STUDY OF DIFFERENT ATTACKS ON MULTICAST MOBILE AD HOC NETWORK

[1]N.SHANTHI, [2]DR.LGANESAN AND [3]DR.K.RAMAR

[1]Asst. Prof. Dept. of ECE, National Engineering College, K.R.Nagar, Kovilpatti - 628 503

[2]Head & Prof., Dept. of CSE, Alagappa Chettiar College of Engineering and Technology, Karaikudi.

[3]Head & Prof, Dept. of CSE, National Engineering College, K.R.Nagar, Kovilpatti - 628 503.

Tamil Nadu, India.

Email : [1]shamathig@gmail.com Fax: (04632) 232749

ABSTRACT

Multicast network support is becoming an increasingly important technology for both military and commercial distributed and group based applications. The security services such as confidentiality, authenticity and data integrity are necessary for both wired and wireless networks to protect basic applications. In this paper we present a simulation based study of the impact of different types of attacks in mobile ad hoc networks. We consider the most common type of attacks namely Gray hole attack and Worm hole attack. Specifically, we study how these attacks affect the performance metrics of a multicast session such as packet delivery ratio, packet latency and packet-consumed energy.

Keywords: *Multicast, Security threats, Performance analysis, Ad hoc Network*

1. INTRODUCTION

A mobile ad hoc network [14,15,1,6,7 & 16] is a self – organizing system of mobile nodes that communicate with each other via wireless links with no infrastructure or centralized administration such as base stations or access points. Nodes in a MANET operates both as hosts as well as routers to forward packets to each other. MANETS are suitable for applications, in which no infrastructure exists such as military, emergency rescue and mining operations.

In these applications, communication and collaboration among a given group of nodes are necessary. Instead of using multiple unicast transmissions, it is advantageous to use multicast in order to save network bandwidth and other resources, since a single message can be delivered to multiple receivers simultaneously. Multicast routing protocols can be classified into two groups: tree based and mesh based. In a multicast routing tree, there is usually only one single path between a sender and a receiver, while in routing mesh, there may be multiple paths between sender – receiver pairs. Example of tree based multicast routing protocols are MAODV[8], AMRIS[17], BEMRP[9] and ADMR[10]. Typical mesh based multicast routing protocols are ODMRP[2], CAMP[3], DCMP[11] and NSMP[12].

Among all the research issues, security is an essential requirement in ad hoc networks. Compared to wired networks, MANETS are more vulnerable to security attacks due to the lack of a trusted centralized authority, easy eaves dropping because of shared wireless medium, dynamic network topology, low bandwidth, battery power and memory constraints of the mobile devices. The security issue of MANETS in group communication is even more challenging because of multiple senders and multiple receivers. Several types of security attack in MANETS have been studied in the literature, and the focus of earlier research is on unicast applications. The impacts of security attacks on multicast in ad hoc networks have not yet been solved.

In this paper, we present simulation-based study of the effects of different types of attacks on tree-based multicast in MANETS. We consider the most common types of attacks namely Gray hole attack and Wormhole attack.

2. MULTICAST SECURITY

Wireless mobile ad hoc nature of MANET brings new security challenges to network design. Mobile ad hoc networks, due to their unique characteristics, are generally more vulnerable to information and physical security threats than wired networks or infrastructure – based wireless networks. Here, we explore the various security requirements (goals) for wireless ad hoc network and the different types of threats on ad hoc network faces. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication.

Multicast security issues and proposed solutions have been studied in [4, 13]. The primary objectives of a multicast security infrastructure are to maintain secrecy and guarantee authentication for all group communication so that only legitimate senders can multicast packets to the group and only packets sent by legitimate group members are accepted. Other security concerns include anonymity, non-repudiation, access control, trust issues, maintaining service availability to protect the network from clogging attacks, etc. Security in multicast is thus considerably more complicated than in the unicast case. Most unicast solutions are prohibitively inefficient for multicast scenarios. Factors affecting security [13] are group type, group size, member (node) characteristics (power, storage, availability), membership dynamics, membership control, number and type of senders, volume and type of traffic and routing algorithm used. Attacks on routing mechanisms are becoming widespread. Thus multicast security is a fairly complex multi-faceted, multi-layered problem. These requirements are even more difficult to fulfil in ad hoc networks where bandwidth, storage and energy constraints of the nodes pose additional problems when coupled with mobility and dynamically changing topology in the absence of a centralized infrastructure.

