An Exercise in Constructing Secure Mobile Ad hoc Network (SMANET)[1]

C. Edward Chow, Paul J. Fong, and Ganesh Godavari
Department of Computer Science
University of Colorado at Colorado Springs
{chow, pjfong, gkgodava}@cs.uccs.edu

Abstract

A secure MANET system, called SMANET, was developed that accepts only those packets whose MAC addresses are in the Linux iptable firewall rules. Detailed iptable set up and the performance of the firewall are presented. SMANET is integrated with a simple intrusion alert system based on TCPDUMP utility.

1. Introduction

Mobile Ad-hoc Networking (MANET) is receiving growing attention as a means of providing communications in environments where there is no existing infrastructure. First responders at a disaster site or soldiers in a battlefield must provide their own communications. A MANET is a possible solution for this need to quickly establish communications in a mobile and transient environment. It uses AODV routing protocol to dynamically establish the route [1,2].

A MANET has several security vulnerabilities. This paper presents the study of these vulnerabilities and investigates possible solutions. Closing these security vulnerabilities will influence the acceptability of a MANET for critical applications.

A MANET node has several physical vulnerabilities. It is lightweight in order to provide mobility and thus can be easily captured or tampered with. Its battery limits its power supply and computation capability. This leaves a MANET node prey to denial of service (DoS) attacks designed to diminish its power supply and overwhelm its computational capability.

1 This work is based on research sponsored by the Air Force Research Laboratory, under agreement number F49620-03-1-0207. The view and conclusions contained herein are those of the authors and should not be interpreted as necessarily represented the official policies or endorsements, either expressed or implied, of the Air Force Research Laboratories or the U.S. Government. It is sponsored by a NISSC Summer 2003 grant.

The MANET network itself is mobile and transient with frequent changes in topology. It lacks central control and depends upon cooperation between nodes. These characteristics invite "man in the middle" or usurpation attacks where a rogue impersonates a trusted node. A mobile attacker may seek out a MANET or lie in wait for it like a submarine in the path of a fleet.

By the very nature of the wireless medium, a transmission can be intercepted or jammed. Passive attacks can occur from an eavesdropper who can decipher and compromise the transmitted information.

Active attacks can take many forms. An impersonator or usurper may disrupt packet routing by sending misleading control information. The attacker can create a "Black Hole" by advertising that it has the shortest path to a given destination and intercepting the packets sent to it. The attacker may create routes that do not exist and overflow the routing tables. Service may be denied by unnecessarily forwarding packets or requesting services [3].

A wireless firewall has been created that allows only hosts with specified Media Access Control (MAC) addresses to join the mobile ad hoc network (MANET). A simple intrusion detection system has been created that reports intrusion attempts.

2. Wireless Firewall

2.1 Unsecured MANET

A MANET without a firewall or authentication provisions, provides an attacker with an opportunity to join the wireless network. We are using NIST implementation of AODV protocol for the MANET. At best, the attacker may passively listen to the network traffic and potentially compromise confidential information. At worst, the attacker may disrupt the network communication.

Figure 1 illustrates an attacker joining an unsecured MANET. By passively listening to the wireless packets exchanged, an attacker determines the network protocol information needed to associate with the unsecured MANET. The attacker then uses the information obtained to send messages to the nearest MANET node to complete the network association protocol.

Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04)
0-7695-2051-0/04 $ 20.00 © 2004 IEEE

2.2 Firewalled SMANET

To secure the MANET, the erection of a firewall is a prudent first step. The firewall is implemented with software in a MANET node that filters packets. The aim is to keep the attacker from joining the network by preventing the processing of packets received from the attacker. Figure 2 illustrates the operation of a firewall that prevents messages from the attacker from being processed by a SMANET node. The packet filtering operation of that firewall will be discussed in the next section.

3. Packet Filtering

3.1 Packet Chains

The MANET nodes in this project use the Linux operating system. When a packet is received by a Linux system, there are two paths it may take. It may be processed locally or forwarded to another node in the MANET.

The packet received from the network is placed in the PREROUTING chain. There, a routing decision is made to either process the packet locally or to forward it to another node in the network. If it is to be locally processed, the packet is placed on the INPUT chain. If it is to be forwarded, it is placed on the FORWARD chain.

