Analysis of Router Poisoning using network attacks

Chodhary Ravi Singh[1]

[1]*Assistant Professor, Deptt. of Computer Sc. & Engineering, Rakshpal Bahadur College of Engineering & Technology, Bareilly, India*

---***---

Abstract:- Security is an essential requirement in ad hoc network. Compared to wired networks, wireless ad hoc network are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Attacks on ad hoc networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. In this paper, we are describing all the prominent attacks and also various attacks on the routing protocol in literature in a consistent manner to provide a concise comparison on attack types to the best of our knowledge,.

Keywords— Ad-Hoc network, Security thread, Routing protocol attack, Internal and external attack, Active and passive attack, ARP

INTRODUCTION

The increase of cheaper, smaller and more powerful mobile devices have made wireless Ad Hoc networks to become one of the fastest growing areas of research. This new type of self-deploying network may combine wireless communication with high degree node mobility. Unlike conventional wired networks they have no fixed infrastructure. This flexibility makes them attractive for many applications for a situation where either supporting structure is unavailable or deployment is unfeasible such as military networks and disaster recovery operations. The ad hoc self organization also makes them suitable for virtual conferences, where setting up a traditional network infrastructure is a time consuming high-cost task. Security is an indispensable need for both wired and wireless network communications. Unlike wired networks, wireless networks pose a number of challenges to security solutions due to their unpredictable topology; wireless shared medium, heterogeneous resources and stringent resource constraints etc. There are a wide variety of attacks that target the weakness of this kind of network. In this type of network, security is not a single layer issue but a multilayered one. We have focused on network layer where the possible attacks are most vulnerable. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:

Confidentiality: Protection of any information from being exposed to unintended entities. In ad hoc networks this is more difficult to achieve because intermediate nodes receive the packets for other recipients, so they can easily eavesdrop the information being routed.

Availability: Services should be available whenever required.

There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services.

Authentication: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes. **Integrity:** Message being transmitted is never altered. The content of the message should always remain whole and unhampered.

Non-repudiation: Ensures that sending and receiving parties can never deny ever sending or receiving the message. There must be constant communication between the sender and the receiver.

TYPES OF SECURITY ATTACKS

External vs. Internal attacks

External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate in the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors. The security attacks in wireless Ad-Hoc can be roughly classified into two major categories, namely passive attacks and active attacks are as described in the figure 1. The active attacks further divided according to the layers.

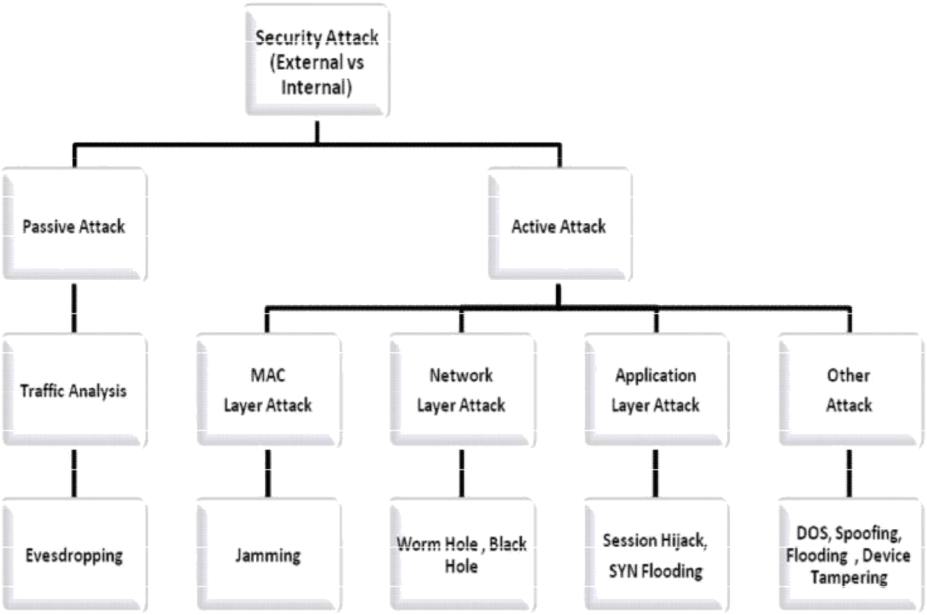

Fig 1: Different Types of Attacks

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, thereby making it impossible for the attacker to get useful information from the data overhead.

Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network thereby 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.

