Invulnerable and Increase Rate Multicast Routing in Wireless Networks

R.Kannan[#1], T.Thilagam[#2],R.Anandh[#3]

[#1,#2,#3] Asst. Professor,CSE&Gojan school of business& Technology, Chennai

Abstract- Recent work in multicast routing for wireless mesh networks has focused on metrics that estimate link quality to increaserate. 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, we identify novel attacks against increase-rate 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 increase-rate metrics. We conclude that aggressive path selection is a double-edged sword: While it increases rate, it also increases attack effectiveness in the absence of defense mechanisms. Our approach to defend against the identified attacks combines measurement-based detection and accusation-based reaction techniques.

Index Terms- Wireless mesh networks, increase-rate metrics, secure multicast routing,metric manipulation attacks

1. INTRODUCTION

Wireless mesh networks emerged as a promising technology that offers low cost Increase bandwidth community wireless services. It is of set of stationary wireless routers that from a multi hop backbone and set of mobile clients that communicate wireless backbone. These applications can benefit from the service provided by multicast routing `protocols. Multicast routing protocols data from a source to destination organized in a multicast group .several protocols [2] ,[3],[4],[5],[6],[7],[8] were proposed to provide multicast services for multi hop wireless networks. These protocols were proposed for mobile ad hocnetworks, focusing primarily on network connectivity and using the number of hops as the route selection metric. Increaserate multicast protocol, nodes periodically send probes to their neighbors to measure the quality of adjacent links. Routediscovery, a node estimate the cast of the path by combining its own measured metric of adjacent link s with the path cost accumulated on the route Discovery packet. The path with the best metric is selected. Recent work in multicast routing for combining its own measured metric of adjacent link s with the path cost accumulated on the route discovery packet. The path with the best metric is selected. Recent work in multicast routing for wireless mesh networks has focused on metrics that estimate link quality to increaserate. Nodes must collaboratein 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 unexpectedconsequences in adversarial networks where compromised nodes act maliciously. In this work, we identify novel attacks against increase 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. The show that these attacks are very effective against

Multicast protocols based on increase-rate metrics. We conclude that aggressive path selection is a double-edged sword: While it increases rate, it also increases attack effectiveness in the absence of defense mechanisms. Our approach to defend against the identified attacks combines measurement-based detection and accusation-based reaction techniques. The solution accommodates transient network variations and is resilient against attempts to exploit the defense mechanism itself.Security implications of using increaserate metrics for multicast in wireless mesh networks. on demand multicast routing protocol is mesh based protocol ,which has the potential to be more attack resilient. In this paper, the main contributions are:

(1).A identifies a class of severe at tacks against multicast protocols that exploit the use of increaserate metrics. Local metric manipulation (LMM) and global metric manipulation (GMM) the aggressive path is selection is a double edged sword. It leads to increased rate. But it leads to effects in the presence of attack

(2).A proposes a secure increase through put multicast protocol S-ODMRP 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.

(3).the performs a detailed security analysis and establishes bounds on the impact of the attacks under the defense scheme. ODM RP and SPP confirm analysis and show that strategy is very effective in defending against the attacks, while incurring a low overhead.

Increaserate mesh based multicast routing protocols provide communication from sources by establishing dissemination structures such as trees or meshes, dynamically updated as nodes join or leave the group.

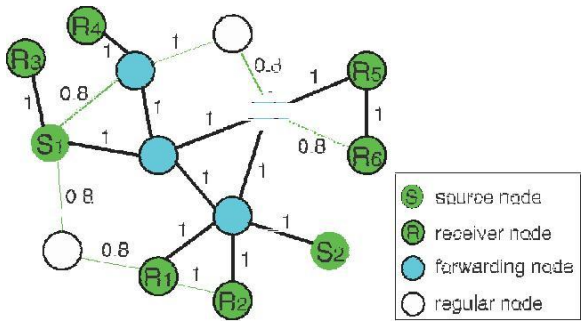

Fig. 1. An example of ODMRP-HT mesh creation for a multicast group with two sources (S1; S2) and six receivers (R1.R6); R6). The label on each link represents the value of the link's SPP metric.

