Sybil Attack In High Throughput Multicast Routing In Wireless Mesh Network

G. Mona Jacqueline[1] and Mrs. Priya Ponnusamy[2]

[1](II M.E., Computer Science And Engineering, Sri Shakthi Institute of Engineering and Technology, Coimbatore)
[2](Assistant Professor, Department of Computer Engineering, Sri Shakthi Institute of Engineering and Technology, Coimbatore)

ABSTRACT

Multicast routing is one in which a source sends data to multiple receivers. Multicast routing uses many types of protocols. In this paper ODMRP protocol is used by slightly modifying it. Instead of using hop count for selecting the route, link quality is used so that high throughput is achieved. Also focus is made on attacks that disrupt routing process by modifying the link value, which are very effective against multicast protocols based on high throughput metrics. Other types of attack such as traffic analysis attack, Sybil attack, eavesdropping, selfish attack etc are not focused. In this paper focus is made on Sybil attack. Sybil attack is defined as an attack, in which a malicious node illegitimately takes on multiple identities by spoofing a legitimate node. Detection of Sybil attack which uses multiple identities can be done by nodes that passively monitor the traffic in the network. One method to detect Sybil attack is Passive Ad hoc Sybil Identity Detection (PASID), where a single node can detect Sybil attacks by recording identities, namely MAC or IP address of other nodes. Overtime the node builds a profile which helps in detecting the Sybil attack.

KEYWORDS:- *Wireless Mesh Network, Multicast Routing, Metric Manipulation Attack, ODMRP Protocol, Sybil attack.*

1. INTRODUCTION:

A wireless mesh network (WMN) is a network that consists of radio nodes that are organized in a mesh topology. A mesh network is highly reliable network as it has multiple routes between the sender and the receiver. When an intermediate node becomes inoperable due to mobility or due to some other reasons, the rest of the nodes can still communicate with the help of other intermediate nodes by creating an alternate route.

Multicast routing is one where data is delivered from a source to multiple destinations. There are various protocols for multicast routing [2], [3] and these protocols were proposed for mobile ad hoc networks (MANETS). The protocols mainly focused on hop counts as routing metric for selecting the route between the source and the receiver. The route having least hop count will be selected. But sometimes this leads to selection of a route having poor quality. Recently protocols were developed based upon a metric, the quality of the link [4], [5]. This is referred as link quality or high throughput metrics.

In high- throughput multicast protocols, the nodes at certain time interval will send probes to its neighbors to measure the link quality. If a node wants to send data, a route discovery process is done. The node estimates the link quality by adding its own cost to its adjacent node’s cost. The route with a high cost i.e., best link quality is selected. Also, this method is efficient only when there are no attackers. The attackers may modify the original cost so that the route including the attacker node is selected.

The protocol chosen for Wireless Mesh Network for multicast routing is On Demand Multicast Routing Protocol(ODMRP), which chooses the path based upon the hop count. Various types of attacks against the mesh are mesh structure attack, metric manipulation attack etc., In addition to this attack, Sybil attack is made focus in this paper. Sybil attack is an attack where an illegitimate node takes the identity of a legitimate node by spoofing the address of the legitimate node. Moreover, the attacker creates a group of nodes. Following are the main concepts focused in this paper:

- Metric manipulation attack causes severe impact on multicast routing and is of two types: local metric manipulation (LMM), global metric manipulation (GMM) [1]
- A technique called RateGuard[1] is proposed to eliminate the attacker. It combines the measurement-based detection and accusation based reaction techniques.
- Sybil attack is detected using the method called Passive Ad hoc Sybil Identity Detection (PASID).

2. HIGH THROUGHPUT MULTICAST ROUTING

Multihop wireless network is considered where each node participates in data forwarding. Wireless mesh network creates a mesh network by connecting the adjacent nodes. Path selection is done based upon the quality of the link in order to maximize throughput.

2.1 High Throughput Metrics

Routing protocols have used hop count as a path selection metric. The focus has shifted toward high-throughput metrics to maximize throughput by selecting paths based on the quality of wireless links. The quality of the link is found by periodic probing. The total link quality of the path is found by aggregating the link quality of all the nodes in that path.

