Energy Efficient Secure Mulicast Routing Data Transmission In Wireless Mesh Network

Ms.N.Nanthini[1], Dr.M.L.Valarmathi[2].
[1] Assistant Professor, [2] Associate Professor.
Department of Computer Science and Engineering,
Government College of Technology, coimbatore, India.
[1]nandhinivecphd@gmail.com@gmail.com

Abstract:-

Multicast routing for wireless mesh networks has focused on metrics that estimate link quality to maximize throughput. Nodes must collaborate in order to compute the path metric and forward data. In high-throughput multicast protocol in wireless mesh networks we identify novel attacks in wireless mesh networks. The attacks exploit the local estimation and global estimation of 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.In this paper Energy efficient based secure high-throughput multicast protocol Energy Efficient Secure - On Demand Multicast Routing Protocol(ES-ODMRP) has been implemented. ES-ODMRP ensures the delivery of data from the source to the multicast receivers even in the presence of attackers, as long as the receivers are reachable through non adversarial paths. To achieve this, ES-ODMRP uses a metric that estimate link quality to maximize the throughput and energy efficient based data transmission on network. The combination of authentication and rate limiting techniques avoid attacks against resource consumption. Also packet dropping and mesh structure attacks are avoided using Rate Guard technique.

Index Terms:- *Wireless mesh networks, high-throughput metrics, secure multicast routing, metric manipulation attacks, Minimum Energy Routing.*

I INTRODUCTION

Wireless mesh networks (WMNs) emerged as promising technology that offers low-cost high bandwidth community wireless services. A WMN consists of a set of mobile clients that communicate through a wireless backbone. Numerous applications envisioned to be deployed in WMNs, such as webcast, distance learning, online games, video conferencing, and multimedia broadcasting, follow a pattern where one or more sources disseminate data to a group of changing receivers in [2]. These applications can benefit from the service provided by multicast routing protocols.

Multicast routing protocols deliver data from a source tomultiple destinations organized i an multicast group. In the last few years, several protocols were proposed to provide multicast services for multihop wireless networks.These protocols were proposed for mobile ad hoc networks(MANETs),focusing primarily on network connectivity and using the number of hops (or hopcount) 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 [10].

Instead, given the stationary nature of WMNs, recent protocols [4] focus on maximizing path throughput by selecting paths based on metrics that capture the quality of the wireless links [5] . We refer to such metrics 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.

Minimum Energy Routing (MER) can be described as the routing of a data-packet on a route that consumes the minimum amount of energy to get the packet to the destination which requires the knowledge of the cost of a link in terms of the energy expanded to successfully transfer and receive data packet over the link as [6], the energy to discover routes and the energy lost to maintain routes.

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 [8]. 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 multihop characteristic of the communication.

II HIGH-THROUGHPUT MESH BASED MULTICAST ROUTING

Considering a multihop wireless network where nodes participate in the data forwarding process for other nodes.I 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. Below, we provide an overview of high-throughput metrics for multicast, then describe in details how such metrics are ntegrated with mesh-based multicast protocols.

We focus on ODMRP as a representative mesh-based multicast protocol for wireless networks. The protocol extension to use a high-throughput metric was first described by Roy [5].We refer to the ODMRP protocol using high-throughput metric as ODMRP-HT in order to distinguish it from the original ODMRP [13] protocol.

a. ODMRP overview

ODMRP is an on-demand multicast routing protocol [12] for multi-hop wireless networks. The source periodically recreates the mesh by flooding a message in the network in order to refresh the membership information and update the routes. 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 message, it activates the path from itself to the source by constructing and broadcasting a 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 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. If so, it makes itself a node part of the mesh and creates and broadcasts a new built upon the matched entries. Once the messages reach the source, the multicast receivers become connected to

the source through a mesh of nodes which ensures the delivery of multicast data. While a node is in the group, it rebroadcasts any non-duplicate multicast data packets that it receives. ODMRP takes a "soft state" approach in that node put a minimal effort to maintain the mesh.

b. ODMRP-HT

Protocol that enhances ODMRP with high-throughput metrics. 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) ODMRPHT uses a weighted flood suppression mechanism to flood JOIN QUERY messages instead of basic flood suppression.

C. **Estimating High-Throughput Metrics**

After forming the mesh structure, calculate the link quality which is used as path metric between all the nodes in the network. High throughput metrics link quality is used to maximize throughput By selecting paths based on the quality of wireless links, The total link quality of the path is found by aggregating the link quality of all the nodes in that path. Based on the link quality the route is selected between the source and receiver. Link quality is measured based on the PDR value of the link. PDR value for the link is calculated by the following formula,

PDR=No of. Packets received / No. of packets sends.

