ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

TRACKING ATTACKS IN MULTICAST ROUTING THROUGH WIRELESS MESH NETWORKS

M.Yamuna Devi[1], S.Aishwarya[2], R.Hemaltha[3], J. Vijitha Ananthi[4]

Graduate, Electronics and Communication Engineering, Indus College of Engineering, Coimbatore, India[1]

Graduate, Electronics and Communication Engineering, Indus College of Engineering, Coimbatore, India[2]

Graduate, Electronics and Communication Engineering, Indus College of Engineering, Coimbatore, India[3]

Assistant Professor, Electronics and Communication Engineering, Indus College of Engineering, Coimbatore, India[4]

ABSTRACT - **Identifying the attacks with high throughput in multicast routing for wireless mesh networks is a challenging task. Recently many protocols were proposed for mobile ad hoc network. Focusing primarily 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, packet delivery ratio, dropping ratio, packet delivery ratio-decrease ratio and high throughput with four sources and destinations in the same network and they are compared.**

Keywords – Wireless mesh networks, metric manipulation attacks, high-throughput metrics, and packet delivery decrease 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. Wireless mesh networking could allow people living in remote areas and small businesses operating in rural neighborhoods to connect their networks together for affordable Internet connections.

A. *Unicasting and Multicasting*

Routing is required in network environments where multiple segments are patched together over a large area. 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 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. 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. Multicasting provides a way for one host to send packets to a selective group of hosts. 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.

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],[1]. 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 [10], 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. SMT [2] and Ariadne [4] use multipath routing to prevent malicious nodes from selectively dropping data. ODSBR [5], [8], [6] provides resilience to colluding Byzantine attacks by detecting malicious links based on an end-to-end acknowledgment-based feedback technique.

In contrast to secure unicast routing, the work studying security problems specific to multicast routing in wireless networks is particularly scarce, with the notable exception of the work by Roy et al. [12] and BSMR [2]. An authentication framework proposed in [12] prevents outsider attacks in a tree-based multicast protocol, MAODV [7], while BSMR [2] complements the work in [12] and presents a measurement-based technique that addresses insider attacks in tree-based multicast protocols. A key point to note is that all of the above existing work in either secure unicast or multicast routing considers routing protocols that use only basic routing metrics, such as hop count and latency. None of them consider routing protocols that incorporate high-throughput metrics.

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.

A. High - Throughput Mesh Based Multicast Routing

ODMRP is a representative mesh-based multicast protocol for wireless network. 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 update the routes. We use the term round to denote the interval between two consecutive mesh creation events. 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. 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 Routing

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. 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.

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. 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. 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. 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.

IV. PROPOSED METHOD

Measure the performance of data delivery using 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. We also measure the strength of the attacks using as metric the PDR decrease ratio (PDR-DR), defined as

$$\text{PDRDR} = \frac{\alpha - \beta}{\alpha}$$

Where α and β represent the PDR when the network is not under attack and under attack, respectively.

