NEIGHBOR ATTACK AND DETECTION MECHANISM IN MOBILE AD-HOC NETWORKS

S. Parthiban[1], A. Amuthan[2], N.Shanmugam[3], K.Suresh Joseph[4]

1Sr. Tech. Asst., Department of Computer Science,Pondicherry University
parthi_ns@yahoo.com
2Associate Professor, Department of Computer Science & Engineering, Pondicherry Engineering College
2samuthan@pec.edu
3Assistant Professor, Department of Computer Science and Engineering,Kanchi Pallavan Engineering College
nkshan1@gmail.com
4 Assistant Professor, Department of Computer Science, Pondicherry University
sureshjosephk@yahoo.co.in

ABSTRACT

In Mobile Ad-Hoc Networks (MANETs), security is one of the most important concerns because a MANETs system is much more vulnerable to attacks than a wired or infrastructure-based wireless network. Designing an effective security protocol for MANET is a very challenging task. This is mainly due to the unique characteristics of MANETs, namely shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among users, limited availability of resources, and physical vulnerability. In this paper we present simulation based study of the impact of neighbor attack on mesh-based Mobile Ad-Hoc Network (MANET). And also we study the number of attackers and position affects the performance metrics such as packet delivery ratio and throughput. The study enables us to propose a secure neighbor detection mechanism (SNDM). A generic detection mechanism against neighbor attack for On Demand Routing Protocols is simulated on GlomoSim environment.

KEY WORDS

MANETs, ODMRP, SNDM, NQ, JQ, PDR

1. INTRODUCTION

A Mobile Ad hoc NETworks (MANETs) is defined as a wireless network of mobile nodes communicating with each other in a multi-hop fashion without the support of any fixed infrastructure such as base stations, wireless gateways or access points. For this reason, MANETs are also called infrastructureless or non-infrastructure wireless networks. The term ad hoc implies that this network is established for a special, often extemporaneous service customized to specific applications. MANETs enable wireless networking in environments where there is no wired or cellular infrastructure; or, if there is an infrastructure, it is not adequate or cost effective. The absence of a central coordinator and base stations makes operations in MANETs more complex than their counterparts in other types of wireless networks such as cellular networks or wireless local area networks (WiFi networks).

Security issues of MANETs in group (multicast) communications are even more challenging because of the involvement of multiple senders and multiple receivers. Although several types

DOI : 10.5121/acij.2012.3207

of security attacks in MANETs have been studied in the literature, the focus of earlier research is only on unicast (point-to-point) applications.

In tree-based multicast protocols, there is usually only one single path between a sender and a receiver, while in mesh based multicast protocols, there may be a multiple path between each sender-receiver pair. Compared to tree-based protocols, mesh-based protocols are robust and more suited in frequently changing topology systems such as MANETs. Examples of tree-based multicast protocols are MAODV [1], AMRIS, BEMRP [11] and ADMR [5]. Typical mesh-based multicast protocols are PMR, ODMRP [7], FGMP [2], CAMP [4], DCMP [3] and NSMP [6]. AMRoute and MCEDAR are hybrid multicast protocols that provide both mesh-based and tree-based infrastructure.

In this paper, we present a simulation-based study of the effects of neighbor attacks on mesh-based multicast in MANETs. We also present a solution for the neighbor attack using SNDM and a simulation-based study for the same.

2. RELATED WORK

As MANETs are dynamic in nature and has very distributed structure it is prone to many routing attacks. There are number of attacks present in the existing systems such as neighborhood, flooding, blackhole, wormhole attacks, etc.. Present system is designed only by considering the work ability and to avoid overhead caused by the transactions of packets through the network. But these systems are more vulnerable to attacks during the routing of packets from one node to other (i.e.) source to destination.
Wide research has been conducted on MANETs for providing security solutions against attack on the basis of cryptographic scheme. Some of the related works with respect to neighbor attack are

a) Propose a novel monitoring approach that overcomes some watchdog's shortcomings, and improves the efficiency in detection. To overcome false detections due to nodes mobility and channel conditions they propose a Bayesian technique for the judgment, allowing node redemption before judgment. Finally, they suggest a social-based approach for the detection approval and isolation of guilty nodes.