2.1. Issuers in secure multicast routing

The fundamental aspects of computer security like confidentiality, integrity, authentication and non-repudiation are valid when production of routing in network is discussed.

Confidentiality ensures that classified information in the network is never disclosed to unauthorized entities. Sensitive information, such as strategic military decisions or location information requires confidentiality. Leakage of such information to enemies could have devastating consequences.

Integrity guarantees that a message being transferred between nodes is never altered or corrupted. Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network.

Availability implies that the requested services (e.g. bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system. Availability of a network can be tempered for example by dropping off packets and by resource depletion attacks.

Authenticity is a network service to determine a user's identity. Without authentication, an attacker can impersonate any node, and in this way, one by one node, it can gain control over the entire network.

Finally, *non-repudiation* ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes.

3. SECURITY ATTACKS AN AD HOC ROUTING PROTOCOL

The complexity and uniqueness of MANETs make them more vulnerable to security threats than their wired counterparts. Attacks on ad hoc wireless networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not.

Passive attacks: A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, there by making it impossible for the attacker to get useful information from the data overhead.

Active attacks: An active attack attempts to alter to destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network.

Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication.

Both passive and active attacks can be made on any layer of the network protocol stack. This section however, focuses on network layer attacks only (routing attacks). Depending upon the various attacking behavior routing attacks can be classified into five categories: attacks using information disclosure, impersonation (masquerading or spoofing), modification, fabrication, and replay of packets. Among these information disclosure is a passive attack while the rest fall under the active category.

4. ATTACKS USING FABRICATION

In fabrication attacks, an intruder generates false routing messages, such as routing updates and route error messages, in order to disturb network operation or to consume other node resources. A number of fabrication based attacks are presented below:

4.1. Resource Consumption Attack

In this attack, a malicious node deliberately tries to consume the resources (e.g. battery power, bandwidth, et.,) of other nodes in the network. The attacks could be in the form of unnecessary route request control messages, very frequent generation of beacon packets, or forwarding of stale information to nodes.

4.2. Rushing Attack

On demand routing protocols that use route discovery process are vulnerable to this type of attack. An attacker node which receives a “route request” packet from the source node floods the packet quickly through out the network before other nodes which also receive the same “route request” packet can react. Nodes that receive the legitimate “route request” packet assume those packets to be the duplicates of the packet already received through the attacker node and hence discard those packets. Any route discovered by the source node would contain the attacker node as one of the intermediate nodes. Hence the source node would not be able to find secure routes.

4.3. Black Hole Attack

In this type of attack, a malicious node falsely advertises good path (e.g., shortest path or most stable path) to the destination node during the path finding process. The intension of the malicious nodes could be to hinder the path finding process or to interrupt all the data packets being sent to the concerned destination node.

4.4. Gray hole attack

We now describe the gray hole attack on MANETS. The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainly [5]. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A gray hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult.

4.5. Wormhole attack

In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multihop route, for example, through use of a single long-rang directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, since it can overhear them in wireless transmission and tunnel

them to the colluding attacker at the opposite end of the wormhole.

If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways. The attack can also still be performed even if the network communication provides confidentiality and authenticity, and even if the attacker has no cryptographic keys. Furthermore, the attacker is invisible at higher layers; unlike a malicious node in a routing protocol, which can often easily be named, the presence of the wormhole and the two colluding attackers at either endpoint of the wormhole are not visible in the route. In the fig (1), *M1* and *M2* are two malicious nodes that encapsulate data packets and falsified the route lengths. Suppose node *S* wishes to form a route to *D* and initiates route discovery. When *M1* receives a *RREQ* from *S*, *M1* encapsulates the *RREQ* and tunnels it to *M2* through an existing data route, in this case {*M1 --> A --> B --> C --> M2*}. When *M2* receives the encapsulated *RREQ* on to *D* as if had only traveled {*S --> M1 --> M2 --> D*}. Neither *M1* nor *M2* update the packet header. After route discovery, the destination finds two routes from *S* of unequal length: one is of 5 and another is of 4. If *M2* tunnels the *RREP* back to *M1*, *S* would falsely consider the path to *D* via *M1* is better than the path to *D* via *A*. Thus, tunneling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

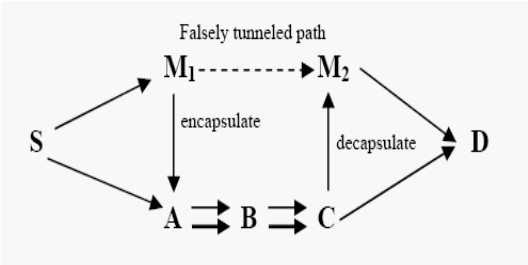

Figure 1. Path length spoofed by tunneling

5. SIMULATION ENVIRONMENT

This section describes the parameters and performance metrics used in our simulation.

