ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

Optimization of Throughput Using Multicast Routing in Wireless Mesh Networks

Akuluri Rakesh, S.R.Jino Ramson, John Major.J

Abstract - **In the recent years the multicast routing in wireless mesh network has given attention on metrics to improve link quality and to increase the high-throughput.Nodes must have always contact with their neighbouring nodes to send the data to the destination.In the wireless mesh network all nodes acts as honest and behave correctly during the data transmission,As well as data transmission leads to unexpected consequences in the network where these nodes acts as intruders. In this work, we discover attackers against high-throughput multicast protocols in wireless mesh network.These intruders allows other malicious nodes to increase large amount of traffic.These attackers are highly successful against multicast protocols based on high-throughput metrics.We conclude that these path selection is very secure.So it increase the throughput and also have high effect on the attackers.So our idea is to defend against the attackers by using Rate guard mechanism.The important protocol used in this wireless mesh network is ODMRP,SPP,and ETX metric to the multicast setting**.

***Index Terms*— Wireless Mesh Network, High-Throughput, RateGuard, Intrders, Multicast Routing.**

I . INTRODUCTION

Wireless mesh network (WMN) is a communications network design of radio nodes planned in a mesh topology. Wireless mesh networks often contains of mesh clients, gateways and mesh routers. The mesh clients are often computers, mobiles,Bluetooth devices and other wireless devices during the mesh routers send traffic from and to the gateways which may be not connect to the Internet.Sometimes called a mesh cloud when the coverage area of the radio nodes work as a single network in Access to the mesh cloud is dependent on the radio nodes working in match with each other to make a radio network. When a node can't operate, the rest of the nodes can still have communication with each other nodes, directly or using the intermediate nodes.

Multicast routing protocol transmits data from source to many destinations in a multicast group.In the previous years,many prorocols [2], [3], [4], [5], [6], [7], [8] were implemented to provide multicast services for wireless networks.However by using hop count sa routing metric can be result in selecting links with bad quality of the path,and also decreasing in the path throughput [9], [10].Recent protocols [11], [12] will be focusing on to maximize the path throughput by selecting paths based on the path metrics.The mesh routers may be mobile, and able to move according to exact demands comming in the network.These mesh routers are not limited in terms of resources compared to other nodes in the network and thus can be used to perform more resource and functions.since in this way, the wireless mesh network different from an ad-hoc network, since these nodes are often forced to do by the resources.Severe attacks against multicast protocols that use of high-throughput metrics, including LOCAL METRIC MANIPULATION and GLOBAL METRIC MANIPULATION. We show that aggressive path selection is a double edged sword: It leads to increased throughput, but it also leads to devastating effects in the presence of attacks. For example, our simulations show that 5 GLOBAL METRIC MANIPULATION attackers can cause the same attack impact as 20 packet dropping attackers.Secure high-throughput multicast protocol SECURE-ON DEMAND MULTICAST ROUTING PRTOCOL that incorporates a novel defense RateGuard mechanism. RateGuard contains measurement-based detection and accusation-based reaction scheme to deal with the metric manipulation and packet dropping attacks. To prevent intruders from distroy the defense mechanism itself, RateGuard limits the total number of accusations that can be produced by a node. RateGuard also chooses a fugitive accusation mechanism that adopts false positive accusations that may be caused by temporary network variations.

II. HIGH-THROUGHPUT MULTICAST ROUTING

In multi-hop wireless network where nodes involves in the data forwarding process for other nodes.In a mesh-based multicast routing protocol, which maintains a mesh connection between multicast sources and receivers. Path selection is based on a metric design to increase through put. The Rate Guard mechanism is calculated using a formula (ePDR-pPDR).when the attackers changes the weights of the node or a link then we are using the RateGuard mechanism.So the expected PDR (ePDR) perceived PDR (pPDR).The

Manuscript received Feb, 2013.
Akuluri Rakesh, *Electronics and Communication Engineering, Karunya University, Coimbatore, India.*
S.R.Jino Ramson, *Electronics and Communication Engineering, Karunya University, Coimbatore, India,*
John Major.J, *Electronics and communication Engineering, Karunya University, Coimbatore, India,*

network has to give a threshold value to detect the mugger in the network.