b) The DRI or the data table of information's routing which is used to identify malicious nodes, it consists in adding two additional bits of information. These bits have as values 0 for "FALSE" and 1 for " TRUE " for intermediate nodes answering the RREQ of node source . The Cross checking solution which consists in hoping on reliable node (nodes by which node source has forwarded the data) to transfer from the packets of data.

c) The proposed solution states that the attack is prevented based on the trust value. A trust value is defined as the ratio of no of data packets sent to the no of data packets received. To identify the misbehavior and to use the trust value to present it accurately, the routing strategy (i. e) route selection is based on not only the (present) trust values and also on the average value of the past experiences. If given more weight to the history of past experiences of the node than its recent behavior, which can prevent a node with high trust value that suddenly starts to drop package will be identified quickly turning to malicious node to disrupt network activities.

d) The sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the network redundancy. Since any packet can be arrived to the destination through many redundant paths, the idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time the sender node will buffer its packets until a safe route is identified. Once a safe route has identified, these buffered packets will be transmitted. When a RREP arrives to the source, it will extract the full paths to the destinations and wait for another RREP. Two or more of these nodes must have some shared hops (in ad hoc networks, the redundant paths in have some shared hops or nodes). From these shared hops the source node can recognize the safe route to the destination. If no shared nodes appear to be in these redundant routes, the sender will wait for another RREP until a route with shared nodes identified or routing timer expired. This solution can guarantee to find a safe route to the destination, but the main drawback is the time delay. Many RREP packets have to be received and processed by the source. In addition, if there are no shared nodes or hops between the routes, the packets will never been sent.

e) Initially each node is assigned a trust level. Then they use several approaches to dynamically update trust levels by using reports from threat detection tools, such as Intrusion Detection Systems (IDSs), located on all nodes in the network. The nodes neighboring to a node exhibiting suspicious behavior initiate trust reports. These trust reports are propagated through the network using one of our proposed methods. A source node can use the trust levels it establishes for other nodes to evaluate the security of routes to destination nodes. Using these trust levels as a guide, the source node can then select a route that meets the security requirements of the message to be transmitted.

f) This solution assumes that nodes are already authenticated and hence participate in communication. Assuming this condition, the black hole attack is discussed Our approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and it is eliminated. The source node transmits the RREQ to all its neighbors. Then the source waits for 'TIMER' seconds to collect the replies, RREP.

    a. A reply is chosen based on the following criteria, In each of the received RREP, the fidelity level of the responding node, and each of its next hop's level are checked. If two or more routes seem to have the same fidelity level, then select the one with the least hop count; else, select the one with the highest level. The fidelity levels of the participating nodes are updated based on their faithful participation in the network. On receiving the data packets, the destination node will send an acknowledgement to the source, whereby the intermediate node's level will be incremented. If no acknowledgement is received, the intermediate node's level will be decremented.

g) This method, each intermediate node is used to send backs the next hop information when it sends back an RREP message. After getting the reply message, the source node does not send the data packets but extracts the next hop information from the reply packet and then it sends a Further- Request to the next hop to verify that it has a route to the intermediate node who sends back the Further reply message, and that it has a route to the destination node.

h) Statistical based anomaly detection approach to detect the blackhole attack, based on differences between the destination sequence numbers of the received RREPs. The key advantage of this approach is that it can detect the attack at low cost without introducing extra routing traffic, and it does not require modification of the existing protocol. However, false positives are the main drawback of this approach due to the nature of anomaly detection.

i) The schemes depends on certificate based cryptography (CBC), which uses public key certificates to authenticate public keys by binding public keys to the owner's identities. A main concern with CBC-based approaches is the need for certificate-based public key distribution. Another approach is to preload each node with all others public key based certificates prior to network deployment.

j) The digital signature is a security Certificate which is a self organized and PKI authenticated by a chain of nodes without the use of a trusted third party. Authentication is represented as a set of security certificates that form a chain. Each node in the network has identical roles and responsibilities thereby achieving maximum level of node participation. Every node in the network can issue certificates to every other node within the radio communication range of each other. A certificate is a binding between a node, its public key and the security parameters Certificates are stored and distributed by nodes themselves. Every node participating in certificate chaining must be able to authenticate its neighbors, create and issue certificate for neighbors and maintain the set of certificates it has issued. The issue of certificates can be on the basis of security parameters of the node. Each node has a local repository consisting of certificates issued by the node to other nodes and certificates issued by others to the particular node. Therefore each certificate is stored twice, one by the issuer and the other for whom it is issued.

