ATLANTIS PRESS
Advances in Engineering Research (AER), volume 142
International Conference for Phoenixes on Emerging Current Trends in Engineering and Management (PECTEAM 2018)

Secure on Demand Multicast Routing for Network Attacks in Wireless Mesh Network

[1]S.Balaji, [2]T.Sasilatha
[1]Research Scholar, Anna University,Chennai,India
[2]Professor and Head, Department of ECE, Srisastha Institute of Engineering and Technology, Chennai, India
balajiit@gmail.com, sasi_saha@yahoo.com

***Abstract*—Multicast routing in wireless mesh networks can be accomplished based on link quality metrics to maximize throughput. Nodes must collaborate in order to compute the path metric and forward data. The assumption that all nodes are honest and behave correctly during metric computation, propagation, and aggregation, as well as during data forwarding, leads to unexpected consequences in adversarial networks where compromised nodes act maliciously. In this work, novel attacks against high throughput multicast protocols in wireless mesh networks. The attacks exploit the local estimation and global aggregation of the metric to allow attackers to attract a large amount of traffic. We show that these attacks are very effective against multicast protocols based on high-throughput metrics. Aggressive path selection is a double-edged sword: While it maximizes throughput, it also increases attack effectiveness in the absence of defense mechanisms. Approach to defend against the identified attacks combines measurement based detection and accusation based reaction techniques based on packet delivery ratio and throughput.**

***Index Terms*—Routing, wireless networks, multicast, Network security , mesh network.**

I. INTRODUCTION

Multicast routing protocols deliver data from a source to multiple destinations organized in a multicast group. In the last few years, several protocols were proposed to provide multicast services for multi hop wireless networks. These protocols were proposed for mobile ad hoc networks (MANETs), focusing primarily on network connectivity and using the number of hop as the route selection metric. However, it has been shown that using hop count as routing metric can result in selecting links with poor quality on the path, negatively impacting the path throughput. Instead, given the stationary nature of WMNs, recent protocols focus on maximizing path throughput by selecting paths based on metrics that capture the quality of the wireless links. Such metrics are considered as link-quality metrics or high-throughput metrics, and to protocols using such metrics as high-throughput protocols. In a typical high-throughput multicast protocol, nodes periodically send probes to their neighbors to measure the quality of their adjacent links. During route discovery, a node estimates the cost of the path by combining its own measured metric of adjacent links with the path cost accumulated on the route discovery packet. The path with the best metric is then selected. High-throughput protocols require the nodes to collaborate in order to derive the path metric, thus relying on the assumption that nodes behave correctly during metric computation and propagation. However, this assumption is difficult to guarantee in wireless networks that are vulnerable to attacks coming from both insiders and outsiders, due to the open and shared nature of the medium and the multi hop characteristic of the communication. An aggressive path selection introduces new vulnerabilities and provides the attacker with an increased arsenal of attacks leading to unexpected consequences. For example, adversaries may manipulate the metrics in order to be selected on more paths and to draw more traffic, creating opportunities for attacks such as data dropping and mesh partitioning, or traffic analysis. Although there has been extensive work on using high throughput metrics to improve performance in wireless networks, work studying the security implications of this choice is relatively scarce. Previous work primarily focused on vulnerabilities of unicast routing protocols that use hop count as a metric and secure wireless multicast was less studied, and the existing work focused primarily on using hop count metric in tree-based protocols.

II. RELATED WORK

In this section, basic procedures assumed in conventional multicast protocols are to be summed, and then introduce a few multicast algorithms proposed in the literature. There has been extensive work in the area of secure unicast routing in multi hop wireless networks. Examples include in general, attacks on routing protocols can target either the route establishment process or the data delivery process, or both. Ariadne and SRP 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. A secure link state routing protocol proposed in ensures the correctness of link state updates with digital signatures and one-way hash chains. To ensure correct data delivery, watchdog technique to detect adversarial nodes by having each node monitor if its neighbors forward packets correctly. ODSBR 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. An authentication framework prevents outsider attacks in a tree-based multicast protocol, MAODV, while BSMR complements the work 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, which have been shown to be critical for achieving high performance in wireless networks.

On the contrary, many existing works even have to remove important performance optimizations in existing protocols in order to prevent security attacks. There are also a few studies on secure QoS routing in wireless networks. However, they require strong assumptions, such as symmetric links, correct trust evaluation on nodes, ability to correctly determine link metrics despite of attacks. In addition, none of them consider attacks on the data delivery phase. To the best of the knowledge, this work is the first work that encompasses both high performance and security as goals in multicast routing and considers attacks on both path establishment and data delivery phases.