OVERVIEW OF SECURITY THREATS OF AD-HOC NETWORK

Black hole: In a black hole attack a malicious node advertises itself as having a valid route to the destination node even though the route is spurious. With this intension the attacker consumes or intercepts the packet without forwarding it. The attacker can completely suppress or modify the packet and generate fake information, which may cause network traffic diversion or packet drop.

Gray hole: In Gray hole attack there is a node in the established routing topology that selectively drops packet with certain probability causing network distraction. Gray hole 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 may behave maliciously for some time period by dropping all packets but may switch to normal behavior later. A gray hole may also exhibit a behavior which is a combination of the above two.

Worm hole: A worm hole attack is where two or more malicious nodes may collaborate to encapsulate and exchange messages between them along existing data routes. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. A worm hole shows a valid route to the destination but it always tunnels the packet to its malicious partner node. This attack is also known as tunneling attack.

Jellyfish attack: In jellyfish attack the malicious node first intrudes into the forwarding group in the network and then it unreasonably delays data packets for some amount of time before forwarding them. This result in significantly high end to- end delay and delay jitter, and thus degrades the performance of real-time applications.

Spoofing: The spoofing attack occurs when a malicious node pretends other node's identity at times. This in turn misguides a non malicious node in order to alter the vision of the network topology that it can gather.

Sybil attack: In Sybil attack, attacker pretends to have manifold identities or nodes. A malicious node can act as if it were a multiple number of nodes either by impersonating other nodes or simply by claiming false identities. This allows him to forge the result of a voting used for threshold security methods for more information.

Eaves dropping: It is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from unauthorized access.
Byzantine attack*:* In Byzantine attack there is a compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

Jamming attack: It is MAC LAYER ATTACKS Jamming is the particular class of DoS attacks. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets. **State Pollution attack:** In state Pollution attack there is a malicious node which gives incorrect parameters in reply, it is called the state pollution attack. For example, in best effort allocation, a malicious allocator can always give the new node an occupied address, which leads to repeated broadcast of Duplication Address Detection messages throughout the wireless Ad-Hoc network and the rejection of new node.

Routing Attacks: There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. Various attacks on the routing protocol are described briefly below:

1) **Routing Table Overflow:** In this attack, the attacker attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. Proactive routing algorithms attempt to discover routing information even before it is needed, while a reactive algorithm creates a route only once it is needed. An attacker can simply send excessive route advertisements to the routers in a network. Reactive protocols, on the other hand, do not collect routing data in advance.

2) **Routing Table Poisoning:** Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes. Routing table poisoning may result in suboptimal routing, congestion in portions of the network, or even make some parts of the network inaccessible.

3) **Packet Replication:** In this attack, an adversary node replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

4) **Route Cache Poisoning:** In the case of on-demand routing protocols (such as the AODV protocol), each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past. Similar to routing table poisoning, an adversary can also poison the route cache to achieve similar objectives.

5) **Rushing Attack:** On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. An adversary node which receives a Route Request packet from the source node floods the packet quickly throughout the network before other nodes which also receive the same Route Request packet can react. Nodes that receive the legitimate Route Request packets assume those packets to be duplicates of the packet already received through the adversary node and hence discard those packets. Any route discovered by the source node would contain the adversary node as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the adversary node. It is extremely difficult to detect such attacks in ad hoc wireless networks.

Systems that are located behind the access point. In unsafe deployments, wireless attackers can compromise traffic between machines on the wired network behind the wireless network, and also compromise traffic between other wireless machines including roaming clients in other cells. Of particular note is the vulnerability of home combination devices that offer a wireless access point, a switch, and a DSL/cable modem router in one package. These popular consumer devices allow a wireless attacker to compromise traffic between computers connected to the built-in switch. Additional vulnerable network architectures are explored below.

ARP cache poisoning is not a new problem; it has been extensively explored and defended against in the context of wired networks. Unfortunately, the design of wireless access points and the corresponding network architecture implications of their use are particularly vulnerable to this class of problems. The path to managing the security risks discovered by Digital and discussed herein involves rethinking network architectures, redesigning or upgrading access point hardware and firmware, deploying VPN solutions on the wireless network, and making wireless access points an integral part of the VPN infrastructure. Any and all applications designed for use over wireless networks must take these risks into account (preferably when they are being designed).

MITIGATION STRATEGIES

After acknowledging the new risks introduced by wireless deployments, the next step is to determine the best ways to mitigate them. Technical mitigation strategies fall into two broad classes: methods of prevention and means of detection. Any mitigation activities must be carried out as the result of a mature risk management approach. That is, any technical decisions should be made in light of business context and threat model.