Periodically certificates from neighbors are requested and routing cache is updated by adding new certificates. If any of the certificates are conflicting, i.e., same public key to different nodes or same node having different public key, it is possible that a malicious node has issued a false certificate A node then labels such certificates as conflicting and tries to resolve the conflict. If certificates issued by any node are found to be wrong, then that node may be assumed to be malicious. If multiple certificate chains exist between a source and destination, the source selects a chain or a set of chains for authentication.

3.1 ODMRP overview

In ODMRP, the source nodes periodically broadcast the network with the route refreshment packet, called "Join Query" to refresh the membership information and update the routes. When a node receives a non duplicate Join query packet it updates source address and ID of the node from which it receives the packet, and then rebroadcasts the packet. When a Join Query packet reaches the multicast receiver, it creates and broadcasts a "Join Reply" packet. The Join Reply packet is relayed towards the multicast source via the reverse path traversed by the Join Query packet. This process constructs (or updates) the routes from sources to receivers and builds a mesh of nodes, the forwarding group.

3.2 MANET attacks

Attacks on MANETs can be classified into two categories: *active* and *passive* attacks. An active attack attempts to destroy the data being exchanged in the network. Active attacks can be divided further into two categories: *external* and *internal* attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented using standard security mechanisms such as encryption techniques or firewalls. Internal attacks are from compromised nodes that belong to the network. Since the compromised adversaries are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect compared to external attacks.

On the other hand, a passive attack affects the network performance without altering the operation of the network. Similar to internal active attacks, detection of passive attacks is also very difficult since the operation of the network itself is not affected. Effective countermeasure solutions for detecting these types of attacks have not been found yet. For this reason, studying the effects of passive and internal active attacks on multicast in MANET is our primary interest in this paper. In the following sections, we describe in the details of the neighbor attack, which is classified as passive attack.

4. Neighbor attack

The goal of the neighbor attack is to disrupt the multicast routes by making two nodes that are in fact out of each other's communication range believe that they can communicate directly with each other. If these two nodes are part of the routing mesh, the join reply packet that they exchange will be lost because there is no actual connection between them. A neighbor attacker violates the routing protocol and does not need to involve itself later in the packet dropping process, since the packets will be lost eventually due to the fake links

Upon receiving a packet, an intermediate node records its IP in the packet before forwarding the packet to the next node. However, if an attacker simply forwards the packet without recording its IP in the packet, it makes two nodes that are not within the communication range of each other believe that they are neighbors (i.e., one-hop away from each other), resulting in a disrupted route. We ran experiments with neighbor attacks implemented, and used the simulation setting as shown in the Section 3.

Figure 1 shows an example of neighbor attack where, Source node S sends Join Query to the Destination node D through its neighbor nodes J and M, when the Attacker node A receives a Join Query it forward to the node K without updating the previous hop field which makes fake link i.e., the nodes J and K assume that they are having link between them. But there is no actual connection between them. Hence the join reply packet form the node D will be lost because there is no actual connection between them.

Using simulation, we study how the number of attackers and their positions affect the performance of a multicast session in terms of packet delivery ratio, throughput, control overhead, and end-to-end delay. Our simulation results show that a large multicast group with a high number of senders and/or a high number of receivers can sustain good performance under these types of attacks due to several alternative paths in the routing mesh. The most damaging attack positions are those close to the senders and around the mesh center.