5.1. SIMULATION PARAMETERS

We conducted our simulation using NS-2 simulator, a scalable simulation environment for wireless network systems. Our simulated network consists of 100 nodes placed randomly with in 1500x300m area. Each node has a transmission range of 250m and moves at a speed of 10m/s. The total sending rate of all the senders of the multicast group, i.e., the traffic load is 1Mbps. We use a high traffic load value, highlight the effects of the attacks on the packet loss rate, as opposed to packet loss due to congestion and collisions from a high traffic load. “Table 1” lists the values of the common parameters used in all our simulation setup.

Table 1. Simulation parameters

Parameter	Values
Channel capacity	2Mbps
Packet size	512bytes
Traffic model of sources	Constant bit rate
Mobility model	Random way point [25]
Path loss model	Two – ray (26)
Queuing policy at routers	First-in-first-out

6. PERFORMANCE METRICS:

We use the following metrics in our simulation.

- Packet Delivery ratio
- Packet Latency
- Packet Consumed energy.

7. SIMULATION RESULTS:

7.1. Load vs Packet Latency

This set of simulations compares the performance of multicast operation over AODV protocol during its normal operation, introducing both gray hole attack and worm hole attack, into the network and then using the security mechanisms such as RSA & MD5 algorithm to secure the MAODV protocol performance against these attacks by varying the number of multicast receivers as 10, 20, 40 and 60 respectively. The number of multicast sender is one. In these graphs, as the data rate (Mbps) is increased, the packet latency rate of the malicious node also rises, shown in “figures 2,3 and 4”.

The longer legitimate JOIN QUERY packets are delayed at intermediate nodes, the more rushed JOIN QUERY packets arrive at the destinations as the first JOIN QUERY of a route refreshment interval, allowing more attackers to be selected into the forwarding group. We also note that the higher

the number of multicast receivers, the higher the attack success rate.

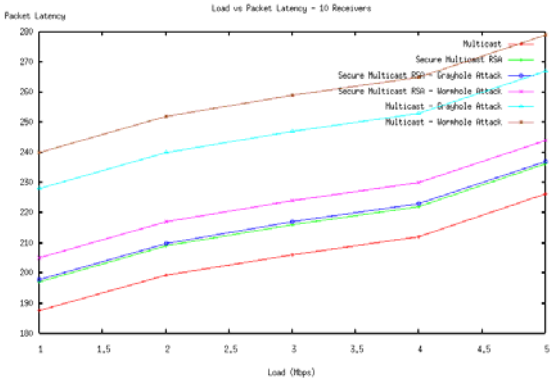

Figure 2. Load vs Packet Latency
(No of receivers - 10)

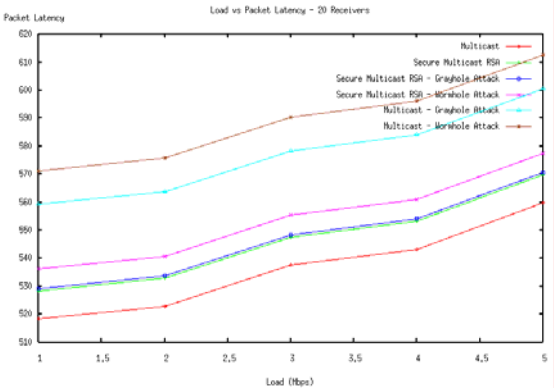

Figure 3. Load vs Packet Latency
(No of receivers - 20)

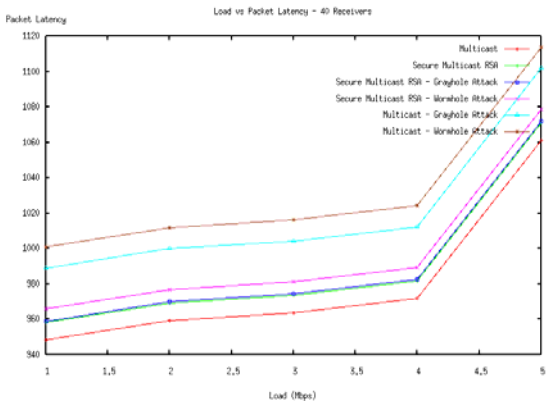

Figure 4. Load vs Packet latency
(No of receivers - 40)

7.2. Load vs Packet Delivery Ratio

As the data rate (Mbps) of legitimate nodes increases, the packet delivery ratio of malicious node decreases. We may also note that the higher the number of multicast receivers, the lower the packet delivery ratio by the malicious nodes. These performance results are shown in the following "figures 5,6 and 7".