The attacks against increaserate multicast protocols focus on attacks that exploit vulnerabilities introduced by the use of increase through put metrics.ODMR-HT a protocol that enhances ODMR with increaserate metrics. The main difference between ODMR-H T and ODMR are
1) Instead of selecting routes based on minimum delay OD MR-HT selects routes based on link-quality metric,
2) ODMR-HT uses a weighted flood suppression mechanism to flood JOIN QUERY messages instead of using basic flood suppression.

JOIN REPLY messages the attacker can drop join query messages to cause its downstream nodes to be detached from the multicast mesh. The attacker can also forward JOIN REP LY to an incorrect hop node to cause an incorrect path being built. The attacker realties directly to its ability to control the mesh structure and to be selected the path s. the use of increaserate metrics gives attackers additional to manipulate the mesh structure by manipulating the route metric
The paper is organized as section II describes the describes the existing system and proposed system. Section IIIoutlines the proposed protocol functions and section IV concludes the paper with future work

II.BACKGROUND WORK

A.EXISTING SYSTEM

In the existing system 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 hops (or hop count) as the route selection metric. However, it has been shown that using hop count as routing metric can result in selecting with poor Quality on the path, negatively impacting the path rate. Rate based data transfer is utilized. Secure communication is not that effective. Data loss occurs often. Node maximum reliability is not calculated.

B.PROPOSED SYSTEM

The stationary nature of WMNs, recent protocols focus on maximizing path rate by selecting paths based on metrics that capture the quality of the wireless links. the refer to such metrics as link-quality metrics or increase-rate metrics, and to protocols using such metrics as increase-rate protocols. In a rate multicast protocol, nodes periodically send probes to their neighbors to measure the quality of their adjacent links

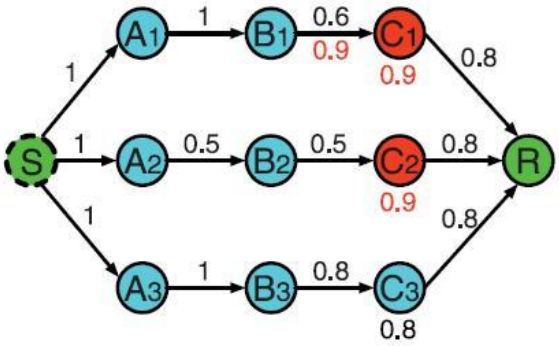

Fig. 2. Metric manipulation attack during the propagation of the flood packet from the source S to receiver R. A label above a link is the link's real SPP metric; a label below a link a node is the accumulated route metric advertised by the node.

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. Increase-rate 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, mesh partitioning, or traffic analysis. Creating opportunities for attacks such as data dropping, mesh partitioning.

Two types of metric manipulation attack. Local metric manipulation (LMM) and global metric manipulation (GMM)

LMM attacks. An adversarial nodeartificially increases the quality it's an adjacent links, distorting the neighbors perception about these 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 for the links toward itself. In fig.2,a malicious node C1 claims that SPP B1→C1=0.9 instead of the correct metric of 0.6.thus, C1 accumulates a false local metric of the metric B1→C1 and advertises to R the metric SPP S→C1=0.9 instead of the correct metric SPP S→C1=0.6.the route S-A1-B1-C1-R will be chosen over the correct route S-A3-B3-C3-R

GMM attack a malicious node arbitraryChanges 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 own contribution to the path metric ,but also the contributions of previous nodes that were accumulated in the path metric. For example, fig 2.attacker C2 should advertise route metric of 0.25 but instead advertises a route metric of 0.9 to node R .The route S-A2-B2-C2-R to be selected over the correct route S-A3-B3-C3-R.

III ODMRP PROTOCOL

ODMRP ensures the delivery of data from the source to the multicast receivers. ODMRP uses a combination of authentication and rate limiting techniques against resource consumption attacks and novel techniques, Rate Guard more challenging packet dropping and mesh structure attacks, including metric manipulations and JOIN REPLY dropping.

Rate Guard dropping packets, attackers do not affect the multicast protocol unless cause a

In the packet delivery ratio (PDR) measurement based attack detection that relies on the ability of honest nodes to detect the discrepancy between the expected (e PDR) and perceived PDR (p PDR)

Mesh creation algorithm

The source code S periodically broadcasts to the entire network a JOIN QUERY message in order to refresh membership information and update the routes.

