ISSN:0975-9646

Secure and Scalable Multicasting Services in Wireless Mesh Networks

B TEJASWI S. SIVANAGESWARA RAO S. GOPI KRISHNA Y.K.SUNDARA KRISHNA

Abstract: **Estimating link quality during multicast routing is vital for maximizing throughput in Wireless mesh networks. To efficiently forward data all mesh nodes must collaborate for computing path metric. If metric computation, propagation, and aggregation is based upon the assumption that all nodes are genuine then this will lead to haywire in adversarial networks where compromised nodes act maliciously. To counter the attacks of the compromised nodes earlier a combined measurement-based detection and accusation-based reaction techniques were implemented instead of aggressive path selection method. Both the attacks and defense were implemented using ODMRP protocol. ODMRP offers more efficient packet forwarding, but the transmissions are much more unreliable due to its difficulty of maintaining forwarding mesh under mobility, which leads to a lower packet delivery ratio. The multicast group joining delay of ODMRP is also much higher. To address these issues we propose to use an efficient and scalable geographic multicast protocol, EGMP in combination with the above security measures instead of ODMRP. It has significantly lower control overhead, data transmission overhead, and multicast group joining delay. We simulate the achievable throughput and security using our proposed mechanism and as certain its claim.**

Index Terms—**Wireless mesh networks, Routing, multicast, and protocol.**

1 INTRODUCTION

Wireless mesh networks (WMNs) emerging and promising technology that offers low-cost, high-bandwidth community for wireless services. A WMN consists of a set of stationary wireless routers which form a multihop backbone, and a set of mobile clients that communicate through wireless backbone. Several protocols were proposed primarily focusing on network connectivity and using hop count as the metric for route selection. However, using hop count as routing metric can result in selecting links with poor quality on the path, negatively impacting the scalability and path throughput.

Recent protocols focus on maximizing path throughput by selecting paths based on metrics that capture the quality of the wireless links. We refer such metrics as link-quality or high-throughput metrics, and protocols is high -throughput protocols. In high throughput protocol an assumption is made that nodes behave correctly while metric computation and propagation. However, assumption is difficult to guarantee in wireless networks. An aggressive path selection introduces new vulnerabilities and provides the attacker with an increased arsenal of attacks leading to unexpected consequences.

Previous work mainly focused on the performance and security implications of using high-throughput metrics for multicast in WMNs. In particular ODMRP protocol is used, as it is a mesh based protocol, which has the potential to be more attack resilient. But ODMRP is unreliable and have very high multicast control overheads when the group size is small. The limitations of ODMRP, the need for network-wide packet floods and requiring that the sources of multicast packets for a group be part of the group's multicast mesh, even if such sources are not interested in receiving multicast packets sent to the group and delay is also much higher.

In this work, we study the performance, scalability and security implications for multicasting in WMNs. In particular, we use an efficient geographic multicast protocol, EGMP, which can scale to a large group size and large network size. EGMP could quickly and efficiently build packet distribution paths, and reliably maintain the forwarding paths in the presence of network dynamics due to unstable wireless channels or frequent node movements.

2 ATTACKS AGAINST HIGH- THROUGHPUT PROTOCOL

In general, the attacker can achieve the goal of interrupting the multicast data delivery by either depleting network resource, causing incorrect mesh establishment or by dropping packets.

2.1 Resource Consumption Attacks

ODMRP floods *JOIN QRY* messages in the entire network, allowing an attacker to insert either

spoofed or its own legitimate *JOIN QRY* messages at a high frequency to cause frequent network wide flooding. By sending many *JOIN RPY* messages, an attacker can cause unnecessary data packet forwarding and activate unnecessary data paths. 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 proper group session with high data rate in order to take away the network resource from honest nodes.

2.2 Mesh Structure Attacks

Mesh structure attacks disrupt the correct establishment of the mesh structure in order to interrupt the data delivery paths. These attacks can be caused by malicious manipulation of the *JOIN QRY* and *JOIN RPY* messages.