III. Contribution Of This Work

A class of severe attacks is identified against multicast protocols that exploit the use of the high throughput metrics in mesh, including local metric manipulation (LMM) and global metric manipulation (GMM). 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 GMM attackers can cause the same attack impact as 20 packet dropping attackers. Secondly a secure high throughput multicast protocol S-ODMRP is proposed that incorporates a novel defense scheme Rate Guard. Rate Guard combines measurement-based detection and accusation-based reaction techniques to address the metric manipulation and packet dropping attacks. To prevent attackers from exploiting the defense mechanism itself, Rate Guard limits the number of accusations that can be generated by a node. Rate Guard also adopts a temporary accusation mechanism that accommodates false positive accusations that may be caused by transient network variations. Finally a detailed security analysis and establish bounds on the impact of the attacks under the proposed defense scheme is performed. Extensive simulations confirm our analysis and show that our strategy is very effective in defending against the attacks, while incurring a low overhead

IV. Secure Multicast Routing In Mesh Network

In this section, Secure on Demand Multicast Routing Protocol is described in details. Secure on demand multicast routing protocol ensures the delivery of data from the source to the multicast receivers even in the presence of Byzantine attackers, as long as the receivers are reachable through non adversarial paths. To achieve this the protocol uses a combination of authentication and rate limiting techniques against resource consumption attacks and a novel technique, Rate Guard, against the more challenging packet dropping and mesh structure attacks, including metric manipulations and JOIN REPLY dropping. Secure on demand multicast routing protocol uses source message authentication to avoid processing non authenticated messages. This eliminates a large class of attacks, including outsider attacks, message spoofing and modification attacks targeting JOIN QUERY and JOIN REPLY messages, and the injection of corrupted data packets.

Source Authentication - We assume that each user authorized to be part of the mesh network has a pair of public and private keys and a client certificate that binds its public key to a unique user identifier. This defends against external attacks from nodes that are not part of the network. We assume source data is authenticated, so that receivers can distinguish authentic data from spurious data. Efficient source data authentication can be achieved with existing schemes such as TESLA

Mesh Creation - Mesh creation follows the same pattern like source node periodically broadcasts to the entire network a JOIN QUERY message in order to refresh the membership information and to update the routes. The JOIN QUERY message is signed by source and is propagated using a weighted flood suppression mechanism. Nodes only process JOIN QUERY messages that have valid signatures and that are received from nodes not currently accused. Nodes record the upstream node and the metric corresponding to the route with the best metric as best upstream and best metric. The JOIN REPLY messages are then sent from receivers back to source along optimal paths as defined by the high throughput metric, leading to the creation of the FORWARDING GROUP. After sending a JOIN REPLY to its best upstream, a node starts to monitor the PDR from its best upstream in order to measure its perceived PDR.

To address attackers that strategically accuse certain nodes in order to disconnect the network, we make one exception from the rule that only non accused nodes are included in the FORWARDING GROUP: If the best metric is advertised by an accused neighbor, a node also activates this neighbor in addition to the best non accused neighbor. This ensures that good paths are still utilized, even if honest nodes on these paths are falsely accused. The additional transmissions are kept to a minimum because the neighbors with the best and second best metric usually share the same upstream node.

A. *Mesh Creation Algorithm*

Executed at the source **node to initiate a new JOIN QUERY message:**
1: create a JOIN QUERY message q
2: q.source = source_id; q.from = source_id
3: q.path_metric = 1; q.seq = join_seq
4: join_seq + +
5: Sign(q); Broadcast(q)

Executed at a node upon receipt of a JOIN QUERY message q:
6: **if** (latest_received_join_seq > q.seq) **then**
7: **return** // ignore old queries
8: Verify(q.from, q.sig)
9: get_new_query = FALSE
10: **if** (latest_received_join_seq < q.seq) **then**
11: // get a new (non-duplicate) query
12: latest_received_join_seq = q.seq
13: best_metric = 0
14: best_upstream = INVALID_NODE
15: fastest_upstream = q.from // for fallback recovery
16: get_new_query = TRUE
17: received_queries.insert(q) // store the query
18: **if** (accusation_list.contains_accused_node(q.from)) **then**
19: q.path_metric = 0
20: **else**
21: q.path_metric = q.path_metric × Link_metric(q.from)
22: **if** (get_new_query OR q.path_metric > best_metric) **then**
23: best_upstream = q.from; best_metric = q.path_metric;
24: q.from = node_id
25: Sign(q); Broadcast(q)
26: **if** (get_new_query AND is_receiver) **then**
27: Start_timer(reply_timer, REPLY_TIMEOUT)

