Security Techniques against Internal Attack in PUMA

Priyanka P. Palkar[1], Prof. V. S. Kadam[2]
Department of Computer Engineering
[1, 2] Sinhgad Institute of Technology, Lonavala, India

Abstract- *Mobile ad hoc networks (MANETs) play a significant role in the communication that is provisionally and promptly in the network. In MANET, the group communication-based applications use the multicast routing protocol where there is single sender node and group of receiver nodes. The benefits of multicast routing protocols are the capability to reduce communication costs and saving the network resources by reproduction of the message over the shared network. Security is the main dispute for multicast routing protocol in MANET as it includes large participants. Security issues become more rigorous in multicast communication due to its high variedness and routing difficulty. In this paper, we consider the internal attack, namely Multicast Announcement Packet Fabrication Attack on PUMA (Protocol for Unified Multicasting through Announcements). We proposed the security techniques to detect the attacks such as multicast activity-based overhearing technique, i.e., traffic analysis-based detection method with unique key_value.*

Keywords- MANET, group communication, PUMA, MA Fabrication Attack, Key Exchange

I. INTRODUCTION

In multicasting, there is one source and a group of destinations. The relationship is either one to many or many to many. In this type of communication, the source address is a unicast address, but the destination address is a group address, a group of one or more destination networks in which there is at least one member of the group that is interested in receiving the multicast data. The group address defines the members of the group. The purpose of a multicast routing protocol for MANET is to maintain the dissemination of data from a sender to all the receiver of a multicast group with the proficient use of accessible bandwidth. Multicasting is very essential in MANET because it reduces bandwidth utilization and broadcasting cost of communication. The multicast routing protocol is further categorized into tree-based, mesh-based and hybrid-based multicast routing protocol depending upon how the paths among group nodes are created.

In tree based multicast routing protocol, there is the establishment of single path between two nodes. Such protocols are bandwidth efficient and power efficient as they require less number of information. In mesh based multicast routing protocol, the set of interrelated nodes forms the mesh structures. The mesh establishment is done by using core points and route discovery is done by broadcasting the information. Such protocols are vigorous in character but protect complex structure provoking control overhead. Hybrid multicast routing protocols are the grouping of characteristics of both mesh-based and tree-based multicast routing protocol. PUMA is mesh-based multicast routing protocol and MAODV is tree-based multicast routing protocol[4].

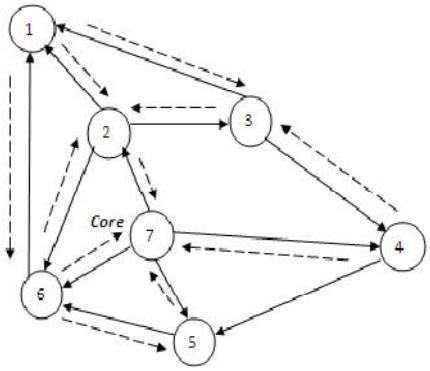
Security is a vital essential in MANET environments. Due to the lack of a trusted centralized authority, lack of trust relationships between nodes, dynamic network topology, low bandwidth, and battery and memory constraints of mobile devices, MANETs are more vulnerable to security attacks as compared to wired network. The security issue of MANETs in group communications is even more difficult because of the participation of many sources and many destinations. Multicast routing protocols are very open to different kinds of security attacks. Security attacks are of two types, Active attacks and Passive attacks. Further Active attacks are classified into internal attacks and external attacks. External attacks can be detected by using different mechanisms but internal attacks are difficult to detect as they are under transmission range of authenticated nodes.

Several security solutions are present for internal attacks in MANET. Using these solutions in the multicast routing protocol is not easy because of the complex structure of multicast routing protocol and involvement of large number of nodes. We consider some techniques against internal attacks in PUMA. In this paper, we organize as the following sections: Section II describes the overview of PUMA. In section III we present internal attack- MA fabrication attack in PUMA. Section IV shows security technique algorithm. Section V shows the impact on the performance metric of PUMA using NS2 result. Finally the conclusion of the paper is described in the Section VI.

II. OVERVIEW OF PUMA

Protocol for unified multicasting thorough announcement (PUMA) is a source-shared mesh based multicast routing protocol in MANET. It is receiver-initiated protocol, which means, the establishment of route is initiated only when receiver wants to link the multicast group or it has

information to send to group of receivers. PUMA has distinctive feature that is PUMA independent of any unicast routing protocols for its fundamental routing operations. A single control packet, Multicast Announcement (MA), is used by PUMA for creating and maintaining mesh structure, selecting the core node, forwarding the data packets[2].



Connectivity List at node 3

Neighbor	Parent	MA (distance_core)	Key_value
2	7	1	1287
1	2	2	9875
5	7	1	2579

Fig 1: Multicast Announcements

The figure shows the Node 3 has three entries in its connectivity list for neighbors 2, 1, and 4. However it chooses the entry it receives from 2 and 4 as the best entry, because it has the shortest distance to core and has been received earlier that the one from node 1. Node 3 uses this entries to generate its own multicast announcement.