For the *JOIN QRY* messages, the attacker can spoof the source node and inject invalid *JOIN QRY* messages, which cause incorrect path i.e., paths toward the attacker node instead of the correct source node. The attackers may also act in a selfish manner by dropping *JOIN QRY* messages, which allows them to avoid participation in the multicast protocol. Sometimes attacker nodes form a vertex cut in the network and prevent legitimate nodes from receiving *JOIN QRY* messages. Finally, the attacker may also modify the accumulated path metrics in the *JOIN QRY* messages incorrectly.

For the *JOIN RPY* messages, the attacker can drop *JOIN RPY* messages to cause its downstream nodes to be separated from the multicast mesh. The attacker can also forward *JOIN RPY* to an incorrect next hop node to cause an incorrect path being built. In many of the above attacks, the power of the attacker relates directly to its ability to control the mesh structure and to be selected on paths.

2.3 Metric Manipulation Attacks

The use of high-throughput metrics requires adjacent links local information of each node. Each node, adjacent links local information is collected by sending periodic probes to its neighbors. This local information is accumulated in *JOIN QRY* packets and propagated in the network, allowing nodes to gain global information about the routes quality from the source. Adversaries can perform two types of metric manipulation attacks: local metric manipulation (LMM) and global metric manipulation (GMM).

LMM attacks. An adversarial node artificially increases the quality of its adjacent links, distorting the neighbors' perception about these links. The falsely advertised "highquality" 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.

GMM attacks. In a GMM attack, before rebroadcasting the flood packet, a malicious node arbitrarily changes the value of the route metric accumulated in the 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.

3 EFFICIENT GEOGRAPHIC MULTICAST PROTOCOL

In this section, we will describe the EGMP protocol that ensures the delivery of data from the source to the multicast receivers even in the presence of Byzantine attackers.

3.1 Protocol Overview

EGMP supports scalable and reliable membership management and multicast forwarding through a *virtual zone-based* structure. In a pre-determined virtual origin, the nodes in the network self-organize themselves into a set of zones as shown in Fig. 1, and a leader is elected in a zone to manage the membership of local group. The leader serves as a representative for its zone to join or leave a multicast group as required. As a result, a network-wide zone-based multicast tree is built.

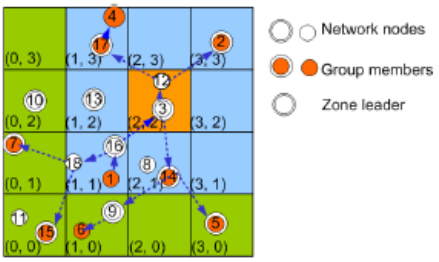

Fig. 1: Zone structure and multicast session example.

The zone-based tree is shared for all the multicast sources of a group. To further reduce the forwarding overhead and delay, EGMP supports bi-directional packet forwarding along the tree structure. That is, instead of sending the packets to the root of the tree first, a source forwards the multicast packets directly along the tree. The multicast packets will flow along the multicast tree both upstream to the root zone and downstream to the leaf zones of the tree. When an ontree zone leader receives the packets, it will send them to the group members in its local zone.

In EGMP, the construction of zone structure is independent with the shape of the network region, and it is very simple to establish and preserve a zone. The zone is used in EGMP to provide location reference and support lower level group membership management. A multicast group can cross multiple zones. With the introduction of virtual zone, EGMP only needs to track the membership change of zones.

There is no need to track individual node movement, which significantly reduces the management overhead and increases the robustness of the proposed multicast protocol.

3.2 Neighbor Table Generation and Zone Leader Election

For efficient management of states in a zone, with minimum overhead a leader is elected. As a node use periodic BEACON broadcast to distribute its position to facilitate leader election and reduce overhead, EGMP simply inserts a flag in the BEACON message, which indicate whether the sender is a zone leader. The broadcast message received by all nodes. To reduce the beaconing overhead, instead of using fixed-interval beaconing, the beaconing interval for the underneath unicast protocol will be adaptive. A non-leader node will send a beacon, when it moves to a new zone or every period of $Intval_{max}$. A zone leader has to send out a beacon every period of $Intval_{min}$ to announce its leadership role.