Routing path between source and destinations is based on link quality metric. Path selection is performed based on a metric designed to maximize throughput.

d. Attacks Against High-Throughput Multicast And Their Impact

In this section, we present attacks against high-throughput multicast protocols. In particular, we focus on attacks that validating the effectiveness of this weighted flood suppression strategy exploit vulnerabilities introduced by the use of high throughput metrics. These attacks require little resource from the attacker, but can cause severe damage to the performance of the multicast protocol. We first present the adversarial model, followed by
the details of the attacks.

*1) Resource Consumption Attacks:*The attackers are insider nodes; an effective

attack isto establish a legitimate group session with high data rate in order to deprive the network resource from honest nodes.

*2) Mesh Structure Attacks:*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 messages.

*3) Data Forwarding Attacks:*The packet dropping attack is straightforward: The attacker node on the data delivery path simply drops data packets instead of forwarding them. Local metric manipulation (LMM) and Global metric Manipulation attacks(GMM) are also detected and removed.

*4) Metric Manipulation Attacks:*It mainly includes *LMM attacks* which is 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 linkstoward itself.

5)Local Metric Manipulation (LMM) Attacks:

An adversarial node artificially increases the quality of its adjacent links, distorting the neighbours perception about these links. The falsely advertised "high-quality" links will be preferred to select the route so, malicious nodes have better chances to be included on forward group. A node can claim a false value for the quality of the links towards itself.

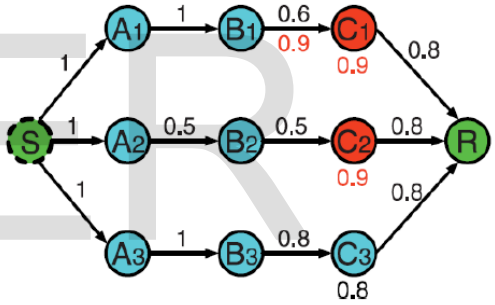

Fig 1 Metric manipulation attack during the propagation of the flood packet from the source S to receiver R.

e. Minimum Energy Routing

MER incurs higher routing overhead, but lower total energy and can bring down the energy consumed of the simulated network within range of the theoretical minimum the case of static and low mobility networks.

However as the mobility increases, the minimum energy routing protocol's performance degrades although it still yields impressive reductions in energy as compared performance of minimum hop routing protocol.

III ES-ODMRP Overview

ES-ODMRP 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 path .

The proposed work is decomposed into two parts: Estimating High-throughput Metrics and Finding Attack against High-throughput multicast. For estimating high – throughput metrics the link quality is measured based on the Packet delivery ratio (PDR) value. The second part of the work is finding the attacks against high – throughput multicast metrics based on the difference between expected Packet Delivery Ratio (ePDR) and perceived Packet Delivery Ratio (pPDR) value of the wireless link.

IV Result and Discussion:

a. ***Topology Formation And Hello Packet Sending***

Using NS-2 WMN environment is created.Initially 40 nodes are randomly placed and hello packe**t** message is send to the neighbouring nodes. Based on the sensing capability each node should identify its topology that is neighbouring nodes. Each node will send hello packets to neighbours those are all in within the communication range (Within 250 metre). Neighbour table is maintained in which the neighbour nodes of each node are maintained.

b. ***Estimating High-Throughput Metrics***

After forming the mesh structure, calculate the link quality which is used as path metric between all the nodes in the network. High throughput metrics link quality is used to maximize throughput By selecting paths based on the quality of wireless links, The total link quality of the path is found by aggregating the link quality of all the nodes in that path. Based on the link quality the route is selected between the source and receiver. Link quality is measured based on the PDR value of the link. PDR value for the link is calculated by the following formula,

PDR= No of. Packets received / No. of packets sends .

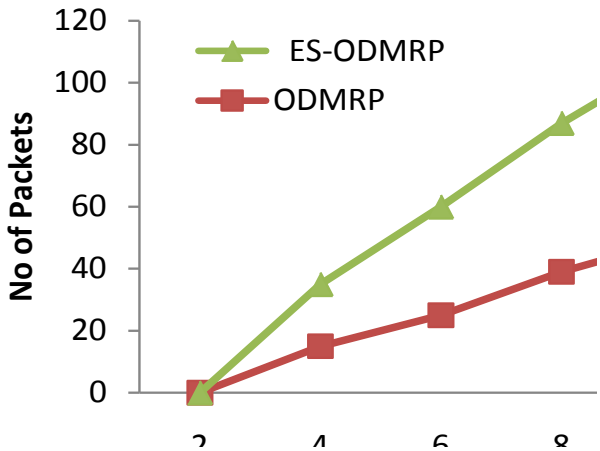

Fig 2: Throughput Performance

Routing path between source and destinations is based on link quality metric. Path selection is performed based on a metric designed to maximize throughput.

c. ***Finding Attack Against High-Throughput Multicast***

Attack detection strategy relies on the ability of honest nodes to detect the discrepancy between the expected PDR (ePDR) and the perceived PDR (pPDR). A technique called Rate Guard is proposed to eliminate the attacker. It combines the measurement-based detection and accusation based reaction techniques. Based on those values malicious nodes are detected in the network. The most straightforward method for estimating pPDR is to use a sliding window method, with pPDR calculated as pPDR = r / w, where r is the number of packets received in the window and w is the number of packets sent by the source (derived from packet sequence numbers) in the window.