III. MULTICAST ANNOUNCEMENT (MA) FABRICATION ATTACK

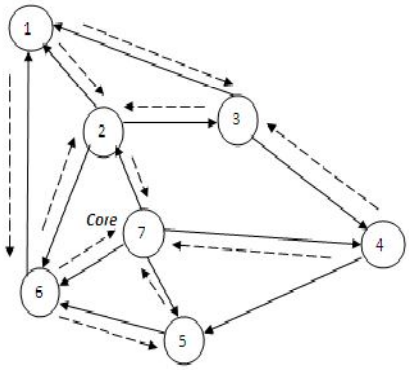
The presence of internal attack is very complex to analyze in multicast group communication as they are the authenticated nodes of the group. The PUMA's control packet are easily effected by the internal attack, attacker modifies the MA (Multicast Announcement) important field distance_core value and the unique key_value assigned to it. Such attacker denies following the procedure which is defined by the multicast routing group. They do not cooperate for the establishment of preeminent route among the receiver and the core. Due to all these, the attacker generates negative impacts on protocol performance metrics such as end-to-end delay and PDR. There are some malicious activities, attacker can do on PUMA[1];

1) Attacker refused to choose the valid parent
2) Create MA packet for non-existing parent
3) Falsely claim distance_core value

IV. PROPOSED SECURITY TECHNIQUES

In the proposed work, though we study secure multicast, no strong parameter is considered for security other than distance_core parameter. Also considering only distance_core may lead to high false positive ratio, thus to improve the security of the multicast network. We can assign a unique key value to all network nodes. While exchanging the MA packets, the nodes also exchange its key value (random generated integer value) to neighbor nodes to core. Thus core node can check the integrity of the key and identify attacker node, if any found.

Node 1 is an attacker



Connectivity List at node 3

Neighbor	Parent	MA (distance_core)	Key_value
2	7	1	1287
1	2	2	5468
5	7	1	2579

Fig 2: Attacker Detection

Parent	Distance_core	Received Time	Key_value

Fig 3 : MA packet with Key_value

We have proposed the activity-based overhearing method along with key exchange to detect the MA fabrication. The MA packet has been modified by the additional parameter i.e. key_value. Figure 1 and Figure 2 shows the detection of attacker. As the core node communicates with the each node, it has the integrity of the key of each neighbor node. In figure 2, node 1 is an attacker which exchanges the incorrect key with the core. The core match the key_value exhanged with the key present in its connectivity list , if match not found then node is added to the blacklist.

Algorithm for the MA fabrication Attacker Detection with key exchange

Int identify(): executed at each node after receiving multicast announcement packet

1. assign key_value to reach node
2. receive MA packet from the neighbor; (ma along with key_value)
3. int distance_diff = 0;
4. int failure_tally = 0;
5. tempnode = get_rear_message_cache();
6. if(tempnode == NULL)then
   Printf("message_cache is empty");
7. else
   Distance_diff = ma.core_distance - tempnode.core_distance;
8. end_if
9. if (distance_diff > 1) and (ma.received_time < temp.originated_time) and (ma.key_value != temp.key_value) then failure_tally ++;
10. else failure_tally = failure_tally;
11. else if (ma.core_distance < temp.core_distance) and (ma.next_hop == node_id) then failure_tally++;
12. else failure_tally=failure_tally;
13. end_if

Int collect_witness (): Excecuted at each node when failure_tally exceeds threshold value

1. send request to neighbors in the status multicast member
2. collect opinion about target node
3. failure_tally=failure_tally+neighbours_failure_tally

Int reaction():executed at each node

1. if (failure_tally > threshold) then
2. generate warning message
3. add this node in black_list by each node
4. end if

V. SIMULATION RESULTS

A. Simulation Environment

We performed our simulation [8] using separate event network simulator ns2.3.4. Our network scenario consists of randomly placed 25 nodes within 1,200 x 1,200 m area. Simulation time was 300 seconds. Nodes were use 2-Mbps transmission rate with transmission range 250-m as we used IEEE 802.11 for MAC protocol. Data packet rate was 512bytes. We used PUMA network layer multicast routing protocol with its default routing parameter values. We used 15 receivers with one sender and source sends packet with size 512 bytes per second. Attackers are randomly placed and randomly activated in order to imitate arbitrary nature of malicious node.

B. Performance Analysis

Figure 6 shows the Packet Delivery Ratio (PDR) of multicast routing protocol PUMA against the number of MA fabrication. If the number of attackers increases then the PDR value is gradually decreases correspondingly.