Some of multicast protocol metrics are SPP, which an adaptation of a unicast metric ETX.

ETX metric: ETX metric [6] was proposed for unicast and it estimates the expected number of transmissions needed to successfully deliver a unicast packet over a link, including retransmissions. ETX is calculated for two nodes A and B by using the following formula:

$$ETX = \frac{1}{d_f * d_r}$$

d_f is the probability taken to deliver data in the forward direction and d_r is the probability taken in the reverse direction. The total value is calculated by aggregating all the ETX.

SPP metric: In multicast both directions are not considered as in unicast. Only the forward direction is considered.

$$SPP_i = d_f$$

3. MESH- BASED MULTICAST ROUTING

Here the ODMRP, ODMRP- HT and how to incorporate the link quality metrics in ODMRP- HT are discussed.

3.1 ODMRP overview:

ODMRP is an on-demand multicast routing protocol for multihop wireless networks, which uses a mesh of nodes for each multicast group. Nodes are added to the mesh through a route selection

3.1.2 JOIN QUERY message

The source node periodically re- creates the mesh by flooding a JOIN QUERY message in the network in order to refresh the membership information and update the routes. JOIN QUERY messages are flooded using a basic flood suppression mechanism, which means nodes only process the first received copy of a flooded message. The node receiving the JOIN QUERY message will again forward the message until the message reaches the destination.

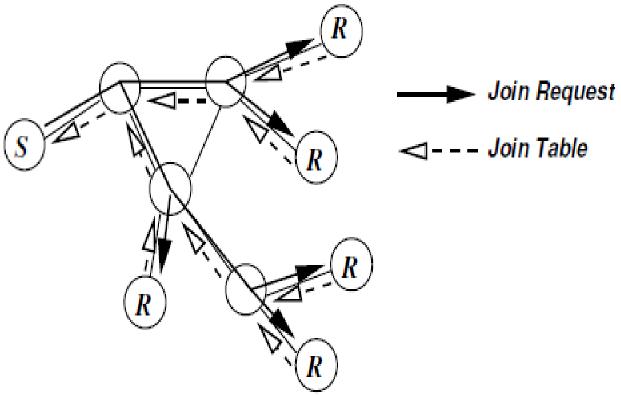

Fig 1: On-Demand Procedure for Membership Setup

3.1.2 JOIN REPLY/ JOIN TABLE message:

When a receiver node gets a JOIN QUERY message, it activates the path from itself to the source node by constructing and broadcasting a JOIN REPLY message that contains entries for each multicast group it wants to join. Each entry has a next hop field filled with the corresponding upstream node. When an intermediate node receives a JOIN REPLY message, it checks if the next hop field of any of the entries in the message matches its own identifier. If so, it makes itself a node part of the mesh (the FORWARDING GROUP) and creates and broadcasts a new JOIN REPLY built upon the matched entries.

Once the JOIN REPLY messages reach the source, the multicast receivers become connected to the source through a mesh of nodes (the FORWARDING GROUP) which ensures the delivery of multicast data. While a node is in the FORWARDING GROUP, it rebroadcasts any non-duplicate multicast data packets that it receives.

3.1.3 Forwarding Group

The forwarding group is a set of nodes that forms a mesh and is capable of forwarding multicast packets. It supports shortest paths between any source and the receiver. All nodes inside the multicast members and forwarding group nodes as shown in fig 2, forward multicast data packets. The multicast receiver can also be a forwarding group node if it is on the path between a multicast source and another receiver as shown in figure 2. The mesh provides richer connectivity among multicast members compared to trees. Flooding redundancy among forwarding group helps overcome node displacements and channel fading. Hence, unlike trees, frequent reconfigurations are not required.

3.2 Incorporating link-quality metrics in ODMRP

To incorporate the new link-quality metrics into ODMRP, the following modification should be done to ODMRP. Each node maintains a NEIGHBOR TABLE that has the costs of the links from its neighbors to itself. The costs are basically a probability value and has a maximum value of one and are periodically updated. In modified ODMRP each node looks up the NEIGHBOR TABLE for the cost of the link from which it received the JOIN QUERY and using this link cost, it updates the cost in the JOIN QUERY packet before rebroadcasting it.