A node neighbor table is constructed without extra signaling. When receiving a beacon from a neighbor, a node records the *flag*, node ID and position contained in the message in its neighbor table. A zone leader is elected through the nodes collaboration and maintained consistently in a zone. When a node appears in the network, it sends out a beacon announcing its existence. Then it waits for an $Intval_{max}$ period for the beacons from other nodes. Every $Intval_{min}$ a node will check its neighbor table and determine its zone leader under different cases:
1) If there is only one of the nodes in the zone has its flag set then that node set is the leader. 2) If there is more than one node in the same zone have their flags set then the node with the highest node ID is elected as leader. 3) The flags of all the nodes in the same zone are unset then the node which is closer to the zone center will announce its leadership role through a beacon message with the leader flag set.

3.3 Zone-supported Geographic Forwarding

With a zone structure, the communication process includes an intra-zone transmission and an inter-zone transmission. In normal geographic unicast routing, location service is required for the source to obtain the destination position. In EGMP, to avoid the overhead in tracking the exact locations of a potentially large number of group members, location service is integrated with zone-based membership management without the need of an external location server. At the network, only the ID of the destination zone is needed. A packet is forwarded towards the center of the destination zone first. After arriving at the destination zone, the packet will be forwarded to a specific receiving node or broadcast depending on the message type.

In the above design, for scalability and reliability, the center of the destination zone is used as the landmark for sending a packet to the group members in the zone although there may be no node located at the center position. This, however, may result in the failure of geographic forwarding.

To avoid this problem, we introduce a *zone forwarding mode* in EGMP when the underlying geographic forwarding fails. Only when the zone mode also fails, the packet will be dropped. In zone mode, a sender node searches for the next hop to the destination based on its neighbor table, which can more accurately track the local network topology. The node selects as its next hop the neighboring node whose zone is the closest to the destination zone and closer to the destination zone than its own zone. If multiple candidates are available, the neighbor closest to the destination is selected as the next hop.

3.4 Multicast Tree Construction

In EGMP, instead of connecting each group member directly to the tree, the tree is formed in the granularity of zone with the guidance of location information, which significantly reduces the tree management overhead. With a destination location, a control message can be transmitted immediately without incurring a high overhead and delay to find the path first, which *enables quick group joining and leaving*. In the following description, except when explicitly indicated, we use G, S and M respectively to represent a multicast group, a source of G and a member of G.

3.4.1 Multicast session initiation and termination

When a multicast session G is initiated, the first source node S (or a separate group initiator) announces the existence of G by flooding a message *NEWSESSION(G;zIDS*) into the whole network. The message carries G and the ID of the zone where S is located, which is used as the initial *rootzone* ID of group G. When a node M receives this message and is interested in G, it will join G. A multicast group member will keep a membership table with an entry (*G; rootzID; isAcked*), where G is a group of which the node is a member, *rootzID* is the root-zone ID and isAcked is a flag indicating whether the node is on the corresponding multicast tree. A zone leader (LDR) maintains a multicast table. When a LDR receives the *NEWSESSION* message, it will record the group ID and the root-zone ID in its multicast table. To end a session G, S floods a message *ENDSESSION*(G). When receiving this message, the nodes will remove all the information about G from their membership tables and multicast tables.

3.4.2 Multicast group join

When a node M wants to join the multicast group G, if it is not a leader node, it sends a *JOIN REQ*(*M; PosM; G; fMoldg*) message to its LDR,

```
Procedure LeaderJoin(me; pkt)
 LDR: the leader itself
 pkt: the JOIN REQ message the leader received
 BEGIN
  if (pkt:srcZone == LDR:zID) then
   /* the join request is from a node in local zone */
   /* add the node into the downstream node list of
the    multicast table */
    AddNodetoMcastTable(pkt:groupID,
pkt:nodeID);
 else
  /* the join request is from another zone */
  if (depthLDR < depthpkt) then
   /* add this zone to the downstream zone list of
the  multicast table*/
    AddZonetoMcastTable(pkt:groupID, pkt:zID);
  else
    ForwardPacket(pkt);
    return;
  end if
 end if
 if (!LookupMcastTableforRoot(pkt:groupID)) then
   /* there is no root-zone information */
   SendRootZoneReq (pkt:groupID);
Elseif
(!LookupMcastTableforUpstream(pkt:groupID))
then   /* there is no upstream zone information */
  SendJoinReq (pkt:groupID);
 else
  SendReply;
 end if
END
```