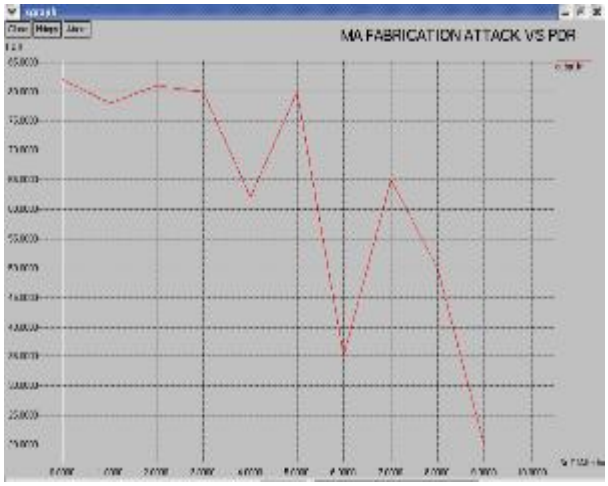


Fig 4: MA fabrication attack vs PDR

Figure 5 explains the multicast routing protocol control overhead against the number of attackers. Figure 6 shows the throughput fluctuation when the data packet attackers increase in PUMA. The throughput variation induced by the attacker is very less with respect to number of attackers in PUMA.

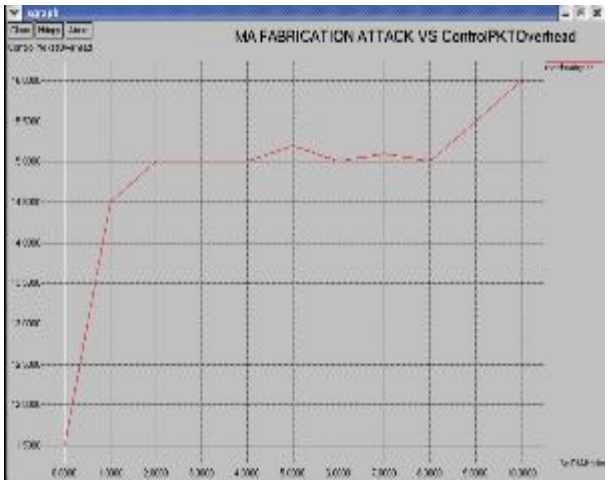


Fig 5: MA fabrication attack vs control packet overhead

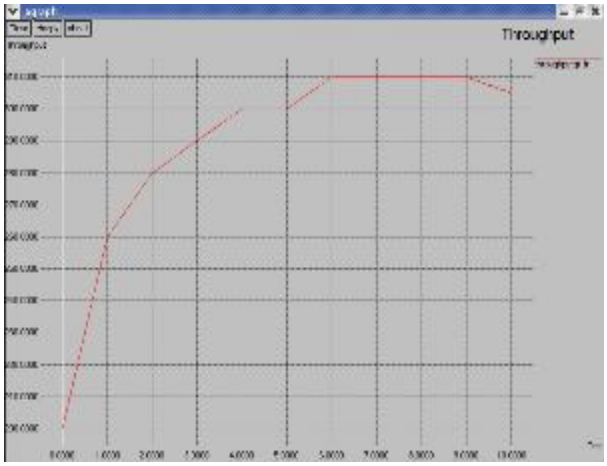


Fig 6: MA fabrication attack vs Throughput

VI. CONCLUSION

Security in multicast routing in MANET is very dangerous. In multicast routing, sender node sends data packet to group of nodes. So it requires less the cost of communication. Multicast routing protocols are more exposed to various types of attack. In this paper we have analyze the MA fabrication attack in PUMA. Simulation results clearly show the impacts of the MA fabrication attack on the performance metrics of PUMA. In future, we will study more multicast routing protocols, possible internal attacks and their appropriate techniques.

REFERENCES

[1] A. Menaka Pushpa, Dr. K. Kathiravan "Secure Multicast Routing Protocol against Internal Attacks in Mobile Ad Hoc Networks." 2013 IEEE GCC Conference and exhibition, November 17-20, Doha, Qatar.

[2] Ravindra Vaishampayan and Garcia-Luna-Aceves, “Efficient and Robust Multicast Routing in Mobile Ad Hoc Networks”, in Proceedings of IEEE Conference on Mobile Ad-hoc and Sensor systems, October 2004.

[3] Djamel Djenouri and Nadjib Badache, “MANET: Selfish behavior on packet forwarding”, Encyclopedia of Wireless and Mobile Communications DOI: 10.1081/E-EWMC-120043599, Taylor & Francis,2008

[4] Luo Junhai, Ye Danxia, Xue Liu and Fan Mingyu, “A survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks”, IEEE Communications Surveys & Tutorials, Vol.11, No. 1, First Quarter 2009

[5] Hang Lan Nguyen, Uyen Trang Nguyen, “A Study of different attacks on multicast in mobile ad hoc networks”, Elsevier Journal of Ad Hoc Networks, pp. 32-46, 2008.

[6] Kargl, F., Klenk, A., Weber, M., Schlott, S, “Advanced detection of selfish or malicious nodes in ad hoc networks”, 1st European Workshop on Security in Ad-hoc and Sensor Networks, ESAS 2004, Heidelberg, Germany, Aug 5–6, 2004.

[7] Marti, Sergio, et al. "Mitigating routing misbehavior in mobile ad hoc networks. "International Conference on Mobile Computing and Networking: Proceedings of the 6th annual international conference on Mobile computing and networking. Vol. 6. No. 11. 2000.

[8] The network simulator - ns2. http://www.isi.edu/ nsnam/ns/