When the JOIN QUERY reaches a receiver, it contains the total cost of the path travelled. The receiver waits for a certain period of time, δ seconds instead of sending JOIN REPLY message immediately on receiving JOIN QUERY message. During this period, it accumulates many duplicate JOIN QUERY packets makes use of the best among them, which is based upon the cost that is the link quality. The path having the highest link quality is selected.

After the expiry of δ seconds, the receiver constructs the JOIN TABLE/ JOIN REPLY message using the stored JOIN QUERY, i.e., the best among all JOIN QUERY packets received during the δ period, and broadcasts the JOIN REPLY to its neighbors

To get high throughput, the forwarding nodes are allowed to forward the duplicate packets. This forwarding is limited to two restrictions. First, a duplicate query is forwarded only if the cost of the path it has traveled is less than that of the minimum cost query received till then. Second, each node sets a timer for a period of $\alpha < \delta$ seconds when it receives the first JOIN QUERY with a particular sequence number. Each node forwards duplicate queries only until the timer of α seconds expires. Choose α as a very small value will lead to minimal path diversity, and a very high value may lead to a high query processing overhead.

3.4 ODMRP- HT:

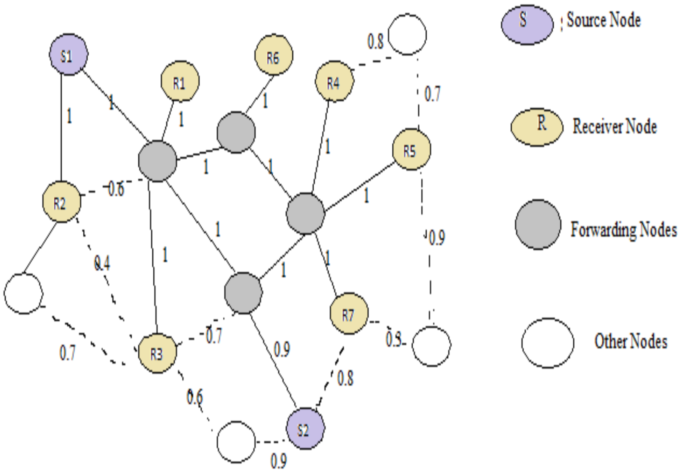

Fig 2: ODMRP-HT Example having two senders and seven receivers. The value on the link is the SPP metric.

In ODMRP- HT, there will be a route cost field, which determines the link quality. This value is probability value having the maximum value one. ODMRP- HT is similar to ODMRP except, ODMRP- HT selects the route based upon the quality of the link and not on hop count. This selection ensures high throughput. When the source receives the JOIN REPLY message, the source will select the route having the high link value. This method is known as weighted flood suppression. The source will also have the alternate routes. If a certain link fails, the source will choose an alternate route.

4. ATTACKS AGAINST HIGH-THROUGHPUT MULTICAST

The attacker when he attack the mesh, can disrupt the multicast data delivery by either consuming the network resource (resource consumption attacks), by causing incorrect mesh establishment (mesh structure attacks), or by dropping packets (data forwarding attacks). The attacker node on the data delivery path simply drops data packets instead of forwarding them. The attacks are described below:

4.1 Mesh Structure Attacks

Mesh structure attacks disrupt the correct establishment of the mesh structure in order to disrupt the data delivery paths. These attacks can be done by malicious manipulation of the JOIN QUERY and JOIN REPLY messages such as sending large number of invalid JOIN QUERY and JOIN REPLY messages.

For the JOIN QUERY messages, the attacker can spoof the source node and inject an invalid JOIN QUERY message, which causes the paths to be built towards the attacker node instead of the correct source node.

For JOIN REPLY messages, the attacker can drop JOIN REPLY messages to cause its downstream nodes to get detached from the multicast mesh. The attacker can also forward JOIN REPLY to an incorrect next hop node to cause an incorrect path being built.