Executed at the source node to initiate 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 receipt of a JOIN QUERY message q:

6:**if** (latest_ received_ join_ seq>q.seq) **then**
7: **return**
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_NOD
E 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)
28:

Executed at a node upon timeout or reply _ timer:

29: 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 ()
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

S is signed using a weight flood suppression mechanism. Nodes only process JOIN QUERYmessage that valid signature line 8.accusation list maintained each node lines(18-19) best_ upstream and best_ metric(line 23) JOIN REPLY messages sentfrom receivers S along to increaserate metric. Node starts to monitor the PDR from its best_ upstream Measure to perceived PDR. It s include FORWARD GROUP. Minimum because1 and 2 metric share the same upstream node.

Attack reaction algorithm

On detecting a discrepancy between e PDR and p PDR:

1. Start _ timer(React_ Timer, β(1-ePDR)

Executed at node on timeout of React _ Timer:

2. **IF (**is _ receiver**) then**
3. Create salvage message ss // fallback
4. Send_ message (ss ,fastest_ upstream)
5. **IF** (accusation_ list. contains_ accuser_node (node _ id**)) then**
6. **Return** //each node can only accuseonce
7. // create and flood accusation message
8. Create accusation message acc
9. Acc .accused=best_ upstream
10. Acc .accused=node_ id
11. Acc. accusation _time = α (e PDR- p PDR)
12. Accusation_ list. Add (acc)
13. Sign (acc); Broadcast (acc)

14.//send recovery message to the sub tree
15: Create recovery message rr
16:rr.accusation=acc
17: Sign (rr)
18: for each downstream node d do
19. Send _ message (rr, d)

Executed at a node on receipt of an accusation message acc:

20: **IF** (accusation_ list. contains_ accuser_ node (acc. accuser)) **then**
21**: return** //only allow one accusation from a node at a time
22: Verify (acc .accuser, acc.sig) 23:accusation_list. Add (acc) 24: Broadcast (acc)

Executed at a node on receipt of a recovery message rr:

25: **IF** (handled_ recovery_ message. Contains (rr)) **then**
26**: return //**ignore duplicate recovery 27: **IF** (accusation_ list. contains_ accuser_ node (rr.acc. accuser)
OR rr. acc. accusation _ time < α (e PDR- p PDR)) **then**
28**: return**
29: Verify (rr)
30:handled_recovery_messages. Insert (rr)
31**: IF** (React_ Timer is active) **then** cancel React _ Timer

Create, sign and flood an ACCUSATION messages in the network N's best upstream node the message contains accusation_ time=@(e PDR-p PDR) @ is a tunable system parameter

Create, sign and send to its downstream nodes a recovery message it's contains accusation message React_ timer of nodes in N's sub tree and fallback procedure of the receivers in N's sub tree.

The above algorithm two techniques measurement based detection and accusation based reaction.

IV.CONCLUSION & FUTURE WORK

In this paper security implications of using increaserate metrics in multicast protocols in wireless mesh networks. It's identified metric manipulation that conflict significant damage of the network. The overcome the challenges novel scheme. Rate Guard the combine measurement based detection and accusation based reaction. The defense is effective the identified attacks, security and resilient to the failures like Byzantine failure and other malicious attacks.

V.REFERENCES

1. J. Dong, R. Curtmola, and C. Nita-Rotaru, "On the Pitfalls of Using Increase-Rate 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.
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. 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. Madruga and J.J. Garcia-Luna-Aceves, "Scalable Multicasting: the Core-Assisted Mesh Protocol," 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 Networks," Mobile Networks and Applications, vol. 7, no. 6, pp. 441-453, 2002.
7. [7] E.M. Royer and C.E. Perkins, "Multicast Ad-Hoc On-Demand Distance Vector (MAODV) Routing," Internet Draft, July 2000.
9. [8] J.G. Jetcheva and D.B. Johnson, "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks," Proc. ACM MobiHoc, 2001. J. Dong, R. Curtmola, and C. Nita-Rotaru, "On the Pitfalls of Using Increase-Rate 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.
10. 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.
11. 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.
12. 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.
13. E.L. Madruga and J.J. Garcia-Luna-Aceves, "Scalable Multicasting: the Core-Assisted Mesh Protocol," Mobile Networks and Applications, vol. 6, no. 2, pp. 151-165, 2001.
14. 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.
15. E.M. Royer and C.E. Perkins, "Multicast Ad-Hoc on-Demand Distance Vector (MAODV) Routing," Internet Draft, July 2000.