BSMR: Byzantine-Resilient Secure Multicast Routing In Multi-Hop Wireless Networks

[1,]Vijay Bahadur Singh, [2,]Ashok Prasad,Mukesh Chauhan
[1,2,]Department Of Information Technology, Institute Of Technology And Management , AL-1 Sector-7 Gida , Gorakhpur

Abstract

Multi-hop wireless networks rely on node cooperation to provide unicast and multicast services. The multi-hop communication offers increased coverage for such services, but also makes them more vulnerable to insider (orByzantine) attacks coming from compromised nodes that behave arbitrarily to disrupt the network.In this work we identify vulnerabilities of on-demand multicast routing protocols for multi-hop wirelessnetworks and discuss the challenges encountered in designing mechanisms to defend against them. We proposeBSMR, a novel secure multicast routing protocol that withstands insider attacks from colluding adversaries. Ourprotocol is a software-based solution and does not require additional or specialized hardware. We present simulationresults which demonstrate that BSMR effectively mitigates the identified attacks.

Keywords –multi-hop destination, multicast routing, Byzantine resilient protocols.Byzantine attacks, Byzantine resiliency, Multi-hop wireless networks**.**

1. Introduction

Multicast routing protocols deliver data from a source to multiple destinations organized in a multicast group. Several protocols were proposed to provide multicast services for multi-hop wireless networks. These protocols rely on node cooperation and use flooding [I], gossip [2], geographical position [3], or dissemination structures such as meshes [4], [5], or trees [6], [7]. A major challenge in designing protocols for wireless networks is ensuring robustness to failures and resilience to attacks. Wireless networks provide a less robust communication than wired networks due to frequent broken links and a higher error rate. Security is also more challenging in multi-hop wireless networks because the open medium is more susceptible to outside attacks and the multi-hop communication makes services more vulnerable to insider attacks coming from compromised nodes. Although an effective mechanism against outside attacks, authentication is not sufficient to protect against insider attacks because an adversary that compromised a node also gained access to the cryptographic keys stored on it. Insider attacks are also known as Byzantine [8] attacks and protocols able to provide service in their presence are referred to as Byzantine resilient protocols.

1.1 Statement of the Problem

Previous work focused mainly on the security of unicast services. Several routing protocols [9]-[12] were proposed to cope with outsider attacks. Methods proposed to address insider threats in unicast routing include monitoring [13], multi-path routing [14] and acknowledgment-based feedback [15], [16]. The problem of secure multicast in wireless networks was less studied and only outside attacks were addressed - [17].

1.2 Significance of the Study

In this paper we study vulnerabilities of multicast routing protocols in multi-hop wireless networks andpropose a new protocol that provides resilience against Byzantine attacks.We identify several aspects that make the design of attack-resilient multicast routing protocols more Challenging than their unicast counterpart, such as a more complex trust model and underlying routingStructure. and scalability. We also discuss potential attacks against such protocols.

.

2. Related Work

Several routing techniques like SEAD, Ariadne and MAODV protocol .Were studied and we analyzed the drawback of every routing protocol against byzantine attacks and maintaining tree structure. In AAS we analyzed the authentication of sending data with acknowledgment but in multicast protocol sending such acknowledgment cannot be done for multi-hop wireless networks. So we used MACT to send acknowledgment from receiver to sender. We implemented an on-demand multicast protocol which threats against Byzantine attacks and maintains tree structures effectively.

3. Network and System Model

3.1 Network Model

We consider multi-hop wireless network where nodes participate in the data forwarding process for other nodes. We assume that the wireless channel is symmetric. All nodes have the same transmitting power and consequently the same transmission range. The receiving range of a node is identical to its transmission range.