While in the INPUT and FORWARD chains, a packet can be filtered. The criteria for accepting or dropping a packet in one of these two chains can be specified by the firewall software.

3.2 Linux "iptables" Facility [4]

The Linux operating system provides a packet filtering facility known as "iptables." This facility allows filtering rules to be defined. The rules allow packets to be dropped or accepted based on match criteria.

The general syntax of an iptables statement is defined below in Table 1. An iptables statement can drop or accept a packet from the INPUT or FORWARD chains based on the specified match criteria.

Table 1 iptables statement

iptables [-t *table*] command [match] [target/jump]

3.3 Node Firewall Filter

Table 2 shows the script executed by a MANET node to implement its firewall. The script is comprised of iptables statements that define the packet filtering criteria.

This firewall is designed to allow wireless communications between wireless nodes with specific media access control (MAC) addresses. Each wireless device conforming to the IEEE 802.11 standard has a unique MAC address. This firewall will drop all wireless packets that do not have one of the two requisite MAC addresses.

In this script, the first two iptables statements specify that all packets on the INPUT and FORWARD chains will be dropped unless they meet the acceptance criteria defined in the iptables statements that follow.

The next two iptables statements specify that all packets in the INPUT chain from the wireless port (eth0) with two specific MAC addresses will be accepted. The last two iptables statements specify the same criteria for packets on the FORWARD chain.

3.4 Gateway Firewall Filter

The gateway node requires a different filter because it has two interfaces: a wireless port and a gateway port to the external network or Internet. The filtering criteria for its wireless port are the same as that of the other MANET nodes. Only packets from a specific MAC addresses will be accepted. There are no filtering criteria for its gateway port so all Internet traffic is accepted through this port.

Table 3 above shows the script executed by the gateway node to implement its firewall. As in the filter of Table 2, the 1st two iptables statements define a default drop policy for the INPUT and FORWARD chains. The next two iptables statements specify that all packets from the gateway port (eth0) will be accepted. The next 4 iptables statements specify that only packets from two specific MAC addresses will be accepted from the wireless port.

4. Firewall Performance

4.1 Control Configuration without Firewall

In the control configuration without a firewall, the attacker was able to associate with the MANET and take advantage of its services. By joining the MANET, the attacker was able to use the gateway to connect to the Internet.

4.2 Firewall Configuration

By erecting firewalls on both the gateway and the SMANET node, IP communications with the attacker is terminated.

Conversely, the attacker can no longer reach any point in the SMANET or Internet.

4.3 Result Analysis

A firewall that filters packets based on MAC addresses can effectively deny an attacker the use of a MANET and its Internet gateway services.

5. Intrusion Detection System

It is desirable to detect intrusion attempts and issue alerts when such an attempt is made. A simple intrusion detection system based on the TCPDUMP utility, has been created.

The TCPDUMP utility provides a mechanism for the detection and warning of intrusion attempts [5]. TCPDUMP can receive and scan wireless frames contained Media Access Control (MAC) addresses. TCPDUMP statements can be written to compare the MAC address against a list of approved MAC addresses.

Frames containing MAC addresses that do not appear in a list of approved addresses will trigger an alert

When the TCPDUMP script is executed, the MAC addresses from frames received are compared to the list of approved MAC addresses. When the MAC addresses received are found to be in the list, no alerts are issued.

When a wireless host with a MAC address not on the list of approved MAC addresses begins to ping the host with the IDS, each frame is from the intruder is detected and a message is displayed.

6. Future work and Conclusion

Future work will comprise of completing the following tasks to further improve MANET security:

- Tighten firewall criteria to counter MAC address spoofing,
- Authenticating routing updates,
- Authenticating through PEAP and TTLS, and
- Responding with group rekeying measures designed to isolate the attacker.

We have demonstrated a simple secure MANET system can be easily created based on the Linux iptables and TCPDUMP utilities. Note that MAC address spoofing was not addressed in the above simple protection testbed. PEAP/TTLS draft protocols address the MAC spoofing issue. A modified freeRadius server with PEAP/TTLS modules was implemented in a separate related project.

7. References

[1] Ad-hoc On-demand Distance Vector Protocol. http://w3.antd.nist.gov/wctg/aodv_kernel/.

