Volume 2, Issue 4, April 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Study of wireless Ad-Hoc Network attack and Routing Protocol attack

Mahendra Kumar*
Dept of C.S.E.
G.C.E.T Greater Noida
mahe.gupta.it@gmail.com

Ajay Bhushan
Dept of I.T.
G.C.E.T Greater Noida

Amit Kumar
Dept of I.T
G.C.E.T Greater Noida

Abstract— Security is an essential requirement in wireless 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 the all prominent attacks and alsoVarious attacks on the routing protocol are described 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.

I. INTRODUCTION

The increase of cheaper, smaller and more powerful mobile devices have made wireless Ad Hoc networks [4, 5] 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 [18, 20]. The adhoc self-organisation 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 [15] 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 [12] 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 intermediates 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.

Non-repudiation: Ensures that sending and receiving parties can never deny ever sending or receiving the message.

Type 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 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 behaviours. 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.

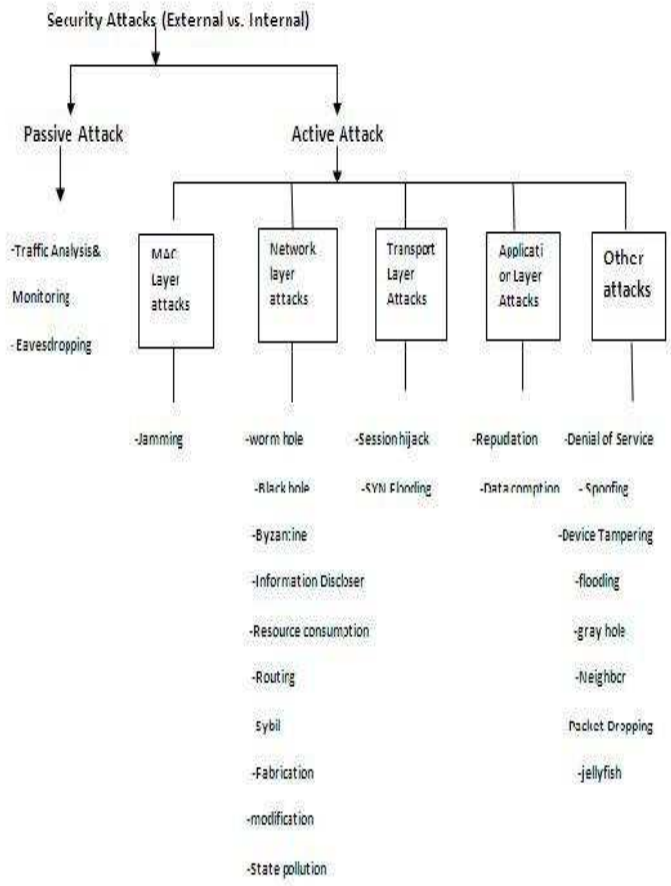

Fig 1: Different Types of Attacks

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, there by 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 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.

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 behaviour later. A gray hole may also exhibit a behaviour 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 tunnelling 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.

Eavesdropping: 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 the 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 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 [11]), 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.

TRANSPORT LAYER ATTACKS

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.

CONCLUSIONS

In this survey paper, Authors try to inspect the security threats in the mobile adhoc 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. As a result, the security needs in the wireless Ad-hoc network are much higher than those in the traditional wired networks.

During the survey, Authors also find some points that can e further explored in the future, such as to find some effective security solutions and protect the wireless Ad-hoc network from all kinds of security risks. Authors will try to explore deeper in this research area

ACKNOWLEDGMENT

The authors would like to acknowledge and thank their parents, god and all the human being with greate 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, October 2002.

[9] P. Papadimitratos and Z.J.Haas, "Securing the Routing Infrastructure", IEEE Communications, vol. 10, no. 40. October 2002, pp. 60-68.

10] C. Perkins Ad hoc On-Demand Distance Vector (AODV) Routing RFC3561[S] 2003-7.

[11] Zhu Daofei, Wang Dongyan, Liu xinran. Secure Routing Protocols for ad hoc Networks: a Survey[J]. Computer Engineering and Applications, 2005,(27):116-119.

[12] DENG Hongmei, L I Wei, AGRAWAL D P. Routing Security inWirelessAd Hoc Networks, IEEE Communication Magazine [J]. 2002, 40 (10): 70-75.

[13] Manel Guerrero Zapata. Secure Ad hoc On-Demand Distance Vetor Routing. drafr-guerrero-manet-saodv-02.txt, 2004-11.

[14] [1] antirez. New tcp scan method. BugTraq, http://www.securityfocus.com/archive/1/11581, February 2001.

[15] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer. A Secure Routing Portocol for Ad HocNetworks[C]. In: Proc of the 10th IEEE intel conf Network Portocols, IEEE press, 2002:78-87.

[16] DU Xinjun , GE Jianhua , WANG Ying. A method for security enhancements in AODV protocol[J]. Journal of Xidian University. 2002, 29(6): 819-821.

[17] WANG Jianxin, ZHANG Yanan ,WANG Weiping, LU Xicheng. A Security Routing Protocol Based on Reputation Systems in MANET[J]. Acta Electronica Sinica. 2005, 33(4): 596-601.

[18] WANG Zhen-zhong, GUAN Yuan, LU Jian-de, CHEN Yu-chun. Routing Security Mechanism Based on Neighbor Nodes Monitoring and Detecting for MANET[J]. Computer Engineering. 2007, 33(18): 148-150.

[19] HU Haiyan,WUMeng. Security Enhancement of AODV and GloMoSim Simulation[J]. Journal of Nanjing University of Posts and Telecommunications. 2005, 25(3):59-63.

[20] HUANG Yufei, WANG Peikang, HUANG Shaobin. Route discovery algorithms based on trust in mobile Ad hoc network[J]. Computer Aided Engineering. 2005, 14(2): 59-62.