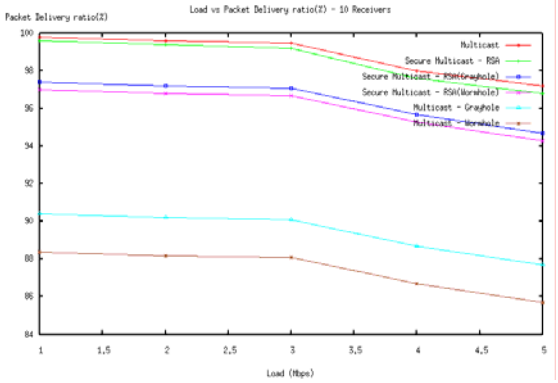

Figure 5. Load vs Packet Delivery ratio
(No of receivers - 10)

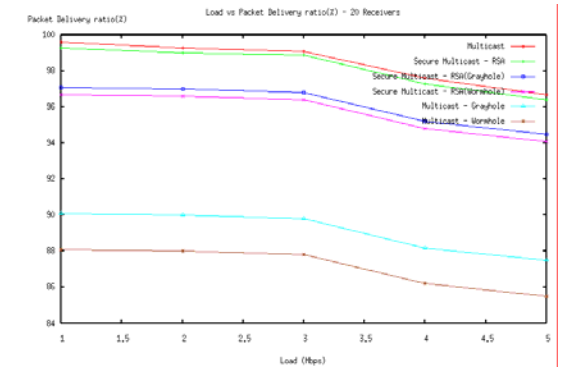

Figure 6. Load vs Packet Delivery ratio
(No of receivers - 20)

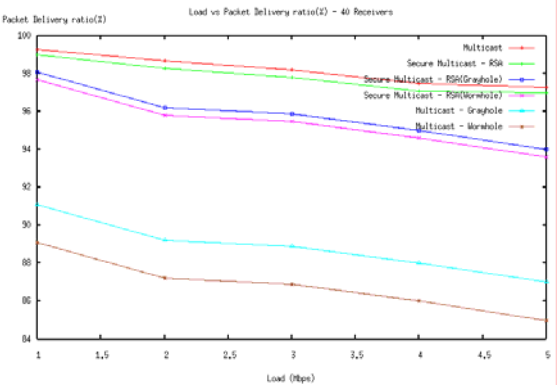

Figure 7. Load vs Packet Delivery ratio
(No of receivers - 40)

7.3. Load vs Packet Consumed Energy

From the graph, it is observed as the number of multicast receiver increases, the energy consumed by the malicious nodes to forward the packet also increases. These comparisons are shown in "figures 8, 9 and 10".

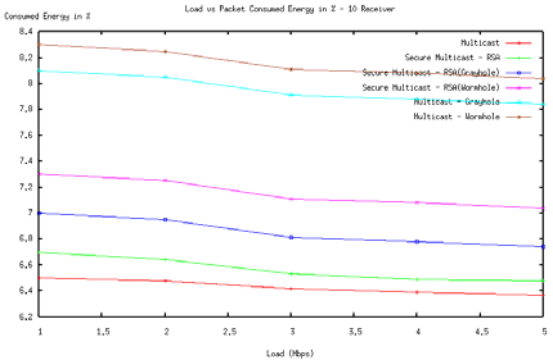

Figure 8. Load vs Packet Consumed Energy (No of receivers - 10)

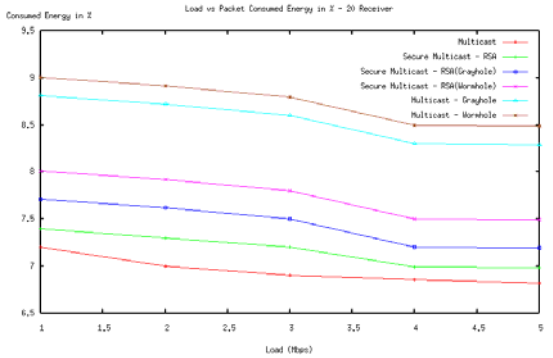

Figure 9. Load vs Packet Consumed Energy (No of receivers - 20)