TRANSPORT LAYER ATTACKS PREVENTION

Session hijacking attack: In Session hijacking, it takes advantage of the fact that most communications are protected (by providing credentials) at session setup, but not thereafter. In the TCP session hijacking attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. Thus the attacker impersonates the victim node and continues the session with the target.

SYN flooding attack: In SYN flooding attack is a denial of service attack. The attacker creates a large number of half opened TCP connections with a victim node, but never completes the handshake to fully open the connection.

ARP POISONING

Address resolution protocol (ARP) cache poisoning is a MAC layer attack that can only be carried out when an attacker is connected to the same local network as the target machines, limiting its effectiveness only to networks connected with switches, hubs, and bridges; not routers. Most 802.11b access points act as transparent MAC layer bridges, which allow ARP packets to pass back and forth between the wired and wireless networks. This implementation choice for access points allows ARP cache poisoning attacks to be executed against

Commercial Installations: There are several levels of increasing protection that can be applied to strengthen the security of these systems.

The first step is separate the wireless network from the organizational wired network. Placing a firewall between the switch connecting the access points and the rest of the wired network will prevent the attacks from spreading beyond the firewall. This technique does nothing to prevent ARP poisoning attacks directed against other wireless clients or the connection between wireless clients and the firewall itself. Firewalling at the access point has the added benefit of providing a way to filter out other attacks or unauthorized access attempts that may originate on the wireless network.

Deploying a Virtual Private Network (VPN) to provide authentication and client-to-gateway security of transmitted data will also provide a partial solution. On a VPN protected network an attacker can still redirect and passively monitor the traffic via the attacks we described, but this will only gain the attacker access to an encrypted data stream. Attackers will still have the ability to cause a denial of service by feeding bogus data into the caches of clients, but the compromise of data will no longer be an issue if the VPN is implemented correctly. (This also addresses the weakness in using the WEP protocol, which makes it a particularly attractive option.)

Note that completely securing a wireless network using a VPN solution involves more than simply setting up an external VPN server on the wired backbone network. While such a set up will protect wired traffic and wireless-to-wired connections, traffic between two wireless hosts will remain outside the scope of the VPN. To address this problem, several vendors have recently announced IPsec aware access points that will block all traffic from or to a host unless a secured connection with this host has been established. Other VPN aware access points are expected to become available as the inadequacy of current techniques becomes more widely recognized. Such products will have the added benefit of reducing the attacks outlined here from a wide-ranging compromise of network traffic to the minor annoyance of small-scale denial of service. Other, less optimal solutions include: isolating each access point with it's own firewall, which limits poisoning to clients within one wireless cell; and having vendors implement a roaming protocol based on routing instead of bridging, thus removing the need for access points to behave as bridges.

Finally we note again that any and all applications designed for use over a wireless network must take into account the specific risk profile. Porting wired applications to wireless installations without revisiting the risks will lead to security problems.

Home Installations: Home users should make an effort to separate wireless traffic from wired traffic. The combined home gateway devices currently do not offer any protection against these attacks. If combination devices are used, precautions should be taken on all individual machines. The use of static ARP entries on each host (through the 'arp' command) will prevent ARP traffic from being generated, and prevent the overwriting of static entries with spurious ARP replies from the network. (Be careful, and make sure things really work this way with any particular OS. Some versions of Windows and other platforms are known to have flaws, allowing dynamic ARP replies to overwrite static entries.)

One way to fix combined home gateway devices is to redesign them to route between the AP, switch, and ISP connection separately, instead of routing only between the combined AP/switch, and the ISP connection. This may require a new product cycle to get better gateways on the market, but it is likely that some home gateway devices will be able to fix this problem through a firmware upgrade.

A third option, for technically savvy home users, is to build a 'three-legged' firewall to separate the three sources of traffic; one port on the firewall for a standalone access point, one for local wired traffic, and one for the upstream connection to an ISP. This provides the most flexibility, but require significant knowledge to set up. This solution also allows security conscious users to add IPsec support to the firewall, and provide adequate encryption to their wireless traffic.

Detection of ARP poisoning attacks is needed for situations where prevention isn't possible, or as an assurance that the prevention methods are working. There are several methods for detecting ARP poisoning attacks in progress.

The arpwatch tool (http://www-nrg.ee.lbl.gov/) provides email notification to administrators when IP to MAC bindings change on a local area network. Most ARP attack tools trigger a flurry of emails when they are used, alerting administrators to the problem. Unfortunately, DHCP address assignments also trigger alerts, limiting the applicability of this tool in DHCP enabled networks because of the large number of false positives.