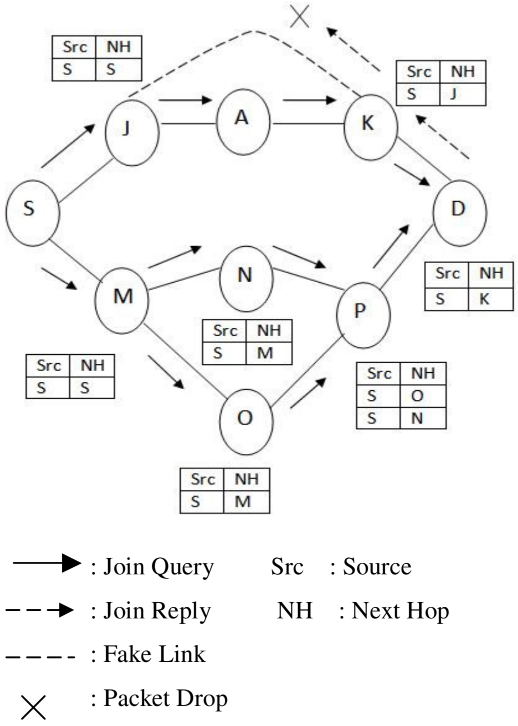


Figure 1 Example of Neighbor attack

5. Simulation Setting

Table 1: Common simulation parameters

Parameters	Values assigned
ODMRP refreshment interval	20 seconds
Channel capacity	2 Mbps
Packet size	512 bytes
Traffic model	Multicast constant bit rate
Mobility model	Random way-point
Queuing policy	First-in-first-out

6. Simulation Parameters

We conducted our experiments using Glomosim version 2.03. Our simulated network consists of 50 mobile nodes placed randomly within a 1000 m x 1000 m area. Each node has a transmission range of 250 m and moves at a speed of 1 m/s. The total sending rate of all the senders of the multicast group, i.e., the traffic load, is 1 packet/s. We use a low traffic load value to highlight the effects of the attacks on packet loss rate, as opposed to packet loss due to congestion and collisions resulting from a high traffic load.

The mobility model chosen for a mobile node was the *random way-point* model. A mobile node begins by staying in one location for a pause time of 30 seconds. Once this time expires, the mobile node chooses a random destination in the simulation area and then travels toward the newly chosen destination. Upon arrival, the mobile pauses for 30 seconds before starting the process again.

The attackers were positioned around the center of the multicast mesh in all experiments. In these experiments, we simulated four scenarios. In the first three scenarios, the attacker group was placed near the senders, near the receivers, and around the mesh center, respectively. In the fourth scenario, the attackers were uniformly distributed over the whole network. The duration of each experiment was 300 seconds in simulated time. Every experiment was repeated 10 times using 10 different randomly generated seed numbers, and the recorded data was averaged over those runs. Table 1 lists the values of the common parameters used in all the experiments. Other parameters will be given in the description of each specific experiment.

7. Performance Metrics

We use the following metrics in our study:

- **Average attack success rate:** The attack success rate of an attacker is defined as the ratio of the number of times the attacker is selected to be a multicast forwarding member over the number of times the route discovery process is initiated. The average attack success rate is the average of the attack success rates taken over all the attackers.
- **Average packet delivery ratio:** The packet delivery ratio (PDR) of a receiver is defined as the ratio of the number of data packets actually received over the number of data packets transmitted by the senders. The average packet delivery ratio is the average of the packet delivery ratios taken over all the receivers.
- **Control Overhead:** Number of control packets transmitted per data packet delivered: This measure shows the efficiency overhead in control packets expended in delivering a data packet to an intended receiver.

Following are our simulation results that demonstrate the effects of neighbor attack on mesh-based multicast in MANET between the first and the last received packets. The average throughput is the average of the per-receiver throughputs taken over all the receivers.

Figure 2.1 PDR without SNDM – Sender Constant

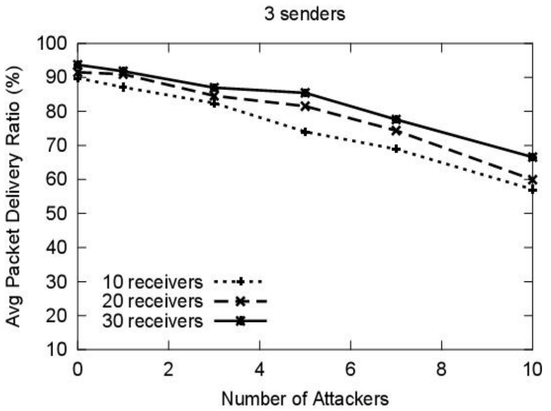
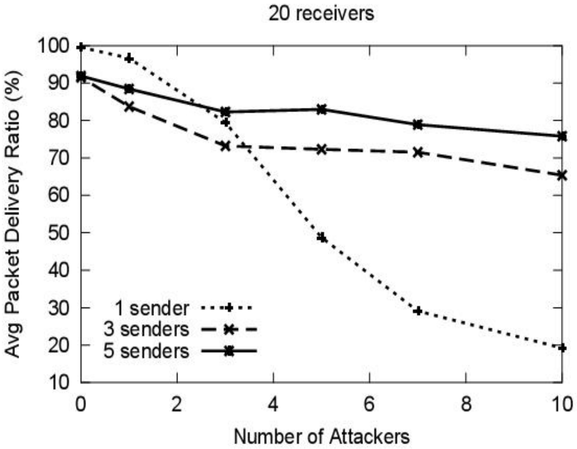