Fig. 2: The pseudocode of the leader joining procedure.

carrying its address, position, and group to join. The address of the old group leader *Mold* is an option used when there is a leader handoff and a new leader sends an updated *JOIN REQ* message to its upstream zone. If M did not receive the *NEWSESSION* message or it just joined the network, it can search for the available groups by querying its neighbors. If a LDR receives a *JOIN REQ* message or wants to join G itself, it begins the leader joining procedure as shown in Fig.2. If the *JOIN REQ* message is received from a member M of the same zone, the LDR adds M to thedownstream node list of its multicast table. If the message is from another zone, it will compare the *depth* of the requesting zone and that of its own zone. If its zone depth is smaller, i.e., its zone is closer to the root zone than the requesting zone, it will add the requesting zone to its downstream zone list; otherwise, it simply continues forwarding the *JOIN REQ* message towards the root zone.

If new nodes or zones are added to the downstream list, the leader will check the root-zone ID and the upstream zone ID. If it does not know the root zone, it starts an expanded ring search. As the zone leaders in the network cache the root-zone ID, a result can be quickly obtained. With the knowledge of the root zone, if its upstream zone ID is unset, the leader will represent its zone to send a *JOIN REQ* message towards the root zone; otherwise, the leader will send back a *JOIN RPY* message to the source of the *JOIN REQ* message. When the source of the *JOIN REQ* message receives the *JOIN RPY*, if it is a node, it sets the isAcked flag in its membership table and the joining procedure is completed. If the leader of a requesting zone receives the *JOIN RPY* message, it will set its upstream zone ID as the ID of the zone where the *JOIN RPY* message is sent, and then send *JOIN RPY* messages to unacknowledged downstream nodes and zones.

Through the joining process, the group membership management is implemented in a distributed manner. An upstream zone only need to manage its downstream zones, and the group membership of a local zone is only managed by its leader. The zone depth is used to guide efficient tree construction and packet forwarding.

3.4.3 Multicast group leave

When a member M wants to leave G, it sends a *LEAVE*(*M;G*) message to its zone leader. On receiving a *LEAVE* message, the leader removes the source of the *LEAVE* message from its downstream node list or zone list depending on whether the message is sent from an intra-zone node or a downstream zone. Besides removing a branch through explicit *LEAVE*, a leader will remove a node from its downstream list if it does not receive the beacon from the node exceeding 2**Intervalmax*. If it's downstream zone list and node list of G are both empty and it is not a member of G either, the leader sends a *LEAVE*(zID, G) message to its upstream zone. Through the leave process, the unused branches are removed from the multicast tree.

3.5 Multicast Packet Delivery

In this section, we explain how the multicast packets are forwarded to the members.

3.5.1 Packet sending from the source

After multicast tree is constructed, all sources of the group could send packets to the tree and the packets will be forwarded along the tree. In most tree-based multicast protocols, a data source