3.2 Multicast Routing Protocol

This protocol is to protect from external attacks against the creation and maintenance of the multicast tree and prevents unauthorized nodes to be part of the network, of a multicast group, or of a multicast tree.It allows a node that wants to join a multicast group to find a route to the multicast tree. To prevent outsiders from interfering, all route discovery messages are authenticated. Only group authenticated nodes can initiate route request.We assume a tree-based on-demand multicast protocol such as [6]. The protocol maintains bi-directional sharedmulticast trees connecting multicast sources and receivers. Each multicast group has a corresponding multicast tree.The multicast source is a special node, the group leader, whose role is to eliminate stale routes and coordinate groupmerges. Route freshness is indicated by a group sequence number updated by the group leader and broadcastperiodically in the entire network. Higher group sequence numbers denote fresher routes.The main operations of theprotocol are route discovery, route activation and tree maintenance. During route discovery a node discovers a path to a node that is part of the multicast tree. A requester first broadcasts a route request message that includes the latestknown group sequence number. The route request message is flooded in the network using a basic flood suppression mechanism and establishes reverse routes to the source of the request. Upon receiving the route request, a node that is part of the multicast tree and has a group sequence number at least as large as the one in the route request, generates a route reply message and unicasts it on the reverse route. The route reply message includes the last known group sequence number and the number of hops to the node that originated the route reply. During route activation, the requester selects the freshest and shortest route (i.e., with the smallest number of hops to the multicast tree) from the routes returned by the route discovery operation. The requester activates that route by unicasting a multicast activation message.Three main operations ensure the tree maintenance: tree pruning, broken link repair and tree merging.Tree pruning occurs when a group member that is a leaf in the multicast tree decides to leave the group.To prune itself from the tree, the node sends a message to indicate this to its parent. The pruning messagetravels up the tree causing leaf nodes that are not members of the multicast group to prune themselvesfrom the tree, until it reaches either a non-leaf node or a group member. A non-leaf group member mustcontinue to act as a router and cannot prune itself from the multicast tree.

4. Attacks Against Multicast Routing

4.1Adversarial Model

We consider a three-level trust model that captures the interactions between nodes in a wireless multicast setting and defines a node's privileges: the first level consists of the source, which must be continually available and assumed not to be compromised (an unavailable or untrusted source makes the multicast service useless); the second level consists of the multicast group member nodes, which are allowed to initiate requests for joining multicast groups; and the third level consists of nonmember nodes, which participate in the routing but cannot initiate group join requests. In order to cope with Byzantine attacks, even group members are not fully trusted.

4.2Attacks in Multicast Routing and inMultihop Wireless Networks

Nodes can maliciously report that other links are broken or generate incorrect pruning messages, resulting in correct nodes being disconnected from the network or tree partitioning. In the absence of authentication, any node can pretend to be the group leader. Although many routing protocols do not describe how to select a new group leader when needed, we note that the leader election protocol can also be influenced by attackers. Attacks against data messages consist of leaves dropping, modifying, replaying, injecting data, or selectively forwarding data after being selected on a route. A special form of packet delivery disruption is a denial-of-service attack, in which the attacker overwhelms the computational, sending, or receiving capabilities of a node. In general, data source authentication, integrity, and encryption can solve the first attacks and are usually considered application specific security. Defending against selective data forwarding and denial of service cannot be done exclusively by using cryptographic mechanisms. Because external attacks can be prevented using the authentication framework described in Section 5.2, we focus on the following Byzantine attacks:

1. **Black hole attack:** One or several adversaries forward only routing control packets, while dropping all data packets.adversaries areplaced strategically around the multicast source, equidistant on a circle with radius of 200 meters.

2. **Wormhole attack:** Two colluding adversariestunnel packets between each other in order to create a shortcut in the network. The adversaries use the low cost appearance of the wormhole to increase the probability of being selected on paths; once selected on a path, they attempt to disrupt data delivery by executing a black hole attack.

3. **Flood rushing attack:** One or severaladversaries rush an authenticated flood through the network before the flood traveling through a legitimate route. This allows the adversaries to control many paths. Flood rushing can be used to increase the effectiveness of a black hole or wormhole attack.

4. **Selfish Nodes:**One or several adversarieswant to preserve its own resources while using the services of others and consuming their resources, such misbehaving nodes participate in the route discovery and maintenance phase but refuse to forward data packets, which degrades routing performance.

5. Secure Multicast Routing Protocol

5.1 SORB Overview

Our protocol ensures that multicast data is delivered from the source to the members of the multicast group, even in the presence of Byzantine attackers, as long as the group members are reachable through non-adversarial path. Here and authentication framework is used to eliminate outside adversaries and ensure that only authorized nodes perform certain operations (only tree nodes can perform tree operations and only group nodes can connect to the corresponding multicast tree). SORB mitigates inside attacks that try to prevent a node from establishing a route to the multicast tree by flooding both route request and route reply. Tree nodes monitor the rate of receiving data packets and compare it with the transmission rate indicated by the source in the form of an MRATE message.