4.2 Resource Consumption Attack

With ODMRP- HT, the JOIN QUERY message is flooded by the nodes to its neighbours. The attacker node will create a JOIN QUERY message or will simply forward with high frequency which will flood the network. Also, the attacker node will inject more number of JOIN QUERY message to flood the network. Addressing such an attack requires admission control mechanisms which can limit the admission and duration of such groups.

4.3 Metric Manipulation Attack

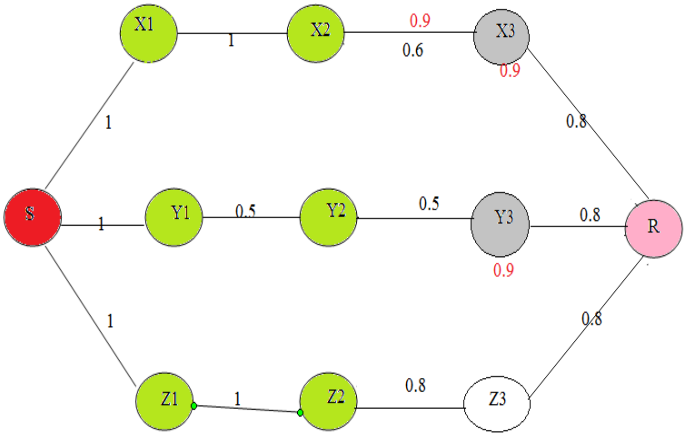

Fig. 3 Example for metric manipulation attack

High throughput multicast routing chooses the route based upon the quality of the link. With metric manipulation attack, the attacker will modify the original link value and will broadcast a false value. There are two types of metric manipulation attack: Local Metric Manipulation(LMM) and Global Metric Manipulation(GMM).

LMM attack: In LMM attack, the attacker will increase the quality of the adjacent link and will broadcast so that the route will be selected along the attacker node. In the above fig, X1 is an attacker. X1 will falsely broadcast the link cost as 0.9 instead of 0.6 so that the route along X1 is selected.

GMM attack: In GMM attack, the attacker instead of broadcasting the adjacent nodes value, will modify the overall accumulated metric and will forward.

5. ATTACK DETECTION AND ELIMINATION

5.1 Measurement based detection

The attack detection is a method that relies on the ability of honest nodes to detect the discrepancy between the expected PDR (ePDR) and the perceived PDR (pPDR). A node can estimate the ePDR of a route from the value of the metric for that route; the node can determine the pPDR for a route by measuring the rate at which it receives data packets from its upstream on that route

If ePDR - pPDR for a route becomes larger than a detection threshold, then nodes suspect that the route is under attack because the route failed to deliver data at a rate with its claimed quality.

5.2 Accusation Based Reaction

A controlled accusation mechanism in which a node, on detecting malicious behavior, temporarily accuses the suspected node by flooding in the network an ACCUSATION message containing its own identity (the accuser node) and the identity of the accused node, as well as the duration of the accusation. As long as the accusation is valid, metrics advertised by an accused node will be ignored and the node will not be selected as part of the FORWARDING GROUP.

5.3 Attack Detection

Attack is detected if there is any variation between ePDR and pPDR.if ePDR- pPDR > δ, then there is an attack. Let n be the number of packets sent by the source and m be the number of packets received by a node in the same period of time. The Wilson estimate requires that n>5, and the confidence interval obtained for pPDR is $(\tilde{p} - e, \tilde{p} + e)$ where

$$\tilde{p} = \frac{m+2}{n+4} \text{ and e = z } \sqrt{\frac{\tilde{p}(1-\tilde{p}}{n+4}}$$

5.4 Attack Reaction

To isolate attackers, protocol uses a controlled accusation mechanism which consists of three components, staggered reaction time-out, accusation message propagation and handling, and recovery message propagation and handling. A react timer is created to act on the adversial node. Based upon this timer the attacker node is accused for a certain period of time.

