ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 5, Issue 1, January 2019

Identification of Malicious Node in Wireless Mesh Network

R. Prashanthi@Punithavathi[1], H. Meharban[2]

Lecturer, Department of Computer Engineering, ADID Polytechnic College, Nagapattinam, India[1]
Lecturer, Department of Electronics and Communication Engineering, ADID Polytechnic College, Nagapattinam, India[2]

ABSTRACT–Malicious node identification with high throughput in multicast routing for wireless mesh networks is a challenging task. Recent work in multicast routing for wireless mesh networks has focused on metrics that estimate link quality to maximizethroughput. Nodes must collaborate in order to compute the path metric and forward data. The assumption that all nodes are honestand behave correctly during metric computation, propagation, and aggregation, as well as during data forwarding, leads to unexpectedconsequences in adversarial networks where compromised nodes act maliciously. Some protocols were proposed mainly in mobile ad hoc network services alsoassume a trusted, non-adversarial environment and do not take security issues into account in their design. Primarily focus on network connectivity and using the number of hops as the route selection metric, this suffers from attacks. To address these challenging task attack should be identified during the metric manipulation is proposed and the attacked node is dropped out. Another path is selected for transmission by considering the link quality, dropping ratio, packet delivery ratio and high throughput in a network.

Keywords – Wireless mesh networks, unicast and multicast routing, high-throughput metrics, dropping ratio

I. INTRODUCTION

A wireless mesh network is a mesh network created through the connection of wireless access points installed at each network user's locale. Each network user is also a provider, forwarding data to the next node. The networking infrastructure is decentralized and simplified because each node need only transmit as far as the next node. It is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one ormore intermediate nodes. A wireless mesh network can be seen as a special type of wireless ad-hoc network. An ad-hocnetwork, on the other hand, is formed ad hoc when wireless devices come within communication range of each other.

Intermediate nodes not only boost the signal, but cooperatively make forwarding decisions based on their knowledge of the network, i.e. perform routing. Such architecture may with careful design provide high bandwidth, spectral efficiency, and economic advantage over the coveragearea. Wireless mesh networks have a relatively stable topology except for the occasional failure of nodes or addition of new nodes. The path of traffic, being aggregated from a large number of end users, changes infrequently.

A. Routing

Routing is required in network environments where multiple segments are patched together over a large area. The segments, which can potentially be different transport media, are linked by routers. No routing is required when nodes are connected to the same network segment, such as a LAN or a point-to-point link. The following two kinds of routing are distinguishable by their different approaches to packet forwarding:

- Unicast routing
- Multicast routing

The unicast routing is to help routers figure out the next hop to pass on packets, along the best path to a target

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 5, Issue 1, January 2019

destination. Choice of the best path is determined by choosing the path with the lowest cost. This best path determination boils down to determination of the data-link or MAC address of the next hop. Each non-directly connected entry in the routing table consists of a prefix, the IP address of the next hop, and the outgoing interface to the next hop.

Actual forwarding may involve extra steps to determine the corresponding data-link address of the next hop from the ARP table or an equivalent address map table for the specific media. If the destination is directly connected, the address resolution retrieves the data-link address of the destination; otherwise, the data-link address of the router at the next hop is obtained.Multicasting is a one-to-many transmission. In contrast, the traditional method of sending messages on the Internet, called uncasing, is a one-to-one transmission. If multicasting is comparable to a conference call, then uncasing is like a private call between two people. Broadcasting is a one-to-all technique in which messages are sent to everybody. Internet routers block broadcasts from propagating everywhere.

Multicasting provides a way for one host to send packets to a selective group of hosts. The key word is "selective." Users choose to be part of a specific multicast. Multicast packets then travel to the user from the multicast source. An important point is that multicast packets only travel across routes where there is an end user that has requested to be part of the multicast. This keeps multicast packets from crossing parts of the network that do not have multicast participants. Still, on the Internet, a multicast group is potentially huge, with members located around the world.