On machines that are the target of ARP poisoning attacks, detection is often possible by examining the contents of the ARP cache. If multiple entries map to the same MAC address, this is a strong indication that an attack of this sort may be in progress or may have recently occurred. Similarly, broadcast of reverse address resolution protocol (RARP) messages for the MAC of each machine expected to be on the network will provoke multiple answers for machines that are being actively attacked. This approach involves significant system administration overhead that may be unacceptable, since a list of all MAC addresses in use must be maintained.

Finally, intrusion detection systems may be able to detect the excessive number of unsolicited ARP replies that are caused by the common tools running in their default configuration. Many of the tools are usable in a stealthy manner, but the average 'script kiddie' doesn't have a deep enough understanding of normal ARP traffic to correctly hide the attack.

CONCLUSION

In this survey paper, Authors try to inspect the security threats in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Due to nature of mobility and open media wireless Ad-hoc network are much more prone to all kind of security risks as covered. Here the Authors have described the various types of attacks prevalent in router poisoning and a short introduction about routing protocol poisoning. The Authors have also mentioned a few measures to mitigate these problems. The Authors will continue further research on these issues.

ACKNOWLEDGMENT

The authors would like to acknowledge and thank their parents and all the other guides and mentors with great heart for their support and encouragement as well.

REFERENCES

[1] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication,” International Journal of Computer Science and Security (IJCSS) Volume: 4 Issue: 3.

[2] Sukla Banerjee , “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks”, Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[3] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ,”Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.

[4] Nishu Garg and R.P.Mahapatra, “MANET Security Issues ,” IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[5] N.Shanthi, Dr.Lganesan and Dr.K.Ramar , “Study of Different Attacks on Multicast Mobile Ad hoc Network,” Journal of Theoretical and Applied Information Technology.

[6] V. Madhu Viswanatham and A.A. Chari, “An Approach for Detecting Attacks in Mobile Adhoc Networks ,” Journal of Computer Science 4 (3): 245-251, 2008 ISSN 1549-3636 © 2008 Science Publications.

[7] Hoang Lan and Uyen Trang Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad hoc Networks”, Proceedings of ICNICONSMCL’06, 0-7695-2552-0/06@ 2006 IEEE.

[8] S. Murphy, “Routing Protocol Threat Analysis,” Internet Draft, draft-murphy-threat-00.txt, Octomber 2002.

[10] Hikmat Farhat, Zouk Mosbeh, A Scalable Method to Protect From IP Spoofing, 978-1-4244-2624- 9/08/$25.00 ©2008 IEEE.

[11] C.Jin, H.Wang, and K. G. Shin, Hop- count filtering: An effective defense against spoofed DDoS traffic, In Proc .of the 10th ACM conference on Computer and communications security, 2003.

[12] K. Park and H.Lee, On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets, In Proc. of ACM SIGCOMM, 2006.

[13]Z.Duan, X.Yuan, and J. Chandrashekar, Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates, IEEE Transactions On Dependable And Secure Computing, Vol. 5, No. 1, January-March 2008.

[14] A.Bremler-Barr and H.Levy, Spoofing Prevention Method, In Proc. of INFOCOM, 2005.

[15] S.Savage, D.Wetherall, Anna Karlin, and Tom Anderson, Network support for IP Traceback. IEEE/ACM Transactions on Networking, Vol. 9, No. 3, June 2001.

[16] Pierluigi Rolando, Riccardo Sisto, SPAF: Stateless FSA-Based Packet Filters, IEEE/ACM Transactions on Networking, Vol. 19, No. 1, February 2011.

[17] A. Perrig, D.Song, and A.Yaar, StackPi: A New Defense Mechanism against IP Spoo_ng and DDoS Attacks, Technical Report CMU-CS-02-208, CMU Technical Report, February 2003.

[18] Stefan sevage, Anna karlin and Tom Anderson, Network Support for IP traceback, IEEE/ACM Transactions on Networking, VOL 9., NO. 3 , June 2001.

[19] Jieren Cheng, Jianping Yin, Zhiping Cai and Chengkun Wu, Dos Attack Detection using IP address Feature Interaction, 2009 International Conference on Intelligent Networking and Collaborative Systems.

BIOGRAPHY

Mr. Ravi Singh is working as Assistant Professor in Rakshpal Bahadur College of Engineering , Bareilly. He is Graduate engineer from Uttar Pradesh Technical University Lucknow. He is having research publication in different domains and his major area of Research is Data Science, Network Security and Cloud Computing.