5.2 Node Authentication

The authentication framework prevents unauthorized nodes to be part of a multicast tree or of a multicast group. Each node authorized to join the network has a pair of public/private keys and node certificate that binds its public key to its IP address. Each node authorized to joinmulticast group has an additional group certificate that binds its public key and IP address to the IP address of the multicast group. Nodes in the multicast tree are authenticated using a tree token, which is periodically refreshed and disseminated by the groupleader in the multicast tree withthe help of pairwise shared keys established between every direct tree neighbors. Only nodes that are currently on the tree will have a valid tree token. To allow any node in the network to check that a tree node possesses a valid tree token, the group leader periodically broad casts in the entire network a tree token authenticator. Hop count authentication is to prevent tree nodes from claiming to be at a smaller hop distance from the group leader than they actually are, we use a technique based on a hash chain. The hop count anchor is also included by the group leader in Group Hello messages, which are broadcast periodically in the entire network. This allows a tree node to prove its hop distance from the group leader to any node in the network

5.3 Route Discovery:

SORB's route discovery allows a node that wants to join a multicast group to find a route to the multicast tree. To prevent outsiders from interfering, all route discovery messages are authenticated using the public key corresponding to the network certificate. Only group authenticated nodes can initiate route requests and the group certificate is required in each request. Tree nodes use the tree token to prove their current tree status. The requesting node broadcasts a route request (RREQ) message that includes the node identifier and its weight list, the multicast group identifier. The RREQ message is flooded in the network until it reaches a tree node. Only new requests are processed by intermediate nodes. When a tree node receives a RREQ from a requester, it initiates a response. The node broadcasts a route reply (RREP) message that includes that node identifier, the requester's identifier and weight list from the request message. The RREP message is flooded in the network until it reaches the requester.

5.4 Multicast Route Activation

The requester signs and unicasts on the selected route an multicast activation message that include its identifier, the group identifier, and the sequence number used in the RREQ phase. The MACT message also includes a one way function applied to on the tree token extracted from RREP, f(requestor, tree token), which will be checked by the tree node that sent the RREP message to verify that the nodes activated the route is the same as the initial requestor. An intermediate node on the route checks if the signature on MACT is valid and if MACT contains the same sequence number as the one in the original RREQ. The node then adds to its list of tree neighbors the previous node and the next node on the route as downstream and upstream neighbors, respectively, and sends MACT along the forward route . During the propagation of the MACT message, tree neighbors use their public keys to establish pairwise shared keys, which will be used to securely exchange messages between tree neighbors. The requester and the nodes that received MACT could be prevented from being grafted to the tree by an adversarial node, selected on the forward route, which drops the MACT message. To mitigate the attack, these nodes will start a WTC-Timer upon whose expiration nodes isolate a faulty link and initiate route discovery. The timer will expire after a value proportional to a node's hop distance to the tree, in the hope that the nodes closer to the tree will succeed in avoiding the adversarial node and will manage to connect to the tree. After a node becomes aware of its expected receiving data rate, it cancels its WTC-Timer.

5.5 Multicast Tree Maintenance

Routing messages exchanged by tree neighbors, such as pruning messages are authenticated using the pair wise keys shared between tree neighbors. Tree pruning occurs when a group member that is a leaf in the multicast tree decides to leave the group. A node initiates pruning from the tree by sending a message to its parent. The group leader periodically broadcasts in the entire network a signed Group Hello message that contains the current group sequence number, the tree token authenticator, and the hop count anchor (described in Section 5.2). A signed Group Hello message containing a special flag alsoensures that when two disconnected trees are merging, one of the group leaders is suppressed.

5.6 Selective Data Forwarding Detection

The source periodically signs and sends in the tree an MRATE message that contains its data transmission rate. As this message propagates in the multicast tree, nodes may add their perceived transmission rate to it. Each tree node keeps a copy of the last heard MRATE packet. The information in the MRATE message allows nodes to detect if tree ancestors perform selective data forwarding attacks. Depending on whether their perceived rate is within acceptable limits of the rate in the MRATE message, nodes alternate between two states. The initial state of a node is disconnected; after it joins the multicast group and becomes aware of its expected receiving data rate, the node switches to the connected state. Upon detecting a selective data forwarding attack, the node switches back to the disconnected state. MRATE is the difference between two distances. The source periodically signs and sends in the tree a multi-cast rate (MRATE) message that contains its data transmission rate. Nodes may add their perceived transmission rate to it. The information in the MRATE message allows nodes to detect if tree ancestors perform selective data forwarding attacks. Depending on whether their perceived rate is within acceptable limits of the rate in the MRATE message, thenode forward the request to next node until it reaches the destination.

