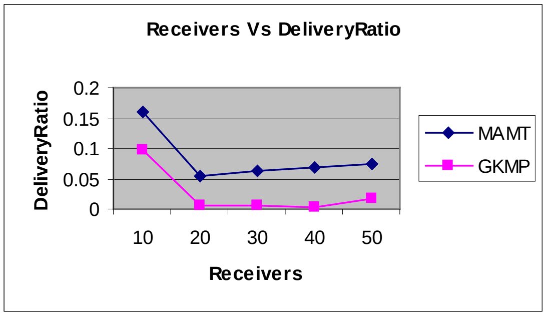


Fig 5: Receivers Vs Delivery Ratio

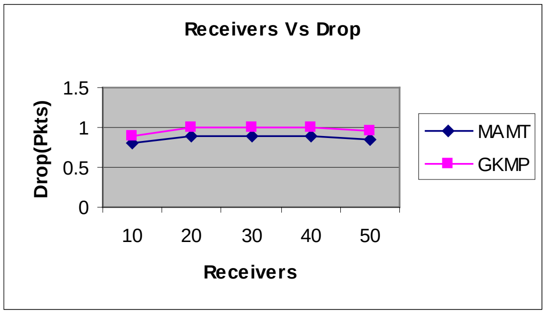


Fig 6: Receivers Vs Drop

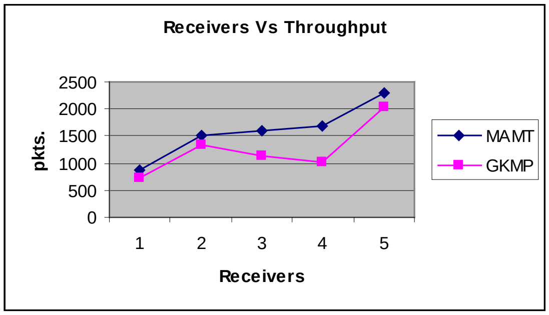


Fig 7: Receivers Vs Throughput

From fig. 5, we can see that our proposed MAMT protocol achieves high delivery ratio than the existing GKMP scheme.

From fig. 6, we can see that our proposed MAMT has less packet drop than the existing GKMP scheme.

From fig. 7, we can see that our proposed MAMT protocol has low Overhead than the existing GKMP scheme.

5. CONCLUSION

In this paper, we have proposed a misbehaving attack mitigation technique for multicast security in MANET. Initially the nodes are categorized into strong and weak nodes according to their stability index. The stability index is estimated based on the link availability and mobility. Among the selected strong nodes, the nodes with high reputation index are chosen as initiator nodes which assist in attack detection. The initiator node estimates the predicted and recognized packet delivery ratio of their neighbor nodes. If the difference of both the packet delivery ratio exceeds threshold, then nodes are detected as misbehaving. Upon detecting misbehaving nodes, initiators employ the recrimination based attack isolation technique to isolate the attacker node during data transmission. Through this technique, the valid paths can be utilized in spite of false recrimination of the strong nodes. By simulation results, we have shown that the proposed approach improves packet delivery ratio and reduces the packet drop in presence of attacker nodes.

REFERENCES

[1] K. Sahadevaiah, O.B.V. Ramanaiah, “Self-Organized Public Key Cryptography in Mobile Ad Hoc Networks”, *Journal of Ubiquitous Computing and Communication*.

[2] Luo Junhai , Xue Liu b and Ye Danxia “Research on multicast routing protocols for mobile ad-hoc networks ” *Computer Networks* 52 (2008) 988–997.

[3] R. Srinivasan, V. Vaidehi, R. Rajaraman, S. Kanagaraj, R. Chidambaram Kalimuthu, and R. Dharmaraj “Secure Group Key Management Scheme for Multicast Networks” *International Journal of Network Security*, Vol.10, No.3, PP.205–209, May 2010.

[4] N.Shanthi, Dr.lganesan and Dr.k.Ramar “Study of different attacks on multicast mobile ad hoc network” *Journal of Theoretical and Applied Information Technology* 2005 - 2009 JATIT.

[5] Loukas Lazos and Radha Poovendran “Power Proximity Based Key Management for Secure Multicast in Ad Hoc Networks” *Journal Wireless Networks* Volume 13 Issue 1, January 2007.

[6] Aishwarya .K, Kannaiah Raju .N and Senthamarai Selvan .A, “ Counter Measures Against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol In Mobile AD-HOC Networks”, *International Journal of Technology And Engineering System*(IJTES), 2011.

[7] Shang-Ming Jen, Chi-Sung Laih and Wen-Chung Kuo, “ A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET”, Sensors 2009, pp 5022-5039; doi:10.3390/s90605022.

[8] V. Palanisamy and P.Annadurai, “ Impact of Rushing attack on Multicast in Mobile Ad Hoc Network”, *International Journal of Computer Science and Information Security* (IJCSIS), Vol. 4, No. 1 & 2, 2009

[9] Mr. A. Amuthan and D. Nagamani Abirami, “Multicast security attacks and its counter measures for PUMA protocol”, *International Journal of computer technology and applications*, Vol 2, pp 594-600, 2011.

[10] Mrs.N.Shanthi and Dr. L.Ganesan, "Security in Multicast Mobile Ad-Hoc Networks", *IJCSNS International Journal of Computer Science and Network Security*, vol.8 No.7, July 2008.

[11] S.Vijayalakshmi and S.Albert Rabara, " Weeding Wormhole Attack in MANET Multicast Routing using Two Novel Techniques - LP3 and NAWA2", *International Journal of Computer Applications*, Volume 16– No.7, 2011.

[12] Jing Dong, Reza Curtmola, and Cristina Nita-Rotaru, "On the Pitfalls of Using High-Throughput Multicast Metrics in Adversarial Wireless Mesh Networks", *5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks* (SECON), pp 224 – 232, 2008.

[13] Mohamed Salah Bouassida, and Mohamed Bouali "On the Performance of Group Key Management Protocols in MANETs" *Joint Conference on Security in Network Architectures and Information Systems* (SAR-SSI'07), Annecy : France (2007)

[14] Network Simulator : http://www.isi.edu.na/nam