A Comparative Overview of Popular Attacks Relevant to Adhoc -Networks

Kiran Babu.T.S, Ragav Krishna.R

Abstract: The wireless ad hoc network become mundane, yet the core issue is the security. There are different types of attacks provided by different researcher but still faces research challenges. In Adhoc networks, nodes have limited resources like bandwidth, battery power and storage capacity. In this paper we pay attention to common attacks which occur in networks layer of OSI model such as Black hole attack ,gray hole attack, Flooding attack, Jamming ,Wormhole attack, Collosion attack traffic monitoring and analysis & DOS. We discuss about the counter measures against them.

Keywords: Attacks, Blackhole, DOS, Grayhole, Wormhole, Adhoc-Networks.

I. INTRODUCTION

. In a world of fast developing technologies and internet network, accessible for everyone, where there are no clear boundaries between the functionality of the "gadgets" and the possibility to com-municate is not an option but necessity, the ad hoc networks play a vital role. As a dynamic network, without any preset antecedent and strictly defined infrastructure (e.g. Wireless Access Points), Adhoc networks makes possible the connection between different types of mediums with-out any additional infrastructure ranging from mobile phones to laptops to personal digital assistants (PDAs), tablets, iPads etc. Adhoc networks is a self-configuring and self-organizing network. For these reasons several attack are bound to occur at network layer of OSI Model certain level of security cannot be established within the periphery of the network. In this paperwork we will heed attention to the different type soft attack that occur in adhoc network. For the better under-standing of the infrastructure of Adhoc networks we will make also have a comparison to the standard wireless networks. we will show the vulnerabilities of the network and the different types of attacks, which are common for Adhoc network and what can be done as countermeasures against them. the structure of this paperwork is build-up as it follows. Section 2 focuses on the theoretical fundamentals of the Adhoc infrastructure and presents some differences in comparison to the standard WLANs. It also casts light on the specific security network lay-ers, which can be implemented on this network.
As precedence, prior to introducing the common attacks within Ahoc networks, the different types of attacks will be classified in order to make clear, which attack against which level of MANet security can be used. Section 3 focuses on countermeasures, which can strengthen up the security level of the network.

Manuscript Received on December 2013.

Kiran Babu T.S., Asst. Professor, Computer Science & Engineering, CMR Institute of Technology (CMRIT) 132, AECS Layout, IT Park Road, Bangalore, India

Ragav Krishna.R, BE Scholar,Dept of Computer Sceience & Engineering, CMR Institute of Technology (CMRIT) 132, AECS Layout, IT Park Road Bangalore, India

Section 4 focuses on concluding with a summary on the Adhoc networks infrastructure and a critical view on the security level of the network, which have already been exhaustively dealt with in this paper work.

II. RELATED WORK

An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect in an impromptu manner. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes simply forward packets to and from each other. Ad Hoc networks can be set up simply and easily with no need for a pre-existing wireless network, or for additional network overhead hardware beyond the nodes in the network themselves. Ad Hoc networks offer economically viable low cost networking as well. The glitches (Disadvantages) of Ad Hoc networks include generally shorter working ranges than those of more highly-powered Infrastructure networks, causing a declivity in performance as and when there is a gradation in the number of devices in an Ad Hoc network and there is no bridge to these wired networks.Yet another disadvantage of conventional Ad Hoc networks is that they do not implement the strongest levels of security now available.
Infrastructure networks are collections of wireless devices attached to an intermediate piece of network infrastructure, quintessentially an access point, router, or Personal Computers currently running access point software. A WiFi ESL in Infrastructure mode entangles into a wireless part of a larger Local Area Network (LAN).

Advantages of Infrastructure networks include greater power and distance than most Ad Hoc networks, thus inherently greater scalability and stability, and better security. These bright spots (advantages) come at the cost of greater expense to set up the network, and of reduced agility.

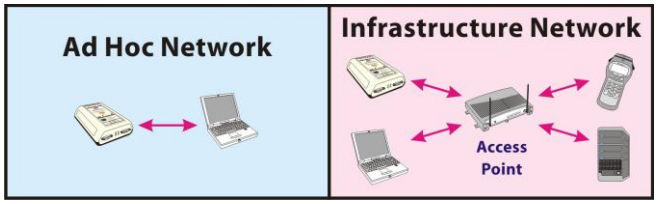

Figure1: Adhoc Networks infrastructure

In order to present some of the existing attacks in Adhoc networks in sectioon 3 we will make clear what are the different levels of security within the network and then classify them. In a standard network (Local Area Network or LAN) there are 7 OSI layers (Physical, Data link, Network, Transport, Session, Presentation, Application layer). As opposed to the LAN or WLAN, the security of Adhoc networks can be divided into 5 OSI layers:

Application layer, Transport layer, Network layer, Data link layer and Physical layer .