II RELATED WORK

There has been extensive work in the area of secure unicast routing in multihop wireless networks. Examples include [11], [9], [3], [4]. In general, attacks on routing protocols can target either the route establishment process or the data delivery process, or both. Ariadne [13] and SRP [12] propose to secure on-demand source routing protocols by using hop-by-hop authentication techniques to prevent malicious packet manipulations on the route discovery process. SAODV, SEAD [7], and ARAN [11] propose to secure on-demand distance vector routing protocols by using one-way hash chains to secure the propagation of hop counts. A secure link state routing protocol proposed in [8] ensures the correctness of link state updates with digital signatures and one-way hash chains. To ensure correct data delivery, [9] proposes the watchdog and path rater techniques to detect adversarial nodes by having each node monitor if its neighbors forward packets correctly. SMT [2] and Ariadne [4] use multipath routing to prevent malicious nodes from selectively dropping data. ODSBR [5], [8] provides resilience to colluding Byzantine attacks by detecting malicious links based on an end-to-end acknowledgment-based feedback technique.

Besides attacks on the routing layer, wireless networks are also subject to wireless-specific attacks, such as flood rushing and wormhole attacks. Defenses against these attacks have been extensively studied in previous work, e.g., [13], [8] and are complementary to our protocol. RAP prevents the rushing attack by waiting for several flood requests and then randomly selecting one to forward, rather than always forwarding only the first one. Techniques to defend against wormhole attacks include Packet Leashes [7] which restricts the maximum transmission distance by using time or location information, Truelink [8] which uses MAC level acknowledgments to infer if a link exists or not between two nodes, and the work in [9], which relies on directional antennas.

III EXISTING METHOD

A multihop wireless network is considered, where nodes participate in the data forwarding process for other nodes. Assume a mesh-based multicast routing protocol, which maintains a mesh connecting multicast sources and receivers. Path selection is performed based on a metric designed to maximize throughput. Below, we provide an overview of high-throughput metrics for multicast, and then describe in details how such metrics are integrated with mesh-based multicast protocols.

A. Mesh - Based Multicast Routing With High Throughput

We focus on ODMRP as a representative mesh-based multicast protocol for wireless networks. Below, we first give an overview of ODMRP, and then describe how it can be enhanced with any link-quality metric. The protocol extension to use a high-throughput metric was first described by Roy et al. We refer to the ODMRP protocol using a high-throughput metric as ODMRP-HT in order to distinguish it from the original ODMRP protocol. 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 and activation protocol. The source periodically recreates the mesh by flooding a JOIN QUERY message in the network in order to refresh the membership information and

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 5, Issue 1, January 2019

update the routes. We use the term round to denote the interval between two consecutive mesh creation events. [10] discussed that the activity related status data will be communicated consistently and shared among drivers through VANETs keeping in mind the end goal to enhance driving security and solace. Along these lines, Vehicular specially appointed systems (VANETs) require safeguarding and secure information correspondences. Without the security and protection ensures, the aggressors could track their intrigued vehicles by gathering and breaking down their movement messages. A mysterious message confirmation is a basic prerequisite of VANETs. To conquer this issue, a protection safeguarding confirmation convention with expert traceability utilizing elliptic bend based chameleon hashing is proposed. Contrasted and existing plans Privacy saving confirmation utilizing Hash Message verification code, this approach has the accompanying better elements: common and unknown validation for vehicle-to-vehicle and vehicle-to-roadside interchanges, vehicle unlinkability, specialist following capacity and high computational effectiveness

JOIN QUERY messages are flooded using a basic flood suppression mechanism, in which nodes only process the first received copy of a flooded message. When a receiver node gets a JOIN QUERY message, it activates the path from itself to the source 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 knows whether it is on the path to the source or not, by checking if the next hop field of any of the entries in the message matches its own identifier.

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 no duplicate multicast data packets that it receives. ODMRP takes a “soft state” approach in those nodes put a minimal effort to maintain the mesh. To leave the multicast group, receiver nodes are not required to explicitly send any message, instead they do not reply to JOIN QUERY messages. Also, a node’s participation in the FORWARDING GROUP expires if its forwarding node status is not updated.

We now describe ODMRP-HT, a protocol that enhances ODMRP with high-throughput metrics. The main differences between ODMRP-HT and ODMRP are: 1) instead of selecting routes based on minimum delay (which results in choosing the fastest routes), ODMRP-HT selects routes based on a link-quality metric, and 2) ODMRP-HT uses a weighted flood suppression mechanism to flood JOIN QUERY messages instead of using basic flood suppression.