5.7 Communication Between MulticastGroups

We can communicate between different Multicast Groups and can form a Grid. To join different Multicast Groups with each other for communication, the Multicast Group Source (Group Leader) which needs to join will send a route request RREQ with a WTC-Timer to the desired Multicast Group Source. Then, the connection has been made with the Group Certificate of both Multicast Groups. Likewise, any Multicast Group can join to the Grid. If a Multicast Group source needs to leave the Grid, It should send the request to all the Grid members with which it has the connections. Once the leaving route request has reached the connected Sources, then the leaving Source has been disconnected from the network. The data can be transmitted from one source to the other provided if the sender Source knows the Group Certificate of the member nodes irrespective of whether it may in its own group or in different group. If it is in its own group, it'll follow as a Multicast Routing Protocol and sends the Data. If it is in different Group, It should communicate with all the Sources to check whether it has the destination node as using Group Certificate, Node Certificate and Tree Token function. Once if it is found with the shortest path, It'll reply to the Sender Source as a route reply RREP. If the sender Source gets RREP, it'll send the data by Selective Data Forwarding Detection method through the Group Leader (Source) which has the destination node.

Algorithm for grid based multicast group communication Multicast protocol

```
Multicast protocol
{
// consider first node as group leader
//Create the node from group leader
Authenticate every node with RREQ, grid,
grpseqno, nc, gc and send request
If this.gc & gc is in same group
{
Add node to the existing group;
}
Else
{
Join the group leader of the different group and
make as grid;
}
//sending multicast msgs to the destinations
Find the route discovery();
Choose shortest path;
WTC-Timer starts ();
Find the MRATE value;
```

If distance-path>data-rate
Send data to the destination;
If data-send takes time
cancel the data transmission;
choose other shortest path and send the data
Proceed until data has been send;
send MACT-msg to sender from receiver;
//leaving a group
If this.gc and gc and confirm .yes
Cancel the node from the source and make free
from n/w;
// leaving a node
If this.nc and nc, and this.gc and gc, and
confirm-yes then
Delete the node;
Maintain tree structure ();
}

6. Implementation

Theoretically implementation has been completed with this idea of routing protocol Which has strong defense against Byzantine?attacks and joining different Multicast Groups Group Leaders and making communication between the Group Leader to any member nodes in any Multicast Groups. We completed the implementation of a Multicast protocol over a Multicast group.

7. Conclusion

In this paper we have discussed several aspects that make designing attack-resilient multicast routing protocols for multi-hop wireless networks more challenging when compared to their unicast counterpart. A more complex trust model and underlying structure for the routing protocol make solutions tailored for unicast settings not applicable for multicast protocols. In the absence of defense mechanisms, Byzantine attacks can prevent multicast protocols to achieve their design goals. We have proposed BSMR, a routing protocol which relies on novel general mechanisms to mitigate Byzantine attacks. BSMR identifies and avoids adversarial links based on a reliability metric associated with each link and capturing adversarial behavior. Our experimental results show that BSNLR's strategy is effective against strong insider attacks such as black holes and flood rushing. We believe that this strategy can also be effective against wormhole attacks and defer the experimental validation for future work.

8. Acknowledgements

The first author would like to thank R5zvan Mus5loiu-E. for fruitful "copy-room" discussions in theEarly stages of this work. This work is supported by National Science Foundation Cyber Trust Award No. 0545949. The views expressed in this research are not endorsed by the National Science Foundation.

References

[1] R. Curtmola and C. Nita-Rotaru, "BSMR: Byzantine-Resilient Secure Multicast Routing in Multi-hop Wireless Networks", IEEETRANSACTIONS ON MOBILECOMPUTING, VOL. 8, NO. 4, APRIL 2009.
[2] R. Chandra, V. Ramasubramanian, and K. Birman, "Anonymous Gossip: ImprovingMulticast Reliability in Mobile Ad-HocNetworks,"Proc. 21st Int'l Conf. Distributed Computing Systems (ICDCS '01), 2001.
[3] Y.-B. Ko and N.H. Vaidya, "GeoTORA: A Protocol for Geocasting in Mobile Ad Hoc Networks," Proc. Eighth Ann. Int'l Conf.Network Protocols (ICNP '00), p. 240,2000.
[4] E.L. Madruga and J.J. Garcia-Luna-Aceves, "Scalable Multicasting. The Core-Assisted MeshProtocol," Mobile Networks and Applications, vol. 6, no. 2, 2001.
[5] S.J. Lee, W. Su, and M. Gerla, "On-Demand Multicast Routing Protocol in Multihop WirelessMobile Networks," Mobile Networks and Applications, vol. 7, 2002.
[6] E. Royer and C. Perkins, "Multicast Ad-Hoc On-Demand DistanceVector (MAODV) Routing", Internet draft, July 2000.
[7] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An Efficient Group RekeyingScheme for Secure Multicast in Ad-HocNetworks", Proc. First Ann. Int'l Conf. Mobile and Ubiquitous Systems (Mobiquitous '04), pp. 42-51, 2004.
[8] L. Lazos and R. Poovendran, "Power Proximity Based Key Management for Secure Multicast in Ad Hoc Networks," ACM J. Wireless Networks, 2005.