A. High-Throughput Metrics

Traditionally, routing protocols have been used hop count as a path selecting metric. In static networks, however, this metric was shown to achieve suboptimal throughput because paths tend to include lossy wireless links . As a result, in recent years, the focus has shifted toward high-throughput metrics that seek to maximize throughput by selecting paths based on the quality of wireless links.The ETX metric was intend for unicast routing and estimates the expected number of transmissions needed to successfully deliver a unicast packet over a link, includes retransmissions. Each node for a time interval broadcasts probe packets received from each of its neighbour node over a period. A couple of neighbouring nodes, X and Y, estimate the quality of the link X to Y.

B. High-Throughput Mesh-Based Multicast Routing

Multicast protocols supply communication from sources to receivers organized in groups by establishing structures such as trees or meshes, dynamically suitable as nodes join or leave the group.

C. ODMRP overview-

On demand multicast routing protocol(ODMRP) is for the multihop wireless network, which uses a mesh of nodes for each multicast group.nodes are joined to the mesh network through a routing selection.

D. JOIN QUERY MESSAGE:

The source node periodically re-creates the mesh network by sending a join query message in the network in order to refresh the membership information and update the routes.When the source node sends the message then the other neighbouring nodes reaches the message which is send by the source node and then if any intermediate node wants to join the network where these nodes are periodically updates the neighbouring nodes data.So it knows the new node is a intruder or a normal intermediate node until the message reaches the destination.

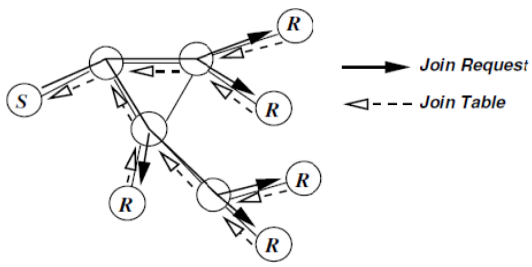

Fig. 1 On demand route and mesh creation

E. Join Reply Message:

In the JOIN REPLY when the reciver node gets a LOIN QUERY message,it creates the path from itself to the source node by constructing and broadcasting a JOIN REPLY message that contains the information for each multicast group if it wants to join.When a intermediate node receives a JOIN REPLY it checks the entries in the message whether it matches its own identifier.If it matches, it makes itself a node part of the mesh and creates a new JOIN REPLY creates upon the matched entries.

III. ATTACKS AGAINST HIGH-THROUGHPUT MULTICAST

A. Mesh Structure Attacks:

Mesh structure attacks disturb the correct organization of the mesh structure in order to disturb the data delivery paths. These attacks can be guarded by malicious manipulation of the JOIN QUERY and JOIN REPLY messages. For the JOIN QUERY messages, the attacker can spoof the source node and gives something new invalid JOIN QUERY messages, which can create paths toward the attacker node instead of forward to the correct source node. The intruders may also act in a disapproving manner by dropping JOIN QUERY messages, which allows them to avoid involving in the multicast protocol. Ever since JOIN QUERY messages are filled in the network, unless the attacker nodes form a vertex cut in the network, they cannot prevent legitimate nodes from receiving JOIN QUERY messages. Finally, the attacker may also modify the accumulated path metrics in the JOIN QUERY messages incorrectly. Such metric manipulation attacks can pose a severe threat to the correctness of path establishment. For the JOIN REPLY messages, the mugger can drop JOIN REPLY messages to cause its downstream nodes to be seperated from the multicast mesh. The intruders can also forward JOIN REPLY to an corrupted next hop node to cause an corrupted path being built .

B. Metric Manipulation Attacks

Multicast protocols using high-throughput metrics chooses paths to the source that are having high quality, while it try to avoid low quality paths. Thus, a good plan for an intruder to increase its chances of being selected in the FORWARDING GROUP is to advertise artificially good metrics for routes to the source. The use of high-throughput metrics needs each node to collect local data about its touching links based on periodic probes packets from its neighboring nodes. This local information is stored in JOIN QUERY packets and broadcasted in the network, allowing nodes to obtain global data about the quality of the routes from the source.These intruders can execute two types of metric manipulation attacks: LOCAL METRIC MANIPULATION (LMM) and GLOBAL METRIC MANIPULATION (GMM).