B. Attacks Against High-Throughput Multicast

In this section, we present attacks against high-throughput multicast protocols. In particular, we focus on attacks that exploit vulnerabilities introduced by the use of high throughput metrics. These attacks require little resource from the attacker, but can cause severe damage to the performance of the multicast protocol. We first present the adversarial model, followed by the details of the attacks.Malicious nodes may exhibit Byzantine behaviour, either alone or in collusion with other malicious nodes. Some examples of Byzantine behaviour are as follows: Dropping, Injecting, Modifying, Replaying, or rushing packets, and creating wormholes Attacks the attacker can achieve the goal of disrupting the multicast data delivery by either exhausting network resource , by causing incorrect mesh establishment, or by dropping packets. The types of attacks are:

- Resource consumption attacks,
- Mesh structure attacks,
- Data forwarding attacks.

Resource Consumption Attacks: ODMRP-HT floods JOIN QUERY messages in the entire network, allowing an attacker to inject either spoofed or its own legitimate JOIN QUERY messages at a high frequency to cause frequent network wide flooding. The attacker can also activate many unnecessary data paths by sending many JOIN REPLY messages to cause unnecessary data packet forwarding. Finally, the attacker can inject invalid data packets to be forwarded in the network. If the attackers are insider nodes, an effective attack is to establish a legitimate group session with high data rate in order to deprive the network resource from honest nodes. Addressing such an attack requires admission control mechanisms, which can limit the admission and duration of such groups.

Mesh structure attacks disrupt the correct establishment of the mesh structure in order to disrupt the data delivery paths. These attacks can be mounted by malicious manipulation of the JOIN QUERY and JOIN REPLY messages. For the JOIN QUERY messages, the attacker can spoof the source node and inject invalid JOIN QUERY messages, which can cause paths to be built toward the attacker node instead of the correct source node. The attackers may also act in a selfish manner by dropping JOIN QUERY messages, which allows them to avoid participation in the multicast protocol.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 5, Issue 1, January 2019

Since JOIN QUERY messages are flooded in the network, unless the attacker nodes form a vertex cut in the network, they cannot prevent legitimate nodes from receiving JOIN QUERY messages. For the JOIN REPLY messages, the attacker can drop JOIN REPLY messages to cause its downstream nodes to be 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.

C. Metric Manipulation Attacks

Multicast protocols using high throughput metrics prefer paths to the source that are perceived as having high quality, while trying to avoid low quality paths. Thus, a good strategy for an attacker to increase its chances of being selected in the FORWARDING GROUP is to advertise artificially good metrics for routes to the source. The types of metric manipulation attacks are:

- Local metric manipulation (LMM)
- Global metric manipulation (GMM)

Local Metric Manipulation: An adversarial node artificially increases the quality of its adjacent links, distorting the neighbors' perception about these links. The falsely advertised "high quality" links will be preferred and malicious nodes have better chances to be included on routes. A node can claim a false value for the quality of the links toward itself. A malicious node C1 claims that SPPs↔c1=0.9 instead of the correct metric of 0.6. Thus, C1 accumulates a false local metric for the link B1↔C1 and advertises to R the metric SPPs↔c1=0.9 instead of the correct metric SPPs↔c1=0.6. The route S-A1-B1-C1-R will be chosen over the correct route S-A3-B3-C3-R.

Global Metric Manipulation: In a GMM attack, a malicious node arbitrarily changes the value of the route metric accumulated in the flood packet, before rebroadcasting this packet. A GMM attack allows a node to manipulate not only its own contribution to the path metric, but also the contributions of previous nodes that were accumulated in the path metric. The attacker C2 should advertise a route metric of 0.25, but instead advertises a route metric of 0.9 to node R. This causes the route S-A2-B2-C2-R to be selected over the correct route S-A3-B3-C3-R. The danger of metric manipulation attacks comes from the epidemic attack propagation due to the epidemic nature of metric derivation. As a result, even a few numbers of attackers can "poison" the metrics of many nodes in the network and create powerful black holes that attract and control the traffic to many receivers.

IV PROPOSED METHOD

We measure the performance of data delivery sing the PDR, defined as the ratio between the average numbers of packets received by all receivers to the number of packets sent by the source.