Figure 2.2 PDR without SNDM – Receiver Constant



8. Secure Neighbor Detection Mechanism

We present a secure detection mechanism that allows detecting the attacker by comparing the previous hop field of Join Query with neighbor table of the current node. In this mechanism before the Join Query flooded through the network each node send a Neighbor Query to its neighbor nodes. A node receives a Neighbor Query it add a non redundant entry to its neighbor table then the Join Query flooded through the network. The Neighbor Query process described given below.

Neighbor Table Entry

Table 2: Neighbor table content

Neighbor Address
Next Neighbor

9. Originating a Neighbor Query

When a multicast source has data packets to send but no route is known, it originates a "Neighbor Query" (NB) before Originating the "Join Query" packet. The TTL should be adjusted based on network size and network diameter, generally at the minimum size of 1. Each node generates NQ by assigning its IP address in the Neighbor IP field in the Neighbor Query Packet.

Each node in the network flushes the Neighbor table before originating NQ. (This mechanism will increase the control overhead nearly equal to the control overhead of a single sender in the same network)

Processing a Neighbor Query (NQ)

When a node receives a Neighbor Query packet:

1. Discard the packet after inserting into the Neighbor table only when the Neighbor table is empty.
2. Insert into the Neighbor table with the information of the received packet (i.e., Neighbor IP address).Only when it is not a duplicate entry. Otherwise discard the received packet. DONE.
3. Decrease the TTL field by 1.
4. If the TTL field value is less than or equal to 0, then discard the packet. DONE.
5. If the TTL field value is greater than 0, then set the node's IP Address into Neighbor IP Address field and broadcast. DONE.

Join Query Process (JQ)

After the NQ process each node has a list of its neighbor nodes address.
When a node receives a Join Query:
1. It compares the previous Hop field of Join Query with its neighbor table.
2. Check if the Previous Hop field node ID is present in the neighbor table.
3. If matches then normal JQ process will be done and the Join Query will be broadcast.
4. If not then the JQ will be discarded because the JQ is came from the non neighbor i.e., attacker.

In the Secure Neighbor Detection Mechanism when a node receives a join query it compares the previous hop field of Join Query with its Neighbor table. If a match exists in the Neighbor table, it will not forward the Join Query, it simply discard it so that Join Query packets from alternate path may reach the destination (if available).

Even if the attackers disrupt the neighbor query by sending the false neighbor address then the attacker will not be participate in the network because in our proposed mechanism the node sends the Join Query to its neighbor nodes from the neighbor table, so the attacker must send its address to the neighbor in order to participate in the network.

10. Simulation Results

In this section, we examine the packet delivery ratio of multicast sessions under Neighbor attacks with our proposed Secure Neighbor Detection Mechanism (SNDM). We analyzed various scenarios by varying the number of senders, the number of receivers, and the number of attackers. In each experiment, we measure the packet delivery ratio (PDR) as a function of the number of attackers and alternative routing paths in the mesh. The results are given in Figure 2 we can see that in almost all cases, there is a marked improvement in the PDR when compared to the graph shown in previous section for neighbor attack. But as the number of attackers increases, the PDR decreases because more number of alternate paths gets blocked by the increase in attackers. The PDR will stay constant until senders have alternate path to reach receivers.

Simulation Results: Number of Receivers

We compare the PDRs of multicast groups having 10, 20 and 30 receivers, respectively. The number of multicast senders is fixed at three. The graph in Figure 3.1 shows that, given the same number of attackers, the higher the number of multicast receivers, the higher the packet delivery ratio until enough alternate paths are available. As the number of receivers' increases, the routing mesh gets denser. If a Query packet is dropped on one path, a duplicate copy of the packet may be delivered to the receivers via other paths in the mesh and thereby taking the normal operation of the ODMRP protocol.