According to the specific layer there are various types of attacks which differ in their essence. For example typical attacks against the Physical layer are Jamming and Eavesdropping; against the Data link layer - traffic monitoring and analysis; against the Network layer - Blackhole attack, Wormhole attack, Flooding attack, Colluding misrelay attack; against the Transport layer - Session hijacking and SYN flooding. The following attacks can be executed against the Application layer - repudiation and data corruption, but since we have already reviewed that the attacks against the application layer are not typical for Adhoc Networks, because of the big variety of involved wireless mediums.

Table 2.1: Classification of Attacks

ADHOC NETWORKS LAYERS	ATTACKS
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Blackhole attack, Wormhole attack, Flooding attack,
	Colluding misrelay attack, Byzantine attack, Link Spoofing attack
Data link layer	Traffic monitoring and analysis,
	disruption MAC(802.11), WEP weakness

III. ATTACKS ON ADHOC NETWORK LAYER

In this section we will pay attention to the attacks, which are applied specifically and aim to work against MANet network layer: flooding attack, Blackhole attack, link spoofing attack and Wormhole at-tack. They will be presented as it follows:a) Flooding attack b) Blackhole attack c) Gray hole attack d) Wormhole attack

FLOODING ATTACKS

The flooding attack occuration was proposed in Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By continuously flooding a_server or a host with several connections that cannot be completely achieved, the flood attack gradually fills the hosts memory buffer. As soon as this buffer is full, no further connections are possible, and the result is a Denial of Service. Flooding packets in the whole network will consume a lot of network resources. To reduce congestion, the protocol has already adopted some methods which are briefly described as follows. Firstly, the number of RREQ that can be originated per second is limited. Secondly, after broadcasting a RREQ, the initiator will wait for a ROUTE REPLY.- If the route has not been received within round-trip milliseconds, the node may attempt to repeat the procedure again to discover a route by broadcasting another RREQ, until it arrives at the value for the maximum number of retry times at the maximum TTL value. The time intervals between each of these repeated attempts by a source node at route discovery for a single destination must satisfy a binary exponential backoff. The first time that a source node broadcasts a RREQ, and then waits the duration of the round-trip time for the reception of a ROUTE REPLY .

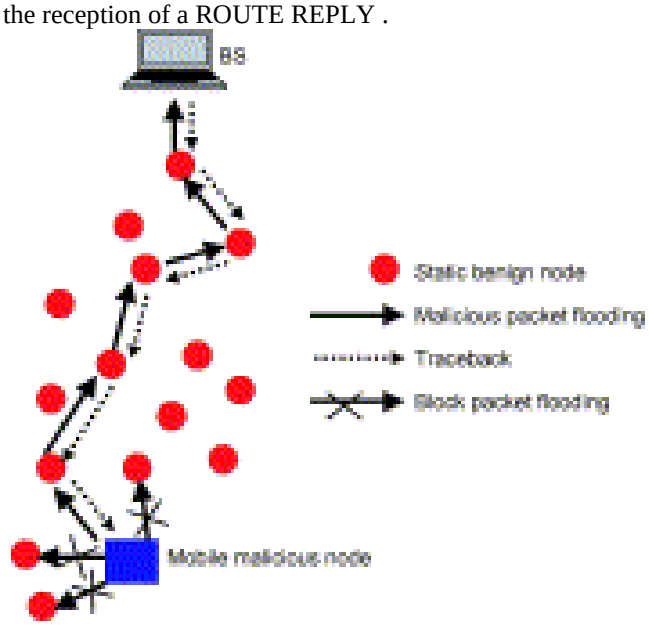

Figure 2: Flooding attack

EFFECT OF FLOODING ATTACK:
Degrade the performance in buffer
Degrade the performance in wireless interface
Degrade the performance in RREQ packets

Black Hole Attack

As the flooding attack, the Blackhole attack also concerns the AODV routing protocol in the net-work layer of Adhoc network. The completion of the attack proceeds in two steps: 1. an attacker or malicious node has to modify the network topology in order to create auspicious "environment" for the attack. It then presents its own self as a legitimate route within the network, aiming to intercept the data exchange between two authentic nodes. 2. Analog to interception attack in the Adhoc networks phys-ical layer, wherein the attacker obstructs the concrete radio signal, generating another stronger one, in the second step of Blackhole attack the malicious node consumes the intercepted data packages; it simply receives the information and does not forward it to the end user (destination node) [2].

The single black hole problem. Figure 3 is an example of single black hole attack in the mobile ad hoc networks . Node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node,which replies to the RREQ packet sent from the source node, and it creates a false response that it has the quickest route to the destination node. And due to this, node 1 erroneously judges the route discovery process with completion, after which it starts to send data packets to node 3. In the mobile ad hoc networks, a malicious node may drop or even consume some packets.

This suspicious node can be regarded as a black hole problem in Adhoc networks . As a result, node 3 might misroute the packets , and the network operation is suffered from this problem.