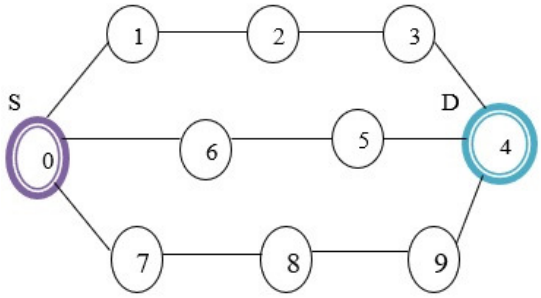

Figure 1 Single source and destination

In figure 1, single source node and destination node are considered in the network for transmission. The source node sends packets to the destination node through the intermediate node 1, 2 and 3. If the attacked node is identified, then the source node will automatically select the alternate path for transmitting the packets. The attacked node will be identified by the high packet drops during transmission. The server node monitors the process and will intimate all other nodes about the attacked node. Finally the attacked node will be moved from the coverage.

V EXPERIMENTAL RESULTS

Now we evaluate the performance of TAM algorithm. The algorithm is implemented in ns-2. In our simulations, we use 30 nodes. The network area is 1500m* 1500m, the transmission rate is 54 Mbps, and the communication range is 240m by default. Here, using Omni directional antennas by all nodes.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 5, Issue 1, January 2019

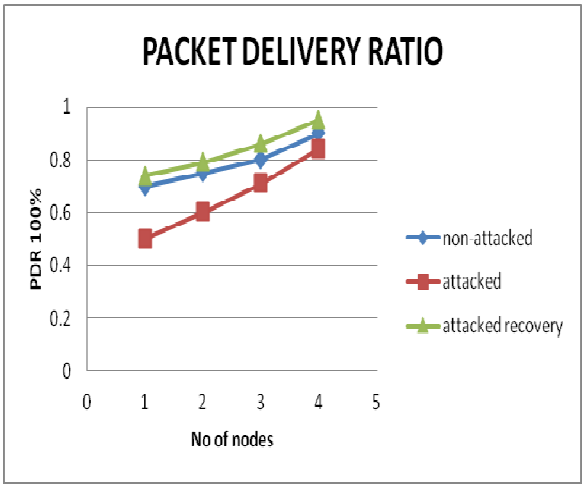

Figure 5 Packet delivery analyses

Figure 5 shows the packet delivery ratio, in this defining sequence numbers with the received packets. Packet delivery ratio is obtained by dividing the number of data packets correctly received by the destinations by the number of data packets originated by the sources. Packet delivery ratio is defined as the ratio of packets delivered to the destination to those generated by the CBR sources. The analysis shows that the packet delivery ratio is 0.95 for attacked recovery, comparing the attacked metric and nonattacked metric with attack recovery metric its packet delivery ratio is high for attacked recovery. [6] discussed because of various appealing focal points, agreeable correspondences have been broadly viewed as one of the promising systems to enhance throughput and scope execution in remote interchanges. The hand-off hub (RN) assumes a key part in helpful interchanges, and RN determination may considerably influence the execution pick up in a system with agreeable media get to control (MAC). In this paper, we address the issue of RN choice while considering MAC overhead, which is brought about by handshake motioning as well as casing retransmissions because of transmission disappointment too. We outline a helpful MAC component with our ideal RN determination calculation, which is called ideal hand-off choice MAC, and utilize a hypothetical model. To investigate the collaboration execution picks up. We direct recreation tests in view of Network Simulator To assess our proposed agreeable MAC. Numerical outcomes approve the adequacy of our investigative model and demonstrate that our composed MAC fundamentally outflanks existing agreeable MAC components that don't consider retransmission MAC overhead