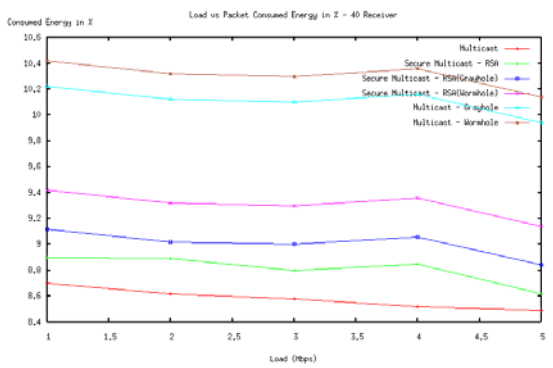

Figure 10. Load vs Packet Consumed Energy (No of receivers – 40)

CONCLUSION:

The routing protocols for Mobile Ad hoc network has to make the basic requirements by dynamically changing network topologies rather well. However, the security issues have been left primarily ignored. The performance of a multicast session in a MANET under attack depends heavily on many factors such as the number of multicast receivers, the number of multicast senders, Our simulation results ensures that the more attackers there are in the network, they cause more damage on a multicast session from the view point of authentication, integrity and confidentiality. We also note that although the operation of Gray hole attack and Worm hole attacks are different, they both cause the same degree of damage to the performance of a multicast group. In our simulation, we have made the performance comparison of MAODV protocol for three different conditions.

REFERENCE:

[1]. L. Zhou and Z.J. Haas. Securing Ad Hoc Networks. *IEEE Network Magazine*, special issue on networking security, 13(6):24–30, Nov,Dec 1999.

[2]. S.J.Lee, W.Su., M.Gerla, On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks, *ACM/Kluwer Mobile Networks and Applications* 7(6) (2002) 441-453.

[3]. J.J.Garcia-Luna-Aceves, E.L.Madruga, The Core-Assisted Mesh Protocol, *IEEE Journal on selected Areas in Communications* 17 (8) (1999) 1380-1994.

[4]. M. J. Moyer, J. R. Rao, and P. Rohatgi. A Survey of Security Issues in Multicast Communications. *IEEE Network Magazine*, 13(6):12–23, Nov/Dec 1999.

[5]. H.Deng, H.Li, and D.P.Ararwal, "Routing security in wireless Ad hoc networks", *IEEE Communication magazine*. Vol. 40, No.10. Oct.2002.

[6]. J-P. Hubaux, L. Buttyan, and S. Capkun. The Quest for Security in Mobile Ad Hoc Networks. *In Proceedings ACM Symposium on Mobile Ad hoc Networking and Computing (MOBIHOC)*, 2001.

[7]. J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. *In Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, pages 85–97, 1998.

[8]. E.M.Royer, C.E.Perkins, Multicast operation of the ad hoc on demand distance vector routing protocol, *in:Proceedings of MobiCom'99*, Seattle, WA, August 1999.

[9]. T.Ozaki, J.b.Kim, T.Suda, bandwidth efficient multicast routing protocol for ad hoc networks, *in: proceedings of IEEE ICCCN'99*, October 1999, pp. 10-17.

[10]. J.G.Jetcheva, D.B.Johnson, Adaptive demand-driven multicast routing in multi-

hop wireless ad hoc networks, *in: Proceedings of ACM MobiHoc'01, Long beach*, CA, October 2001.

[11]. S.K.Das, B.S.Manoj, C.Siva Ram Murthy, A dynamic core-based multicast routing protocol for ad hoc wireless networks, *in: Proceedings of ACM MOBIHOC* 2002, June 2002, pp 24-35.

[12]. S.Lec, C.Kim, Neighbor supporting ad hoc multicast routing protocol, *in: Proceedings of ACM MOBIHOC* 2000, August 2000, pp.37-50

[13]. R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas. Multicast Security: a Taxonomy and Some Efficient Constructions. *In Proceedings of IEEE INFOCOM*, pages 708–716, Mar 1999.

[14]. S. Jacobs and M.S. Corson. MANET Authentication Architecture. *Internet Draft, IETF*, August 1998.

[15]. *Mobile Ad hoc Networks IETF Chapter*. http : // www.ietf.org / html.charters / manet charter.html

[16]. C.E.Perkins. *AD HOC NETWORKING*. Addison Wesley, 2001

[17]. C.W. Wu, Y.C. Tay, C.K.Toh, Ad hoc multicast routing protocol utilizing increasing id-numbers (amris) functional specification, *Internet draft, work in progress, draft-ietf-manet-amris-spec-00.txt*, November 1998.