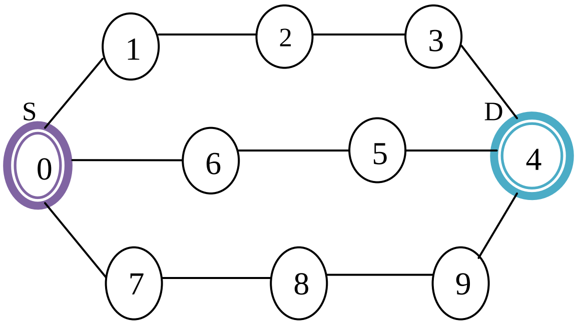

Figure 1 Single source and destination

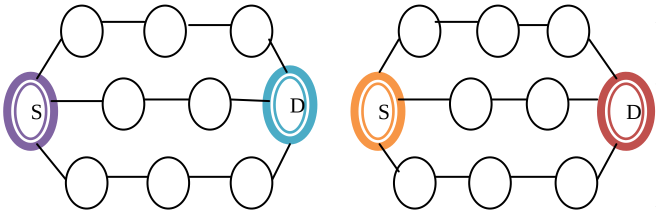

Figure 2 Two sources and destination

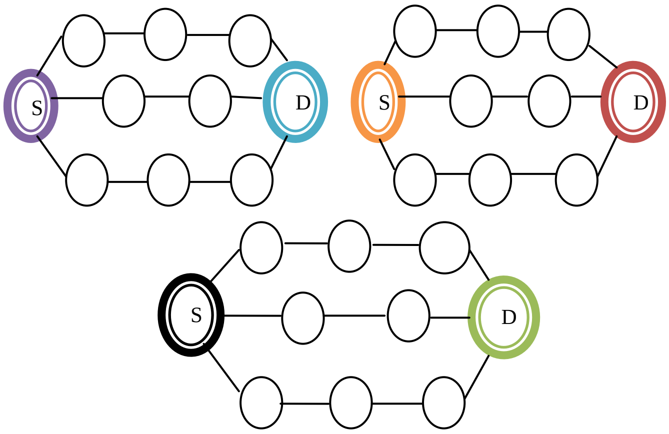

Figure 3 Three sources and destination

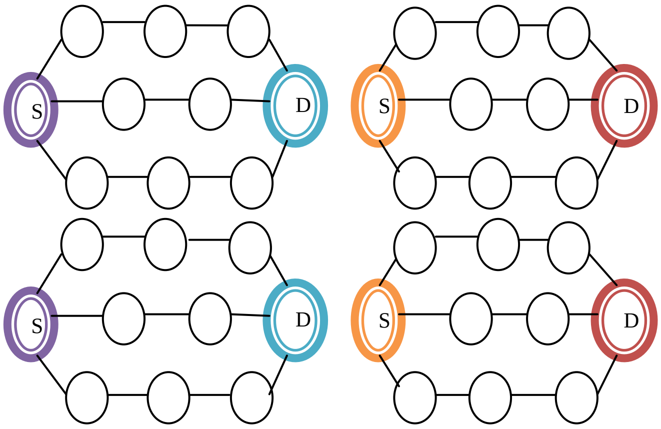

Figure 4 Four sources and destination

A. *Algorithm*

1. Connected graph G(V,€)
2. S← G(V,€) (Source)
3. C← G(V,€) (Destination)
4. T ← G(V,€) (Intermediate node)
5. S→T→C
6. T→ Attacked, S selects V
7. V→ Another intermediate node ← G(V,€)

Algorithm explains that G (V, €) is a whole network which is our input and 'S' is our source's' is our destination in the network G (V, €) and 'T' is our intermediate node. Source node S sends packets to destination node through T. If the intermediate node T gets attacked, so the source node S selects the alternate path to transmit packets. V is the alternate intermediate node in the network G (V, €). The server node will find the attacked node by indentifying the more number of packet drops and will choose the alternate path for transmission.

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. Two sources and destination is considered in a network for transmission which is shown in fig 2. The throughput is increased comparing the existing method. In existing method number of attackers is considered whereas here we considering the number of sources and destination in the same network. Likewise we are considering three and four sources and destinations in the same network for transmission shown in figure 3 and figure 4.

V. EXPERIMENTAL RESULTS

Now we evaluate the performance of TAM algorithm. The algorithm is implemented in ns-2. In our simulations, we use 65 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.