Simulation Results: Number of Senders

In this set of experiments, the multicast group has 20 receivers. The number of senders is set to one, three and five, respectively. Figure 3.2 shows the packet delivery ratio for one, three and five senders as a function of the number of attackers. As we would expect, the higher the number of attackers, the lower the PDR because there is more chance of the attackers surrounding the small number of senders and blocking all possible paths to the receiver. The packet delivery ratio also depends on the position of the attacker and if the attackers are scatters around the mesh then the PDR increases allowing the senders to take the alternate paths available.

Only if all alternate paths gets blocked by the attacker the PDR between those two pair decreases drastically. In all other cases, we can see an improved PDR when compared to the one with the attack. This indicates that multicast sessions with a higher number of senders perform better under this neighbor attack solution. This neighbor attack solution is works greater when a higher number of alternative routing paths in the mesh. If a Query packet is dropped by an attacker, a duplicate copy of this packet may still be delivered to the destination(s) successfully via another adversary-free path.

Figure 3.1 PDR with SNDM – Sender Constant

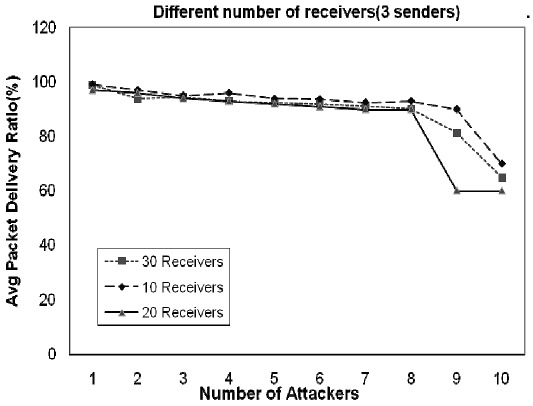


Figure 3.2 PDR with SNDM – Receiver Constant

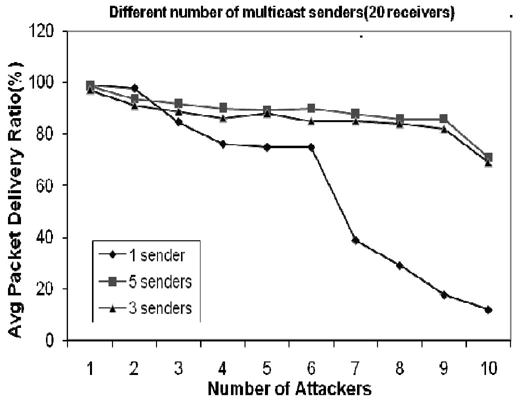
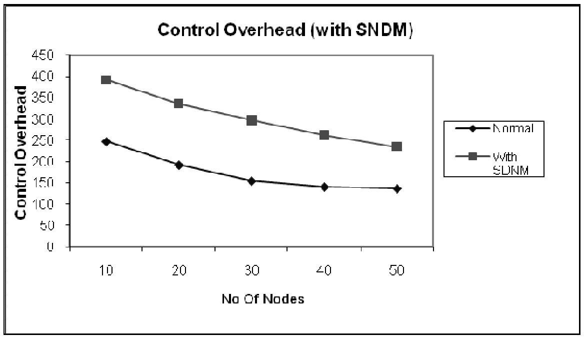


Figure 4.1 Control Overhead



11. CONCLUSION

In this paper, we have described Neighbor attack, a novel and powerful attack against on-demand ad-hoc network routing protocols. This attack allows attacker to disrupt multicast routes against previously proposed on demand ad hoc network routing protocols. Routes against previously proposed on demand ad hoc network routing protocols.

We have also presented Secure Neighbor Detection Mechanism (SNDM), a new mechanism that prevents the neighbor attack. We arrived at the following conclusions regarding neighbor attack solution. The performance of a small multicast group will degrade seriously under these types of attacks even the solution is available. A large multicast group with a high number of senders and/or a high number of receivers can sustain good performance under these conditions due to more alternative paths in the routing mesh. With respect to attack positions, areas near the senders are the most damaging positions since the original packets are intercepted early, before being duplicated at branch points. However, when the number of attackers is smaller than the number of multicast senders, the mesh center is the strongest attack position, causing the most packet losses. Our future work is to implement three-way handshake protocol for the neighbor table entry.