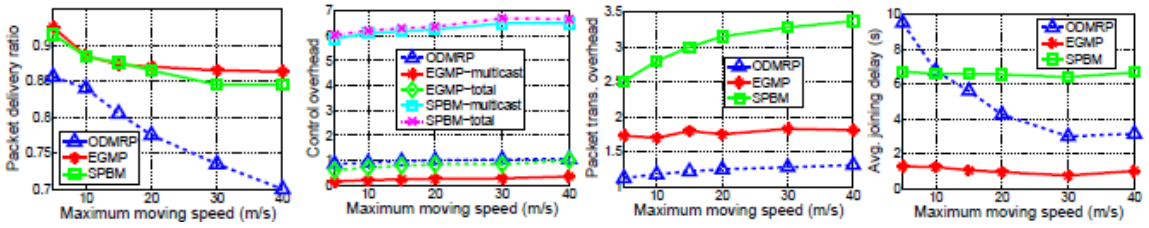

Fig 3: Performance vs maximum moving speed

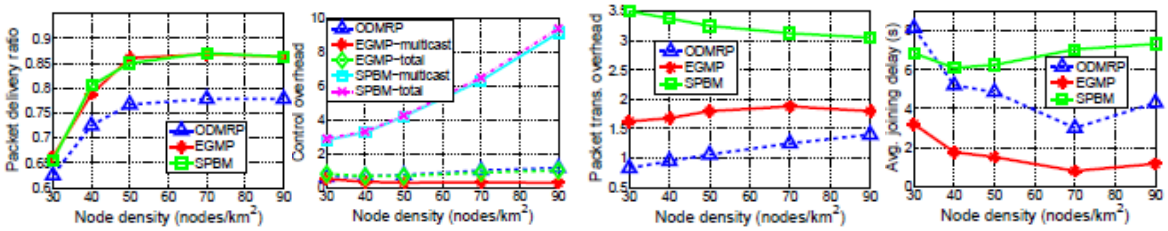

Fig 4: performance vs node density

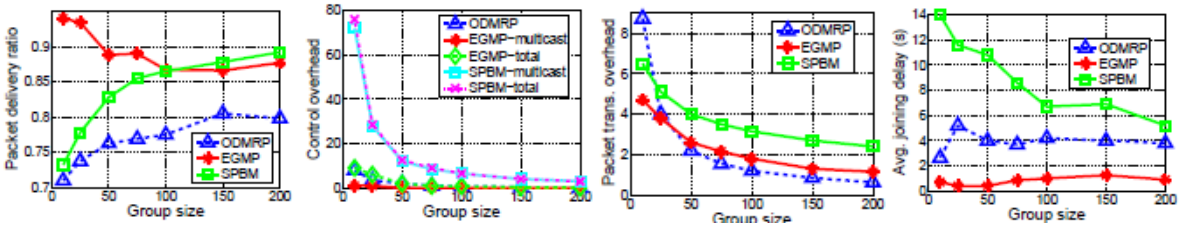

Fig 5: performance vs Group size

needs to send the packets initially to the root of the tree. The sending of packets to the root would introduce extra delay especially when a source is far away from the root. Instead, EGMP assumes a bi-directional tree-based forwarding strategy, with which the multicast packets can flow not only from an upstream node/zone down to its downstream nodes/zones, but also from a downstream node/zone up to its upstream node/zone.

A source node is also a member of the multicast group and will join the multicast tree. When a source S has data to send and it is not a leader, it checks the *isAcked* flag in its membership table to find out if it is on the tree. If it is, i.e., its zone has joined the multicast tree, it sends the multicast packets to its leader. When the leader of an ontree zone receives multicast packets, it forwards the packets to its upstream zone and all its downstream nodes and zones except the incoming one.

When a source node S is not on the multicast tree, for example, when it moves to a new zone, the *isAcked* flag will remain unset until it finishes the rejoining to G through the leader of the new zone. To reduce the impact of the joining delay, S will send packets directly to the root zone until it finishes the joining process.

3.5.2 Multicast data forwarding

In our protocol, only LDR maintain the multicast table, and the member zones normally cannot be reached within one hop from the source. When a node N has a multicast packet to forward to a list of destinations (*D1;D2;D3; : : :*), it decides the next hop node towards each destination (for a zone, its center is used) using the geographic forwarding strategy. After deciding the next hop nodes, N inserts the list of next hop nodes and the destinations associated with each next hop node in the packet header. Then N broadcasts the packet *promiscuously* (for reliability and efficiency). Upon receiving the packet, a neighbor node will keep the packet if it is one of the next hop nodes or destinations, and drop the packet otherwise. When the node is associated with some downstream destinations, it will continue forwarding packets similarly as done by node N.