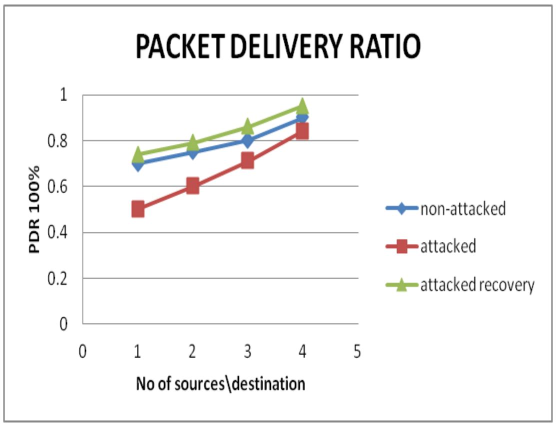

Figure 5 Packet delivery analyses

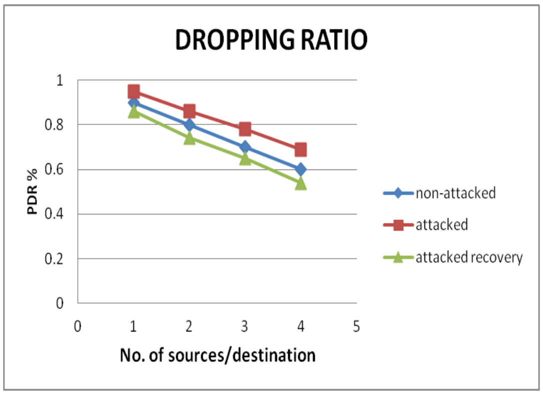

Figure 6 Dropping ratio analyses

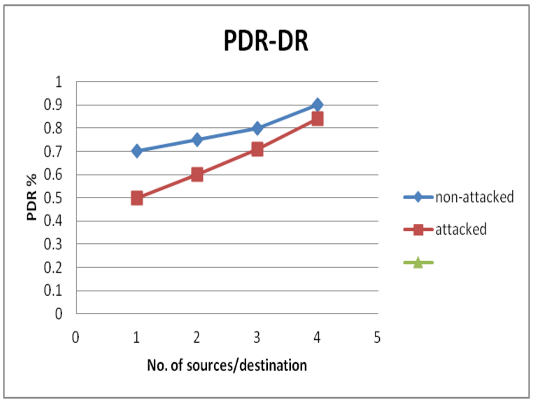

Figure 7 Packet delivery ratios – decrease ratio

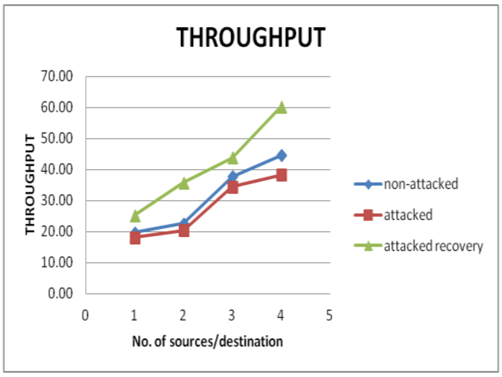

Figure 8: Throughput analyses

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.

In figure 6 dropping ratio is shown between number of sources and destination and PDR in percentage. The analysis shows the dropping ratio between the nonattacked node, attacked node and attack recovery node in a network.
The dropping ratio for attack recovery in four source and destination is 0.54 where as for attacked node network is 0.69 and for nonattacked node is 0.6. Figure 7: shows the number of sources and destination and PDR percentage. Packet delivery ratio decrease ratio is defined as the ratio between the difference of packet delivery ratio of non attacked and packet delivery ratio of attacked to the packet delivery ratio of attacked.

Comparing the PDR decrease ratio of attacked and nonattacked network, PDRDR is high for non attacked network. Below graph shows the comparison of throughput between the nonattacked, attacked network and attack recovery network. Throughput is high for attack recovery network. Throughput is defined as the 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] Hu. Y.-C, A. Perrig, and D.B. Johnson, “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols,” Proc. Second ACM Workshop Wireless Security (WiSe), 2003.

[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] Newsome.J, E. Shi, D. Song, and A. Perrig, “The Sybil Attack in Sensor Networks: Analysis & Defenses,” Proc. Third Int’l Symp. Information Processing in Sensor Networks (IPSN ’04), 2004.

[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.

BIOGRAPHY

Ms. M.Yamuna Devi received B.E degree in Electronics and communication from SNS College of Technology, in 2008. Since July 2011, she has been a student of M.E in Applied Electronics in Indus College of Engineering, Coimbatore. Her research Interest includes in Communication and Wireless networks.

Ms. S.Aishwarya received B.E degree in Electronics and Communication from SNS College of Technology, in 2008. Since July 2011, she has been a student of M.E in Applied Electronics in Indus College of Engineering, Coimbatore. Her research Interest includes in communication and networks.

Ms. R.Hemalatha received B.E degree in Electronics and Communication from SNS College of Technology, in 2008. Since July 2011, she has been a student of M.E in Applied Electronics in Indus College of Engineering, Coimbatore. Her research Interest includes Qos in wireless networks.

Ms. J. Vijitha Ananthi received B.E degree in Electronics and Communication from Anna University, in 2010 and Master’s Degree in communication System from Karunya University, India. Currently she is working as an Assistant Professor at Indus College of Engineering, Coimbatore, India. Her interests are in overlay in Wireless Networks.