Port Change Attack in Wireless Ad Hoc Networks

VISHNU K
MNNIT B.Tech CSE Allahabad,
INDIA

MOHIT JAIN
Maharaja Surajmal Institute of
Technology
(Affiliated To Guru Gobind Singh
Indraprastha University,Delhi)
Department of Information
Technology
B.Tech Information Technology, New
Delhi, INDIA

SHALINI JAIN
Maharaja Surajmal Institute of
Technology
(Affiliated To Guru Gobind Singh
Indraprastha University,Delhi)
Department of Information
Technology, New Delhi, INDIA

Abstract
Mobile Ad hoc networks are mostly used in places where providing a network infrastructure seems difficult. In an Ad hoc network the nodes are free to move around and may join and leave the network at their wish. Due to this feature of freedom and unconstrained mobility it is prone to many security related issues. In this paper we present a new idea for a Transport layer attack.

Keywords
Component, Ad hoc Networks, Routing, Port Scan Attack, TCP/UDP

I. INTRODUCTION

A mobile ad hoc network (MANET) is a network formed by nodes that does not have any pre existing infrastructure. The networks in such occasions are formed by self willing mobile nodes that are free to move around, join and leave the network independently. They mutually co operate with each other by forwarding one anothers packets. Due to its intrinsic nature of lacking any centralized access control and limited resources mobile ad-hoc networks are often vulnerable to several different types of security attacks.

Firstly a Port scan attack refers to scanning all the open port number of the victim node, in order to find out all the services one can break into. In a port scan attack, the attacker basically sends a message to each of the 65,535 ports or in some case just a few common ports, whichever is feasible. Now depending on the reply the attacker gets back from each of the ports, one can decide on which of the ports are open.

However there exists one problem with such a port scan. It is that, some of the services in the destination node may create a log scan and if the service identifies that a connection has been made but no data received in return, the log reports an error. But again in order to counter this many stealth scan techniques [7] have been developed.

In this attack that we propose an adversary first exhibits the same behavior as an honest node during the route discovery process. It then launches a port scan attack on the Destination node, whose packets are to be intercepted. Once the Port Scan attack is successful the adversery places itself in the routing path of the destination and launches our proposed attack.

The rest of the paper is organized as follows. Section II discusses some related work. Section III describes the Network model. Section IV describes the details of the proposed mechanism of the attack. Section V concludes the paper while highlighting some future scope of work.

II. RELATED WORK

Juan et al [4] proposed the black hole injection attack in AODV according to which the malicious node replies positively for every RREP and hence gets into the route. It then silently drops all the data packets to be forwarded.

In case of a gray hole attack et al [9], it is a variation of the black hole, in which the nodes are initially not malicious but turn malicious later on. Also in such an attack the gray node may selectively drop data packets which make it further difficult to detect it.

Marco et al [7] discusses a review of port scanning techniques. He discusses some of the stealth and indirect scanning techniques. Further he also briefs up on Fragmented decoy and Co ordinated scanning techniques. A brief overview of UDP scanning has also been presented.

The SYN flooding attacks et al [13] makes use of the fact that in case of TCP every connection is initialized with a SYN packet from the client side. In response to that the server sends back a SYN/ACK packet and then waits for the ACK packet back from the client. Since the server can maintain only a few connections at a time, it has a limited backlog queue, in which it stores all its half open connection. An attacker makes use of this fact and sends a large number of SYN packets to the victim with a spoofed IP address. Hence there is no chance of an ACK packet in return to the server. This consumes all the resources of the

Manuscript received August 5, 2010
Manuscript revised August 20, 2010

server and puts it to an idle state for a particular amount of time. If repeated periodically the victim can be made numb.

Ping et al [14]proposed the “Ad Hoc Flooding Attack” (AHFA) in which instead of flooding with the SYN packets, one floods the network with a mass number of Route Request (RREQ) packets. In this case the entire network is affected in terms of bandwidth consumption.

Of course many authors have proposed solutions to each of the above mentioned attacks.

III. Network Model

We assume that the nodes in the network are randomly distributed throughout and that they use the TCP/IP protocol. We also assume that the network uses bidirectional link.