4 SIMULATION RESULTS

We first compare the performance of ODMRP, SPBM and EGMP with the variation of moving speed and node density, we then study the

scalability of the three protocols with the change of group size and network size.

4.1 Effect of moving speed

When ODMRP compared with both geometric multicast protocols EGMP and SPBM are more robust to the mobility , and achieve more than 20% higher delivery ratios at the highest mobility as shown in fig 3. EGMP has the minimum control overhead and group joining delay under all the mobility. The control overhead of ODMRP and EGMP are comparable, while the overhead of SPBM is about six times their overhead. Similarly, the joining delay of SPBM is also six times that of EGMP. The joining delay of ODMRP reduces with the increase of mobility, and is still three times that of EGMP at the highest mobility.

4.2 Effect of node density

All the protocols perform better in a denser network as in fig 4. EGMP and SPBM have consistently higher delivery ratios than that of ODMRP. SPBM has a significantly higher control overhead and joining delay in a dense network as a result of its periodic multi-level flooding of membership management message, while EGMP remains to have the lowest delay as it allows group members to join and leave the group immediately on demand. SPBM has more transmissions in a sparse network due to the more frequent use of recovery forwarding of the underlying geometric unicast protocol, while the transmissions of both EGMP and ODMRP increase at a higher node density, as EGMP has more on-tree zones and ODMRP has more nodes in the forwarding mesh.

4.3 Effect of the group size

EGMP has high delivery ratios for all the group sizes as in fig 5. When there is no need of member management in a zone then it does not incur unnecessary control overhead but in contrast, SPBM and ODMRP have much lower delivery ratios when the group sizes are small because SPBM has less stable membership and ODMRP has less robust mesh paths. Due to use of periodic flooding messages regardless of the group size both SPBM and ODMRP have much higher normalized control overheads at smaller group sizes. As the group size increases, the data transmission overheads for all the protocols reduce due to the aggregations of packet transmissions. Group size has little impact on joining delay of EGMP, while SPBM has a significantly higher joining delay when the network is sparse.

4.4 Effect of the network size

In a large network, due to transmission infrastructures and its virtual-zone-based geometric membership management, EGMP performs much better than SPBM and ODMRP and has a significantly lower control overhead, lower joining delay and higher delivery ratio.

5 CONCLUSION

There is an increasing demand and a big challenge to design more scalable and reliable multicast protocol. In this paper, we propose an efficient and scalable geographic multicast protocol, EGMP. The scalability of EGMP is achieved through a virtual-zone-based structure, which takes advantage of the geometric information to greatly simplify the zone management and packet forwarding. ODMRP takes advantage of broadcasting to achieve more efficient packet forwarding, but the transmissions are much more unreliable due to its difficulty of maintaining forwarding mesh under mobility, which leads to a lower packet delivery ratio. The multicast group joining delay of ODMRP is also much higher than that of EGMP. EGMP makes use of geographic forwarding for reliable packet transmissions, and efficiently tracks the positions of multicast group members without resorting to an external location server. As compared to traditional multicast protocols, our scheme allows the use of location information to reduce the overhead in tree structure maintenance and can adapt to the topology change more quickly.

6 REFERRENCES

[1] 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.

[2] 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.

[3] X. Xiang and X. Wang. An Efficient Geographic Multicast Protocol for Mobile Ad Hoc Networks. In *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Niagara-Falls, Buffalo, New York, June 2006.

[4] 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.

[5] C. Gui and P. Mohapatra. Scalable Multicasting for Mobile Ad Hoc Networks. In *Proc. IEEE INFOCOM*, Mar. 2004.

[6] S. Roy, 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.

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

[8] X. Zhang and L. Jacob. Multicast zone routing protocol in mobile ad hocwireless networks. in *Proceedings of Local Computer Networks*, 2003(LCN 03), October 2003.