Executed at a node upon timeout of reply_timer**:**
28: Send_reply()

Executed at a node upon receipt of a JOIN REPLY message r:
29: **if** (latest_received_reply_seq < r.seq) **then**
30: latest_received_reply_seq = r.seq
31: Refresh_timer(FG_timer, FG_TIMEOUT)
32: **if** (not is_receiver) **then**
33: Send_reply()

Send_reply()
34: create a JOIN REPLY message r
35: r.seq = latest_received_join_seq
36: Send_message(r, best_upstream)
37: **if** (best_metric > 0) **then**
38: start monitoring the PDR of best_upstream
39: **if** (Get_best_metric(received_queries) > best_metric) **then**
40: // Activate the accused neighbor with best metric
41: Send_message(r, Get_neighbor_best_metric(received_queries))
42: received_queries.clear() // purge stored queries

Fig.1. Mesh Creation Algorithm

Attack Detection - Attacks are detected using a measurement-based mechanism, where each FORWARDING GROUP and receiver node continuously monitors the discrepancy between expected packet delivery ratio and perceived packet delivery ratio and it flags an attack if it exceeds the threshold value.

B. *Attack Detection and Recovery*

Upon receipt of an ACCUSATION message, a node checks if it does not have an unexpired accusation from the same accuser node and verifies the signature on the message. Accusations are removed from the ACCUSATION LIST after the accusation time has elapsed. Upon receipt of a RECOVERY message from its best upstream node, a FORWARDING GROUP node N checks if it does not have an unexpired accusation from the same accuser node and verifies the signature on the message. In addition, the node also checks that the accusation time in the message is at least as much as its own observed discrepancy. This prevents attackers who cause a large PDR drop by accusing its upstream node only for a short amount of time. If all checks pass, it cancels its pending React Timer, forwards to its downstream nodes and if it is a receiver, activates the recovery procedure. A side effect of metric manipulation attacks is metric poisoning, which prevents recovery by relying on the metrics in the current round. We address this inability by falling back to the fastest route for routing during the remainder of the round. Specifically, during the JOIN QUERY flooding, besides recording the best upstream node, each node also records the upstream for the fastest route as fastest upstream. To recover from an attack, a receiver sends a special JOIN REPLY message to its fastest upstream node. Each node on the fastest route forwards the special JOIN REPLY message to their fastest upstream node and becomes part of the FORWARDING GROUP.

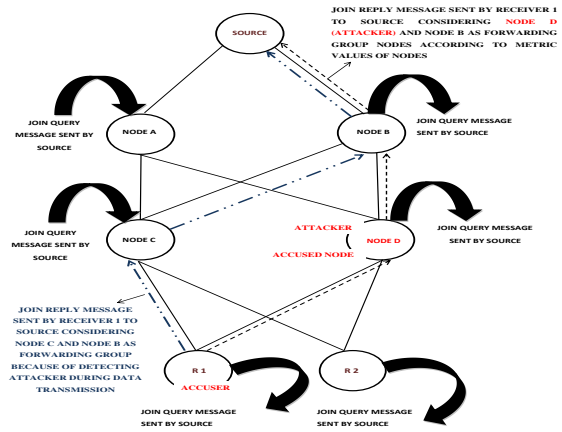

Fig. 2. Attack Detection and Recovery

V. PERFORMANCE EVALUATION

The evaluation is performed in NS2 with the specified simulation environment .The protocol used here is AODV. Effectiveness of our defense against different types of attacks, compared to the insecure protocol. Secure on demand multicast routing protocol suffers only a small PDR decrease relative to the baseline. Our defense is very effective against all the attacks. The small PDR decrease for Secure on demand multicast routing protocol can be attributed from the showed results. First, common to all reactive schemes, attackers can cause some initial damage, before action is taken against them. Second, as the number of attackers increases, some receivers become completely isolated and are not able to receive data. This outcome reflects the design of our defense mechanism in which accusations last proportional to the discrepancy in PDR. Attacks that cause a small discrepancy are forgiven sooner and can be executed again, while attacks that cause a large discrepancy result in a more severe punishment and can be executed less frequently.