[2] Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das. "Ad Hoc On Demand Distance Vector (AODV) Routing." *IETF Internet draft*, draft-ietf-manet-aodv-11.txt, June 2002 (Work in Progress).

[3] Zapata, M.G. "Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing." http://www.ietf.org/internet-drafts/draft-guerrero-manet-saodv-00.txt , Internet Draft, October 2001.

[4] http://www.netfilter.org/

[5] http://www.tcpdump.org/

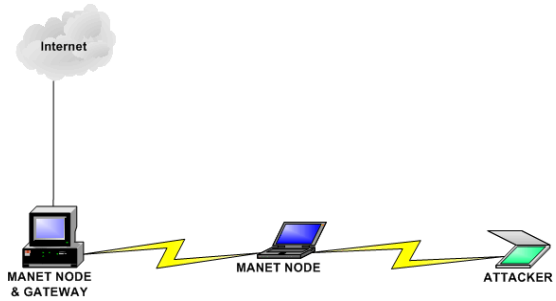

Figure 1 Unsecured MANET

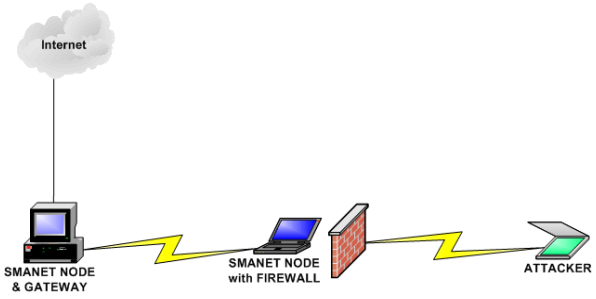

Figure 2 Firewalled SMANET

Table 2 Node Filter

```
#!/bin/sh

# NODE-FILTER
# eth0:  wireless port
# eth0 is sole communications port

# DROP all wireless packets from the INPUT and FORWARD chains
# except those with the following MAC addresses:
#    00:09:B7:7B:B2:58  Cisco 350 PCI
#    00:0A:B7:8B:5C:1D  Cisco 350 PCMCIA

# Set default policy on INPUT & FORWARD chains to DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP

# Apply INPUT chain filtering to wireless port eth0
iptables -A INPUT -i eth0 -p ALL  -m mac --mac-source 00:09:B7:7B:B2:58 -j ACCEPT
iptables -A INPUT -i eth0 -p ALL  -m mac --mac-source 00:0A:B7:8B:5C:1D -j ACCEPT

# Apply FORWARD chain filtering to wireless port eth0
iptables -A FORWARD -i eth0 -p ALL -m mac --mac-source 00:09:B7:7B:B2:58 -j ACCEPT
iptables -A FORWARD -i eth0 -p ALL -m mac --mac-source 00:0A:B7:8B:5C:1D -j ACCEPT
```

Table 3 Gateway Filter

```
#!/bin/sh

# GATEWAY-FILTER
# eth0:  gateway port
# eth1:  wireless port
#
# DROP all wireless packets from the INPUT and FORWARD chains
# except those with the following MAC addresses:
#     00:09:B7:7B:B2:58  Cisco 350 PCI
#     00:0A:B7:8B:5C:1D  Cisco 350 PCMCIA

# Set default policy on INPUT & FORWARD chains to DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP

# ACCEPT all packets on gateway port eth0
iptables -A INPUT -i eth0 -p ALL -j ACCEPT
iptables -A FORWARD -i eth0 -p ALL -j ACCEPT

# Apply INPUT chain filtering to wireless port eth1
iptables -A INPUT -i eth1 -p ALL -m mac --mac-source 00:09:B7:7B:B2:58 -j ACCEPT
iptables -A INPUT -i eth1 -p ALL -m mac --mac-source 00:0A:B7:8B:5C:1D -j ACCEPT

# Apply FORWARD chain filtering to wireless port eth1
iptables -A FORWARD -i eth1 -p ALL -m mac --mac-source 00:09:B7:7B:B2:58 -j ACCEPT
iptables -A FORWARD -i eth1 -p ALL -m mac --mac-source 00:0A:B7:8B:5C:1D -j ACCEPT
```