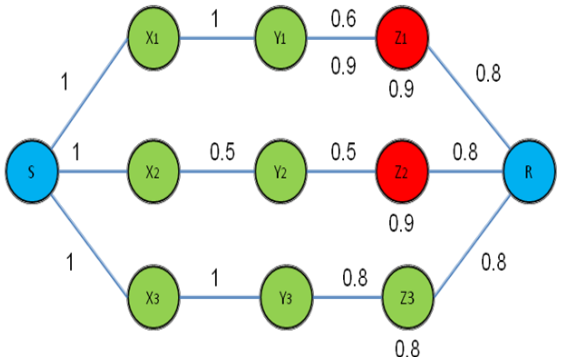

Fig. 2 Metric Manipulation attack during the broadcasting packets from the source(S) to receiver(R)

These attacks are complicated in nature, as they are performed by nodes that have the credentials to participate in the routing protocol, but are under adversarial control local metric manipulation attacks- An adversarial node artificially increases the quality of its adjacent links, disfigure the neighboring nodes' discernment about these links.The fake advertise "highquality" links will be preferred and byzantine nodes have better chances to be comprise on routes. A node can claim a false value for the quality of the links toward itself. In Fig.2, a malicious node Z1 claims that SPP of Y1 to Z1is 0.9 instead of the correct metric of 0.6. Thus, Z1 accumulates a false local metric for the link Y1 to Z1 and advertises to R the metric SPP of S to Z1 is 0.9 instead of the correct metric SPP of S to C1 is 0.6. The route S-X1-Y1-Z1-R will be chosen over the correct route S-X3-Y3-Z3-R.GLOBAL MANIPULATION METRIC attacks- In a GLOBAL MANIPULATION METRIC attack, a malicious node arbitrarily changes the value of the route metric accumulated in the flood packet, before rebroadcasting this packet. A GLOBAL MANIPULATION METRIC attack allows a node to manipulate not only its own donation to the path metric, but also the donation of previous nodes that were accumulated in the path metric. For example, in Fig.2, attacker Z2 should advertise a route metric of 0.25, but instead present a route metric of 0.9 to node R. This causes the route S-X2-Y2-Z2-R to be selected over the correct route S-X3-Y3-Z3-R.

IV. SECURE HIGH-THROUGHPUT MULTICAST ROUTING

A. *Authentication Framework*

We belive that each user approved to be part of the mesh network has two some of public and private keys and a client license that attaches its public key to a rare user identifier. This protection against external attacks from nodes that are not part of the network. We assume source data is verified, so that receivers can differentiate verified data from false data.

B. *S-ODMRP*

Secure-On Demand Multicast Routing Protocol uses a combination of verification and rate limiting techniques against resource utilization attacks and a novel technique, RateGuard, against the more demanding packet sinking and mesh structure attacks,as well as metric manipulations and JOIN REPLY dropping.

Sign(m): sign message m using this node's private key
Verify(n_id, sig): verify the signature sig using node n_id's public key and exit the procedure if the verification fails
Start_timer(timer, t): start timer timer with timeout t
Refresh_timer(timer, t): if timer is not active, then call Start_timer(timer, t); otherwise, set timeout of timer to t
Broadcast(m): broadcast message m one hop
Flood(m): flood message m in the entire network
Send_message(m, n_id): reliably send message m to neighbor n_id
Link_metric(n_id): return the measured link metric to neighbor n_id
Get_best_metric(query_set): return the best metric of all queries in the set query_set, regardless of accusation status
Get_neighbor_best_metric(query_set): return the neighbor that has the best metric in the set query_set, regardless of accusation status

Fig. 3 Basic Description of the S-ODMRP Protocol

C. *Attack scenarios*

1. No-Attack:
The invader do not execute any action in the network. This represents the ultimate case where the intruders are identified and totally cutoff in the network, and serves as the baseline for calculating the impact of the intruder and the act of our defense.

2. Drop-Only:
The mugger drop data packets, but take part in the protocol correctly otherwise the attack has effect only when mugger are selected in the FORWARDING GROUP.

3. LMM-Drop:
The mugger combine local metric manipulation with the data sinking attack. The attackers conduct the LOCAL METRIC MANIPULATION attack by promoting the same metric they received in JOIN QUERY, which is comparable to making their link metric of the previous hop equal to 1 (best).

4. GMM-Drop:
The mugger combine global metric manipulation with the data sinking attack. The mugger conduct the GLOBAL METRIC MANIPULATION attack by compare a metric of 1 (best) after receiving a JOIN QUERY.