To isolate attackers, accusation based reaction technique in which a node, on detecting malicious behavior, temporarily accuses the suspected node by flooding in the network message containing its own identity and the identity of the accused node, as well as the duration of the accusation. The alternate path is selected to forward the data packets between source and receiver.

d. Energy constraints on Network

The energy level on the network is must and most important one of the quick data transmission on their network. its calculated from their each node energy consumption is must of the network.

*Energy consumption = no of packets * initial energy level*

Remained energy = energy consumption – no of packets in node

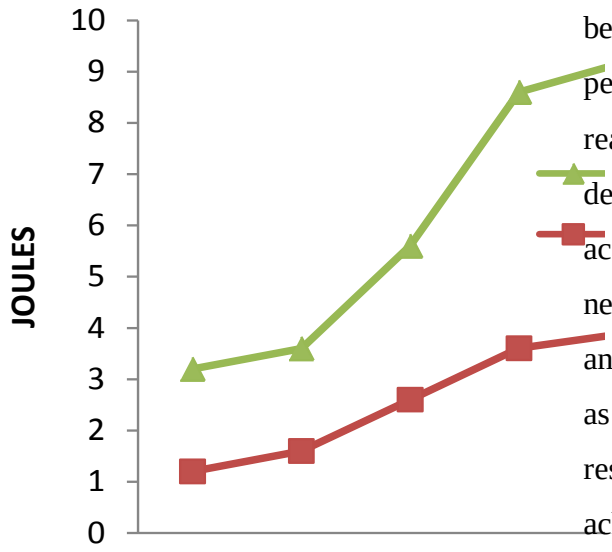

Fig 3: Energy Consumption

if any node none to data transmit that node to save the energy on the network.

V CONCLUSION AND FUTURE WORK

In this paper using a secure high-throughput multicast protocol, called ES-ODMRP, is implemented to maximize throughput of the network, and a technique called Rate Guard is implemented to eliminate the attacker. It combines the measurement-based detection and accusation based reaction techniques. ES-ODMRP ensures the delivery of data from the source to the multicast receivers even in the presence of attackers, as long as the receivers are reachable through non adversarial paths. ES-ODMRP uses a metric that estimate link quality to maximize the throughput. Measurement-based detection is a generic attack detection strategy that discrepancy between the expected PDR (ePDR) and the perceived PDR (pPDR). Accusation based reaction techniques in which a node on detecting malicious behaviour, temporarily accuses the suspected node by flooding in the network message containing its own identity and the identity of the accused node, as well as the duration of the accusation. Simulation results also shown that ES – ODMRP achieves high throughput and our defense is effective against the identified attacks, and imposes a small overhead.

They have to perform an MER used if the no data process the node to save the energy and reduce the energy consumption level. This network has to take parameters for success ratio, average end-to-end delay, throughput and consumption of energy model on this network. All the parameters are to take comparison of the network level and the Energy level on the network.

A secure multicast routing ES–ODMRP is implemented. This technique can be further improved by delivering the compensation packets through Retransmission diversity mechanism. Dropping attack only consider in ES-ODMRP other attacks such as injecting, modifying, and replaying are can be consider

these are interesting topics for fu future research.

REFERENCES

1. J. Dong, R. Curtmola, and C. Nita-Rotaru, "Secure High-Throughput Multicast Routing in Wireless Mesh Networks," IEEE Transaction On Mobile Computing MAY 2011.
2. 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.
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. 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.
5. P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS), pp. 27-31, Jan. 2002.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.

11. E.M. Royer and C.E. Perkins, "Multicast Ad-Hoc On-Demand Distance Vector (MAODV) Routing," Internet Draft, July 2000.

12. J.G. Jetcheva and D.B. Johnson, "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks," Proc. ACM MobiHoc, 2001.

13. H. Lundgren, E. Nordstrom, and C. Tschudin,"Coping with Communication Gray Zones in IEEE 802.11b Based Ad Hoc Networks," Proc. Fifth ACM Int'l Workshop Wireless Mobile Multimedia (WOWMOM'02),2002.