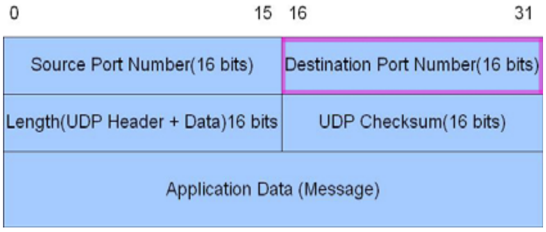
IV. Methodology

TCP/UDP needs two identifiers, the IP address and the port number at each end to make a connection. This combination of an IP address and a port number called a socket address defines the application level process uniquely.

Whenever an application layer process starts in a node that requires networking capabilities it requests for a port number from the operating system And all the data packets from/to the network for this particular application are tunneled through this port. Hence some implementations create both an incoming and an outgoing queue with each process. Other implementations create only an incoming queue associated with each process. The queues remain open as long as the process is running.

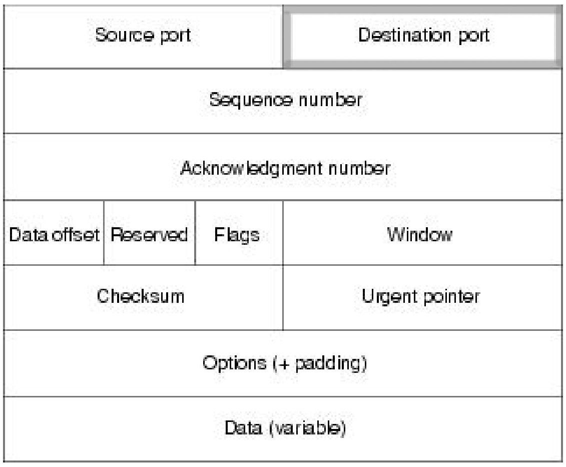
A. *Source port number:* This is the port number from which the application layer process in the source node is sending its data packets. In case of ephemeral processes this port number also denotes the port number at which the destination node replies. It is 16 bit long, which means it can range from 0 to 65,535.

B. *Destination port number*: This is the port number that is kept open by the destination node’s application proces in order to receive the incoming data packets. Hence this is the port number specified in the source node’s data packet’s destination port number field. It is also 16 bit long.



0 15	16 31
Source Port Number(16 bits)	Destination Port Number(16 bits)
Length(UDP Header + Data)16 bits	UDP Checksum(16 bits)
Application Data (Message)	

Fig 1. TCP packet header format



Source port			Destination port
Sequence number			
Acknowledgment number			
Data offset	Reserved	Flags	Window
Checksum			Urgent pointer
Options (+ padding)			
Data (variable)			

Fig 2. UDP P packet format

The attack approach proposed in this paper structures in four successive steps (see Figure 3):

1. The malicious node (M) first launches a port scan attack[1][7] on the destination node and finds out all the open ports.
2. Then it induces itself into the routing path between the source node and the destination by emitting protocol-compliant messages for leading both Source and Destination nodes to choose such a link for their communications[4][9] (see Figure 4).
3. The malicious node (M) now starts altering the data packet's that are routed through it such that the Destination port number is changed to any other port that is open at the Destination node. The open ports at the Destination has already been found out by a Port Scan Attack (see Figure 5).
4. The node (M) will also have to change back the port number of the acknowledgement packets to the original port number, if they are routed through the same link (hence the assumption bidirectional link).

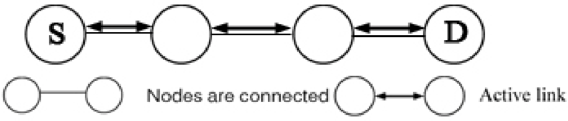


Fig 3. Before Attack Scenario.