5. False Accusation:
The mugger exploit our accusation mechanism by false accusing random a truthful node at start-up for the whole experiment period in order to reduce the PACKET DELIVERY RATIO.

V. SIMULATION RESULTS

We have concluded that using the S-ODMRP,ETX metrics, and SPP the performance of the network will be

increased and, we have evaluated in terms of parameters such as Throughput, Packet Delivery Ratio(PDR), Drop, and Delay.

Network Structure created is Defined as follows,
a)*Throughput* is defined as the ratio of the total number of transmitted packets to the total number of packets send from the source to the receiver.
b)*Packet Delivery Ratio(PDR)* is defined as the ratio of total number of transmitted packets to the total number of packets send from the source to the receiver.
c)*Delay* is the time taken for a data packets transmitted across a network from source to receiver.
d)*Drop* is the total number of packets dropper when the transmission takes place over a network from source to the receiver.
Throughput is the average rate of successful message delivery over a communication channel. The throughput is measured in bits per second and in data packets per second. The system throughput or throughput is the sum of the data rates that are delivered to all stations in a network.

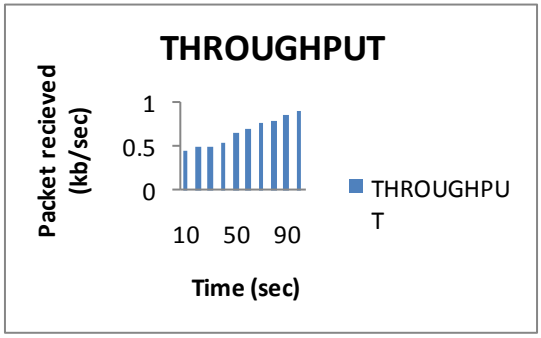

Fig. 4 Packet received versus time

The *packet delivery ratio (PDR)* is classify as the ratio of the number of packets received by the receiver and the number of packets broadcast by the source. Packet delivery ratio is conspire against number of mobile nodes in Once the sender has the receiver's address, it can forward the packet. The way the MAC header of that packet is addressed, depends on the network's topography. It depends on whether the source node and the destination node are separated by a router. This ratio directly change the maximum throughput that the network can maintain. Packet delivery ratio raise with an raise in time for stable nodes.

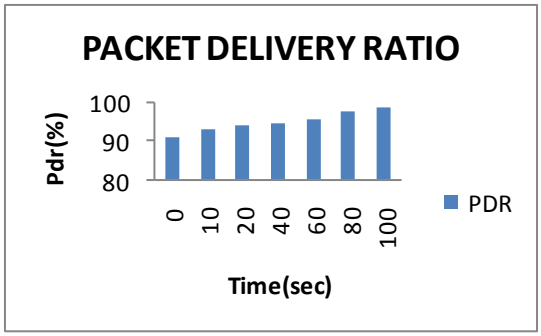

Fig. 5 Packet delivery Ratio with number of nodes
Delay is the time taken for a data transmitted in a network from the source to the receiver.the delay is reduced in the network because of blocking the muggers in the network so the delay will be reduced by the RateGuard mechanism.The delay is calculated by using Time.

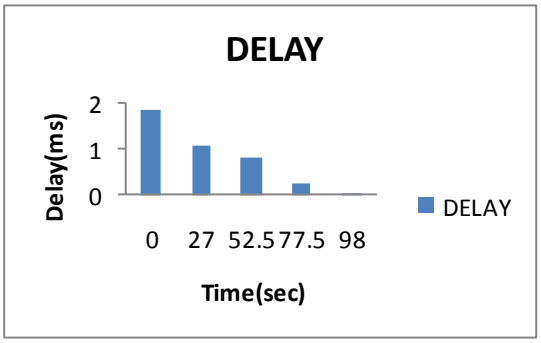

Fig. 6 Delay variation versus time
Packet Drop is the total number of data packets dropped in a network when the transmission takes place from the source to the receiver.The packets are dropped in the network when the attackers are involved in the network and the attackers changes the weights of the link or the node values and shows the values in higher.when the transmission takes place then the attackers will drop the data packets.