6. SYBIL ATTACK

Sybil attack is an attack where a node claims multiple identities by spoofing a legitimate node address or ID. In Sybil attack a malicious node behaves as if it were in large number of nodes by impersonating other nodes or simply by claiming false identities**.**

A Sybil attack is one in which an attacker subverts the reputation system network by creating a large number of pseudonymous entities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically.

6.1 Prevention of Sybil Attack

Validation techniques can be used to prevent Sybil attacks and dismiss masquerading hostile entities. A local entity may accept a remote identity based on a central authority which ensures a one-to-one correspondence between an identity and an entity and may even provide a reverse lookup. An identity may be validated either directly or indirectly. In direct validation the local entity queries the central authority to validate the remote identities. In indirect validation the local entity relies on already accepted identities which in turn vouch for the validity of the remote identity in question.

6.2 Detecting Sybil Attack

There are several forms of the Sybil attacks are the distributed storage, routing data aggregation, voting, resource allocation and misbehavior detection. Then present the proposed detection technique for these Sybil attacks. The detection has two versions namely a single observer case and a multi-observer case.

6.2.1 Single Node Observer

The single node observer does not require any active probing of suspected Sybil nodes. It operates effectively on a single node that records the identities of nodes. Nodes that are about to detect will record the identities of all other nodes. The time period required for this recording will be depend on the protocol used. After recording the identities, the following steps will be followed by the node.

1. Calculate A_{ij}, the affinity between nodes i and j, as

$$A_{ij} = (T_{ij} - 2L_{ij})\frac{T_{ij} + 2L_{ij}}{N}$$

where Tij is the number of intervals in which nodes i and j were observed together, Lij is the number of intervals in which either i or j were observed alone, and N is total number of intervals in the observation period.

2. After calculating the affinity, construct a graph in which the vertices as the identities and the unidirected edges are weighted with the affinity values between them. Only edges that are greater than a specific threshold parameter are included. Using our measure of affinity, we recorded our results using a threshold of 0.1.

3. Depth-first search (DFS) is then run over each vertex to discover the connected components. Each of the components found represents a possible Sybil attacker..

6.2.2 Multiple Node Observers

A subset of the legitimate nodes in the network can share observations periodically using the normal data transmission capabilities of the ad hoc network, and that these nodes can trust each other to perform this task honestly. Each node again tracks all other nodes that it hears over many time buckets. At the end of the observation period, it exchanges the information of what identities were heard during what time periods with the other nodes it trusts in the calculations

7. CONCLUSION

ODMRP- HT, the various types of attacks using high throughput metrics in multicast protocols in wireless mesh networks was considered. Various types of attacks such as metric manipulation attacks, Sybil attack were considered.. Also the Sybil attack was considered. This attack can be detected either using single node or multiple node observer. Further, other types of attacks can be considered. As an initial work, ODMRP-HT protocol is developed.

REFERENCES:

[1] Jing Dong, Reza Curtmola, Cristina Nita-Rotaru ”Secure high Throughput Multicast Routing in Wireless Mesh Network”, *IEEE Transactions On Mobile Computing, Vol. 10, No. 5, May 2011*

[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 (ICDCS ’01), 2001.*

[4] S.J. Lee, W. Su, and M. Gerla, “On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks,” *Mobile Networks and Applications, vol. 7, no. 6, pp. 441- 453, 2002.*

[5] D.S.J.D. Couto, D. Aguayo, J.C. Bicket, and R. Morris, “A High-Throughput Path Metric for Multi-Hop Wireless Routing,” *Proc.ACM MobiCom, 2003.*

[6] S. Roy, D. Koutsonikolas, S. Das, and C. Hu, “High- Throughput Multicast Routing Metrics in Wireless Mesh Networks,” *Proc. 26th IEEE Int’l Conf. Distributed Computing Systems (ICDCS),2006.*

[7] Brian Neil Levine, Clay Shields, N. Boris Margolin, “A Survey of Solutions to the Sybil Attack”, *Dept. of Computer Science, Univ. of Massachusetts, Amherst, Dept. of Computer Science, Georgetown University*

[8] John R. Douceur, “The Sybil Attack”, *Microsoft Research.*