A. Bandwidth Usage(Mbps).

The test cases were compared with 500 nodes shown in Figure 3.Due to high bandwidth usage the comparison shows high drop of data packets in the network.

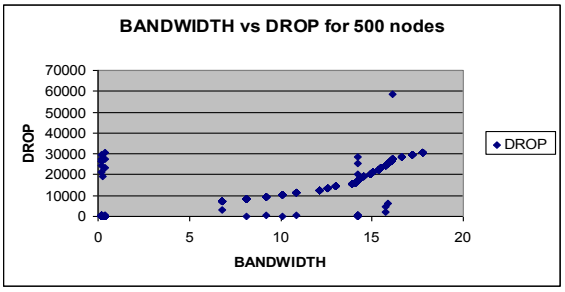

Fig . 3. Bandwidth vs Drop for 500 nodes.

B. Packet Delivery Ratio (PDR).

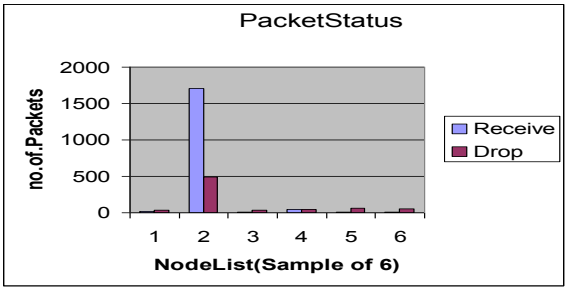

Fig. 4. PDR ratio for sample 6 clients.

The test cases of packet status were compared with first six nodes (as sample) as shown in Figure 4.Here the node2 packets were dropped and received high compared with the limit .In a modularity approach, tests are performed for rest of the nodes.

C. Attack Detection And Prevention Results.

The results shown here is the integration of all the attacks combined and compared with 500 nodes in three scenario and simulation time as follows .100, 200 and 1500 sec with normal, after attacks, prevention respectively.

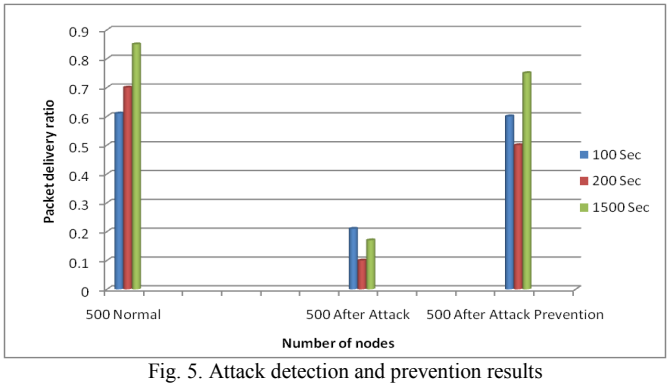

Fig. 5. Attack detection and prevention results

VI. CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] R. Curtmola 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.

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

[6] S.J. Lee, W. Su, and M. Gerla, "On-Demand Multicast Routing Protocol in Multi hop Wireless Mobile Networks," 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] E.M. Royer and C.E. Perkins, "Multicast Operation of the Ad Hoc On-Demand Distance Vector Routing Protocol," Proc. ACM/IEEE MobiCom, pp. 207-218, Aug. 1999.

[9] C. Wu, Y. Tay, and C.-K. Toh, "Ad Hoc Multicast Routing Protocol Utilizing Increasing Id-Numbers (AMRIS) Functional Specification,"Internet draft, Nov. 1998.

[10] C.-C. Chiang, M. Gerla, and L. Zhang, "Forwarding GroupMulticast Protocol (FGMP) for Multihop Mobile Wireless Networks,"ACM J. Cluster Computing, special issue on mobilecomputing, vol. 1, no. 2, pp. 187-196, 1998.

[11] J.J. Garcia-Luna-Aceves and E. Madruga, "The Core-Assisted Mesh Protocol," IEEE J. Selected Areas in Comm., vol. 17, no. 8,pp. 1380-1394, Aug. 1999.

[12] M. Gerla, S.J. Lee, and W. Su, "On-Demand Multicast Routing Protocol (ODMRP) for Ad Hoc Networks,"Internet draft, draftietf-manet-odmrp-02.txt, 2000.

[13] P. Papadimitratos and Z. Haas, "Secure Data Transmission inMobile Ad Hoc Networks," Proc. Second ACM Workshop Wireless Security (WiSe), pp. 41-50, 2003.

[14] J. Dong, 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.

[15] 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.