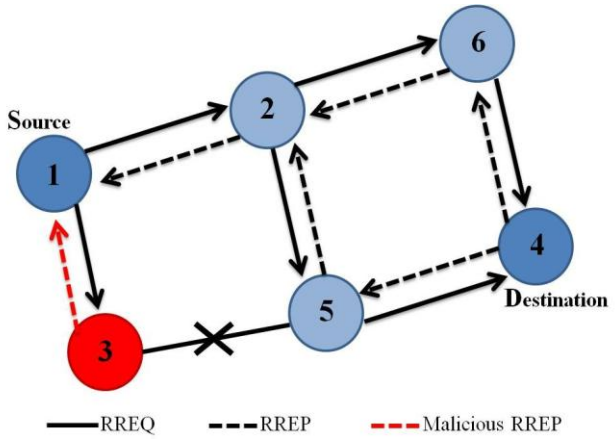

Figure 3: Black Hole Attack

Worm Hole Attack

The wormhole attack is a severe threat against packet routing in sensor networks that is particularly challenging to detect and prevent. In this particular attack, an adversary receives packets at one location in the network and tunnels them (possibly selectively) to another location in the network, and then the packets are resent into the network again. An instance of a wormhole attack would involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel (defined by the wormhole Start Point and the End Point) available only to the attacker. Hence a false route would then be established which would shorten the hop distance between any two non-malicious nodes.

Wormhole attacks can cause Denial-of-Service through Data Traffic, Denial-of-Service through Routing Disruptions and Unauthorized Access. In Denial-of-Service through Data Traffic, the malicious node(s) can insinuate itself in a route and then drop data packets. Denial-of-Service through Routing Disruptions can prevent discovery of legitimate routes and Unauthorized Access could allow access to wireless control system that are based on physical proximity, e.g. wireless car keys.

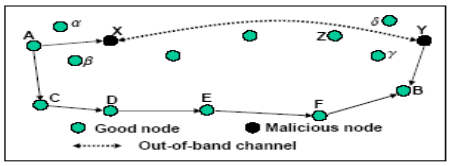

Figure 4: Worm hole Attack

The focus of this study is to determine the impact that wormholes can have on node localization for isotropic wireless sensor networks where only a limited fraction of nodes have self-positioning capability and the node positions have been determined using the "DV-hop" propagation method. At various places on the network grid, the wormhole is positioned, and its impact for varying hop lengths at each position is studied.

Gray hole Attack

The Gray Hole attack is a kind of Denial of Service (DoS) attacks. In this attack, an adversary initially exhibits behaviour

That is the same as an honest node during the route discovery process, and then quietly drops some or even all of the data packets sent to it, for the process of further forwarding even when no congestion occurs. The malicious nodes could degrade the network performance disturb route discovery process. Figure 5 describe the gray hole Attack.

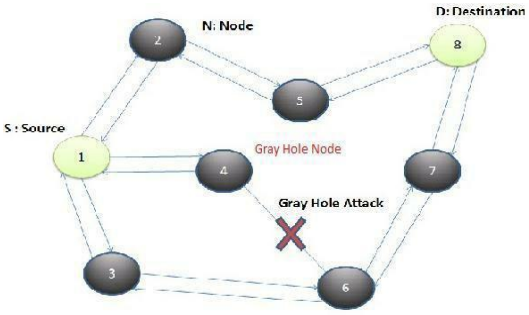

Figure 5: Gray Hole attack

IV CONCLUSION

This paper pays attention to the complex and fast changing infrastructure of the mobile ad hoc network as well as the common attacks, which occur within Adhoc networks. The theoretical fundamentals of its dynamic infrastructure and the different types of security layers are represented to give an overview on the system. It then offers an explanation as to which type of attack can be executed on which specific layer and also what countermeasures can be taken in order to prevent this specific attack.

REFERENCES

1. A. Tanenbaum, *Computer Networks*, PH PTR, 2003.
2. L. Zhou and Z. Haas, Securing Ad Hoc Networks, *IEEE Network Magazine* Vol.13 No.6 (1999) pp. 24-30.
3. S. Yi, P. Naldurg, and R. Kravets, Security Aware Ad hoc Routing for Wireless Networks. Report No.UIUCDCS-R-2002-2290, UIUC, 2002.
4. H. Luo and S. Lu, URSA: Ubiquitous and Robust Access Control for Mobile Ad-Hoc Networks, *IEEE/ACM Transactions on Networking* Vol.12 No.6 (2004) pp. 1049-1063.
5. M. Zapata, Secure Ad Hoc On-Demand Distance Vector (SAODV). Internet draft, draft-guerrero-manet-saodv-01.txt, 2002.
6. Y. Hu, A. Perrig, and D. Johnson, Packet Leashes: A Defense Against Wormhole Attacks inWireless Ad Hoc Networks. *Proc. of IEEE INFORCOM*, 2002