REFERENCES

[1] Elizabeth M. Belding-Royer and Charles E. Perkins. Multicast Operation of the Ad Hoc On-Demand Distance Vector Routing Protocol. In Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking, pages 207–218, August 1999.

[2] Ching-Chuan Chiang, Mario Gerla, and Lixia Zhang. Forwarding Group Multicast Protocol (FGMP) for Multihop, Mobile Wireless Networks. Cluster Computing, Springer Special Issue on Mobile Computing, 1(2):187–196, 1998.

[3] Subir Kumar Das, B.S. Manoj, and C. Siva Ram Murthy. A Dynamic Core-Based Multicast Routing Protocol for Ad Hoc Wireless Networks. In Proceedings of the Third ACM International Symposium on Mobile Ad Hoc Networking and Computing, pages 24–35, June 2002.

[4] J.J. Garcia-Luna-Aceves and Ewerton L. Madruga. The Core-Assisted Mesh Protocol. IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, 17(8):1380–1994, 1999.

[5] Jorjeta Jetcheva and David B. Johnson. Adaptive Demand-Driven Multicast Routing in Multi-HopWireless Ad Hoc Networks. In Proceedings of the Second ACM International Symposium on Mobile Ad Hoc Networking and Computing, pages 33–44, October 2001.

[6] Seungjoon Lee and Chongkwon Kim. Neighbor Supporting Ad Hoc Multicast Routing Protocol. In Proceedings of ACM the First ACM International Symposium on Mobile Ad Hoc Networking and Computing, pages 37–44, August 2000.

[7] Sung J. Lee, William Su, and Mario Gerla. On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks. Mobile Networks and Applications, Kluwer Academic Publishers, 7(6):441–453, December 2002.

[8] Hoang Lan Nguyen and Uyen Trang Nguyen. A Study of Different Types of Attacks on Multicast in Mobile Ad-hoc Networks. Elsevier Journal of Ad Hoc Networks, August 2006.

[9] Hoang Lan Nguyen and Uyen Trang Nguyen. Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks. In Proceedings of the Fifth IEEE International Conference on Networking, pages 149–254, April 2006.

[10] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks. In Proceedings of the Eighth ACM Annual International Conference on Mobile Computing and Networking, pages 12–23, September 2002.

[11] Tomochika Ozaki, Jaime Bae Kim, and Tatsuya Suda. Bandwidth Efficient Multicast Routing Protocol for Ad Hoc Networks. In Proceedings of the Eighth IEEE International Conference on Computer Communications and Networks, pages 10–17, October 1999

[12] Luo Junhai, Ye Danxia, Xue Liu, and Fan Mingyu, A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks, in: IEEE Communications Surveys & Tutorials, 11 (1) (2009), pp.78-91.

[13] V. Palanisamy, P.Annadurai, Impact of Rushing attack on Multicast in Mobile Ad Hoc Network, in (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009

[14] Dr. Aditya Goel, Ajaii Sharma, Performance Analysis of Mobile Ad-hoc Network Using AODV Protocol, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (5)

Authors

S. Parthiban, currently working as Senior Technical Assistant in the Department of Computer Science, Pondicherry University, Puducherry. Completed his M.E. in Computer Science & Engineering from Anna University, Chennai.

A. Amuthan, currently working as Associate Professor in the department of Computer Science & Engineering, Pondicherry Engineering College, Puducherry. Completed his Under graduate B.Tech in Computer Science & Engineering from Pondicherry Engineering College, M.E. from College of Engineering, Anna University, Chennai. He is currently persuading his doctorate in the area of Information Security at Pondicherry Engineering College under Pondicherry Universi*ty*.

N.Shanmugam working as Assistant Professor in Department of Computer Science and Engineering, Kanchi Pallavan Engineering College, Kolivaakam. Completed his M.E. in Computer Science & Engineering from Anna University.

K.Suresh Joseph working as Assistant Professor in Department of Computer Science, Pondicherry University. Completed his B.E. in Computer Science & Engineering from University of Madras, M.E. from Bharathiyar University, Tamil Nadu. He is currently persuading his doctorate in at Anna University, Coimbatore.