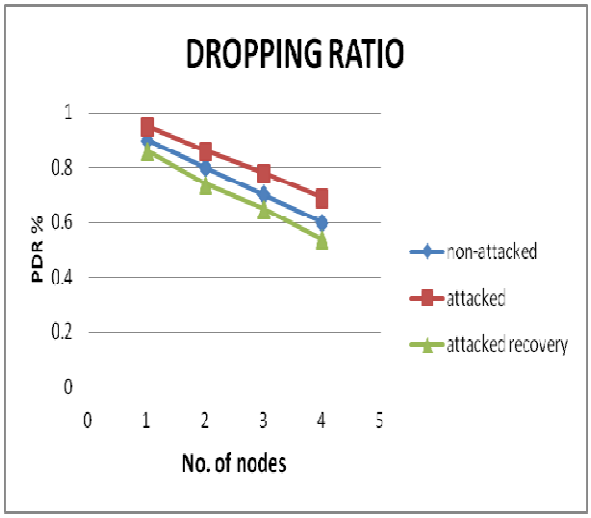

Figure 6 Dropping ratio analyses

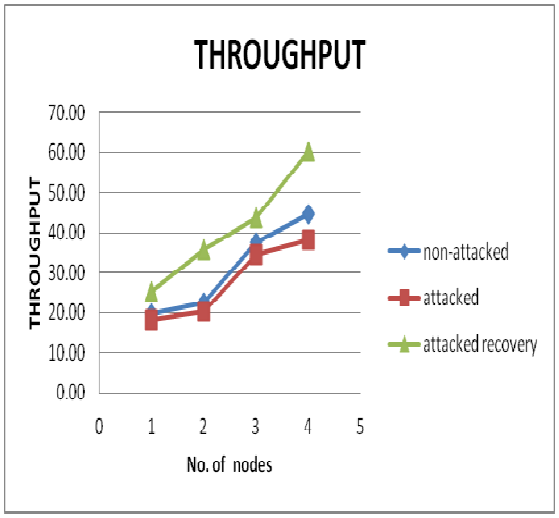

Figure 7: Throughput analyses

In figure 6 dropping ratio is shown between number of sources and destination and PDR in percentage.The above graph shows the comparison of throughput between nonattacked network, attacked network and attack recovery network. Throughput is high for attack recovery network. Throughput is defined as the

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 5, Issue 1, January 2019

number of packets received divided by the time. The attacked and non attacked node may have the more packet drops with respect to the time.

VI CONCLUSION

We considered the security implication of using high throughput metrics in multicast protocols in wireless mesh networks. In particular, we identified metric manipulation attacks that can inflict significant damage on the network. The attacks not only have a direct impact on the multicast service, but also raise additional challenges in defending against them due to their metric poisoning effect. We demonstrate through analysis and experiments that our path metric manipulation is effective against the identified attacks, resilient to malicious exploitations, and imposes a small overhead.

REFERENCES

[1] Adya.A, P. Bahl, J. Padhye, A. Wolman, and L. Zhou, "A MultiRadio Unification Protocol for IEEE 802.11 Wireless Networks," Proc. First Int'l Conf. Broadband Networks (BroadNets '04), 2004

[2] Curtmola.R and C. Nita-Rotaru, "BSMR: Byzantine-Resilient Secure Multicast Routing in Multi-Hop Wireless Networks," IEEE Trans. Mobile Computing, vol. 8, no. 4, pp. 445-459, Apr. 2009.

[3] Dong.J, R.Curtmola, and C.Nita-Rotaru, "On the Pitfalls of Using High-Throughput Multicast Metrics in Adversarial Wireless Mesh Networks," Proc. Fifth Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '08), 2008.

[4] Draves.R, J. Padhye, and B. Zill, "Routing in Multi-Radio, MultiHop Wireless Mesh Networks," Proc. ACM MobiCom, 2004.

[5] Draves.R, J. Padhye, and B. Zill, "Comparison of Routing Metrics for Static Multi-Hop Wireless Networks," Proc. ACM SIGCOMM, 2004.

[6] Christo Ananth, Dr. G. Arul Dalton, Dr.S.Selvakani, "An Efficient Cooperative Media Access Control Based Relay Node Selection In Wireless Networks", International Journal of Pure and Applied Mathematics, Volume 118, No. 5, 2018,(659-668).

[7] Jetcheva.J.G and D.B. Johnson, "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks," Proc. ACM MobiHoc, 2001.

[8] Ko.Y.B 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.

[9] Marti.S, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom, Aug. 2000.

[10] Christo Ananth, Dr.S. Selvakani, K. Vasumathi, "An Efficient Privacy Preservation in Vehicular Communications Using EC-Based Chameleon Hashing", Journal of Advanced Research in Dynamical and Control Systems, 15-Special Issue, December 2017,pp: 787-792.

[11] Sanzgiri.K, B. Dahill, B.N. Levine, C. Shields, and E. BeldingRoyer, "A Secure Routing Protocol for Ad Hoc Networks," Proc. 10th IEEE Int'l Conf. Network Protocols (ICNP), 2002.

[12] Roy.S, V.G. Addada, S. Setia, and S. Jajodia, "Securing MAODV: Attacks and Countermeasures," Proc. Second Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '05), 2005.

[13] Roy.S, D. Koutsonikolas, S. Das, and C. Hu, "High-Throughput Multicast Routing Metrics in Wireless Mesh Networks," Ad Hoc Networks, vol. 6, no. 6, pp. 878-899, 2007.