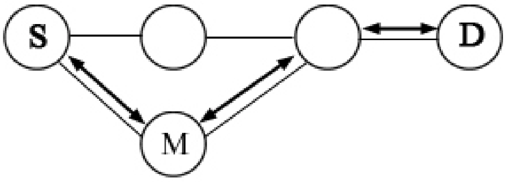


Fig 4. M gets control over A-D communication link

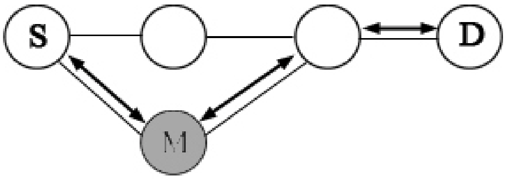


Fig 5. M turns malicious by launching port scan attack & altering port numbers of data packets

Here it is necessary to 1st launch a port scan attack on the Destination node because if the attacker alters the original port number to a port number that is closed at the Destination, the Destination node's TCP/UDP discards the user datagram and sends an “ICMP Port Unreachable” message, which may lead to suspicion.

Since the TCP acknowledgements are also received safe and sound back at the Source node the TCP protocol wouldn't suspect a data loss. The data flow abnormality can be observed only at the application layer and that too only if it is designed to do so. This is because the application process fully relies on the TCP for an error free, complete transmission of data and in this case TCP fails. Eventually the destination node's application process starves without data, while all of its data packets are being processed by another process of the same node. The other process may also get corrupted due to the absurd flow of data.

Also none of the Malicious Node detection schemes would be able to detect any packet loss/drop as no explicit packet dropping occurs anywhere in the network.

V. Conclusion And Future Work

In this paper we have proposed an alternate methodology to empower other network layered attacks. As future work we hope to -

- Develop simulations to analyze the performance of the above variation.
- Develop an efficient solution to the above proposed attack.

References

[1] "Detection and Characterization of Port Scan Attacks", Cynthia Bailey Lee, Chris Roedel, Elena Silenok, Department of Computer Science & Engineering University of California, San Diegohttp://cseweb.ucsd.edu/users/clbailey/PortScans.pdf

[2] ”Routing Security in Wireless Ad Hoc Network”, Hongmei Deng, Wei Li, and Dharma P. AgrawalIEEE Communications Magzine, vol. 40, pp. 70-75, 2002.

[3] “Security Issues in Mobile Ad Hoc Networks- A Survey” Wenjia Li and Anupam Joshi, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County.

[4] “Black Hole Attack Injection in Ad hoc Networks” Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Instituto de las TIC Avanzadas (ITACA) Universidad Politécnica de Valencia, Campus de Vera s/n, E-46022, Valencia, Spain

[5] “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, S.Marti, T.J. Giuli, K. Lai, and M. Baker. In Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM 2000), August 2000.

[6] “SCAN: Self-organized network-layer security in mobile ad hoc networks”, H.Yang, J. Shu, X. Meng, and S. Lu, IEEE Journal on Selected Areas in Communications, vol. 24, issue 2, pp. 261-273, February 2006.

[7] "A Review of Port Scanning Techniques", Marco de Vivo, Eddy Carrasco, Germinal Isern, Gabriela O. de Vivo ACM SIGCOMM Computer Communication Review Volume 29 , Issue 2 (April 1999) Pages: 41 – 48.

[8] “Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks”, Oscar F. Gonzalez, Michael Howarth, and George Pavlou,. Center for Communications Systems Research, University of Surrey, Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.

[9] ”Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks“, Piyush Agrawal, R. K. Ghosh, Sajal K. Das, In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.

[10] ”Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, S.Marti, T. J. Giuli, K. Lai, and M. Baker, Proceedings of the 6th annual intrnational conference on Mobile Computing and Networking (MOBICOM), Boston, Massachusetts, United States, 2000, 255-265.

[11] “Prevention of cooperative black hole attack in wireless ad hoc networks”, S.Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. In Proceedings of 2003 International Conference on Wireless Networks (ICWN’03), pages 570–575. Las Vegas, Nevada, USA, 2003.

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

[13] ”Detecting SYN Flooding Attacks”, Haining Wang, Danlu Zhang, and Kang G. Shin, IEEE INFOCOM'2002, New York City, 2002

[14] “A New Routing Attack in Mobile Ad Hoc Networks", International Journal of Information Technology Vol. 11 No. 2, Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong, Department of Computing and Information Technology.