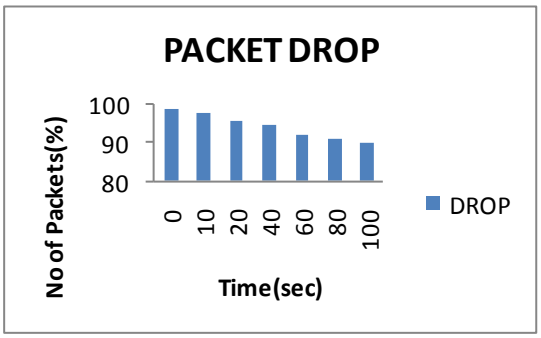

Fig. 7 Number of packets drop versus time

CONCLUSION

After the security is applied to the network to maximizes the throughput in the wireless mesh network.We discover metric manipulation attacks that can give damage to the network.We over comes the challenges with our scheme,Rate Guard mechanism,which will help to detect the intruders in the network.So through analysis and experiments we identifies that the throughput increases in the network and drop is reduced to the maximum.

ACKNOWLEDGMENT

The Author would like to acknowledge the support by Karunya University, Coimbatore.

REFERENCES

[1] J.Dong, R. Curtmola, and C. Nita-Rotaru,''On the Pitfalls of using High-throughput Multicast Metrics in Adversarial Wireless Mesh Network," *Proc.Fifth Ann. IEEE Comm. Soc. Conf.Sensor, Mesh and Ad Hoc Comm. And Networks (SECON'08),* 2008.
[2] Y.B. Ko and N.H. Vaidya, "Flooding-Based Geocasting Protocols for Mobile Ad Hoc Networks*," Mobile Networks and Applications*,vol. 7, no. 6, pp. 471-480, 2002.

[3] R. Chandra, V. Ramasubramanian, and K. Birman, "Anonymous Gossip: Improving Multicast Reliability in Mobile Ad-Hoc Networks," *Proc. 21st IEEE Int'l Conf. Distributed Computing Systems (ICDS '01),* 2001.
[4] Y.-B. Ko and N.H. Vaidya, "GeoTORA: A Protocol for Geocasting in Mobile Ad Hoc Networks," *Proc. Int'l Conf. Network Protocols (ICNP),* pp. 240-250, 2000.
[5] E.L. Ma durga and J.J. Garcia-Luna-Aceves, "*Mobile Networks and Applications*, vol. 6, no. 2, pp. 151-165, 2001.
[6] S.J. Lee, W. Su, and M. Gerla, "On- Demand Multicast Routing Protocol in Multihop Wireless Mobile Network," *Mobile Networks and Applications,* vol. 7, no. 6, pp. 441-453, 2002.
[7] E.M. Royer and C.E. Perkins, "Multicast Ad-Hoc On-Demand Distance Vector (MAODV) Routing," Internet Draft, July 2000.
[8] J.G. Jetcheva and D.B. Johnson, "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks," *Proc.ACM MobiHoc,* 2001.
[9] H. Lundgren, E. Nordstrom, and C. Tschudin, "Coping with Communication Gray Zones in IEEE 802.11b Based Ad Hoc Networks," *Proc. Fifth ACM Int'l Workshop Wireless Mobile Multimedia (WOWMOM '02),* 2002.
[10] D.S.J.D. Couto, D. Agguayo, J.C. Bicket, and R. Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing," *Proc. ACM MobiCom,* 2003.
[11] S. Roy, D. Koutsonikolas, S. Das, and C. Hu, "High-Throughput Multicast Routing Metrics in Wireless Mesh Network," *Proc. 26th IEEE Int'l Conf. Distributed Computing System (ICDCS),* 2006.
[12] A. Chen,D.Lee,G. Chandrasekaran,and P. Sinha, "HIMAC: High Throughput MAC Layer Multicasting in Wireless Networks," *Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor System (MASS'06),* 2006.

Mr. Akuluri Rakesh received his B.E degree from Karunya University in the year 2010. Currently pursuing his master's degree in communication systems. His area of interest includes Wireless Sensor Networks.
Mr. S.R.Jino Ramson received his B.E degree from Karunya University. He received his M.tech from Karunya University. Currently working as Assistant Professor in Karunya University.
Mr. J. John Major received his B.E degree from JACSI College of Engineering, Anna University in the year 2011. Currently pursuing his master's degree in communication systems. His area of interest includes Wireless Sensor Networks, Wireless Mess Networks and Antenna Design. Currently working on trust management in Wireless Sensor Networks.