國立交通大學

資訊科學與工程研究所

碩士論文

無線區域網路中非法擷取點之偵測與定位

Detecting and Locating Rogue Access Points in WLANs

研 究 生：盧牧英

指導教授：簡榮宏　教授

中 華 民 國　九 十 五　年 六 月

無線區域網路中非法擷取點之偵測與定位

Detecting and Locating Rogue Access Points in WLANs

研究生：盧牧英　　Student：Mu-Ying Lu

指導教授：簡榮宏　　Advisor：Rong-Hong Jan

國立交通大學
資訊科學與工程研究所
碩士論文

A Thesis
Submitted to Institute of Computer Science and Engineering
College of Computer Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of
Master
in

Computer Science

June 2006

Hsinchu, Taiwan, Republic of China

中華民國九十五年六月

無線區域網路中非法擷取點之偵測與定位

研究生：盧牧英　　　　指導教授：簡榮宏 博士

國立交通大學資訊科學與工程研究所

摘　　要

由於近年來無線網路技術日益進步，架設無線網路環境越來越簡單且成本亦趨低廉，使得無線網路的普及率越來越高。由於架設擷取點相當容易，使得有心人士可以利用此私接之擷取點連上骨幹網路，擷取資料或進行攻擊行為。為了偵測出此類非法擷取點，我們提出了一個基於憑證及掃瞄信標的偵測方法，利用檢查擷取點的硬體位址與檢驗憑證的內容來判斷此擷取點是否合法。此外，合法擷取點會定期或隨機掃瞄周遭的頻道以收集來自其他擷取點的信標，並將掃瞄後的結果傳給網路管理者，網路管理者可以透過比對掃瞄結果中是否有未經過檢驗的硬體位址，來判斷環境中是否有非法擷取點的存在。偵測出非法擷取點後，我們利用訊號強弱判斷模組來計算出此非法擷取點的位址。本篇論文，也針對所提出的系統加以實做並評估其效能，以此展示方法的優越性。

Detecting and Locating Rogue Access Points in WLANs

Student：Mu-Ying Lu　　　　Advisor：Dr. Rong-Hong Jan

INSTITUTE OF COMPUTER SCIENCE AND ENGINEERING

NATIONAL CHIAO TUNG UNIVERSITY

Abstract

As the cost of 802.11 hardware continues decreasing, the case of installing unauthorized wireless access points (APs) into enterprise or school networks grows. These rogue APs expose the WLAN to a breach of security. Most of the current approaches of detecting rogue APs are easily evaded. In this thesis, we proposed the certificate-based and scan-based detection method to detect rogue APs at a central location (Access Router, AR). We determine an AP if rogue or legal by checking its MAC address and then verifying its certificate. Furthermore, the legal APs will scan channels and gather beacon frames from other APs at fixed or random interval, and then send the collected data to network manager. Network manager can discover a rogue AP with MAC address spoofing by comparing the scan results from the legal APs with the legal APs list in AR. After detecting, we utilize signal strength to calculate the location of the rogue AP by propagation model. The proposed methods in this thesis are implemented and the experimental results that are given to show the performance of our approach are superior.

Contents

1 Introduction **4**

2 Related Works **7**

2.1 Rogue Access Point Detection 7

2.1.1 Wired Detection Approaches 8

2.1.2 Wireless Detection Approaches 13

2.2 Rogue Access Point Location 17

2.2.1 Client-Based Location 17

2.2.2 Sniffer-Based Location 18

3 System Design **19**

3.1 Certificate-Based Detection 19

3.1.1 System Architecture 20

3.1.2 System Components 21

3.1.3 Main State Machine 22

3.1.4 Detection Procedure 24

3.1.5 Firewall 30

3.1.6 Summary of Certificate-Based Detection 31

3.2 Scan-Based Detection 32

3.2.1 Drawback of Certificate-Based Detection 32

3.2.2 Design of Scan-Based Detection 32

3.3 Sniffer-Based Location 35

4 Implementation and Performance Evaluation 37

4.1 Experimental Environment 37

4.2 Rogue AP management program of scan-based detection 39

4.3 System Performance Evaluation 41

5 Conclusions and Future Work 46

List of Figures

2.1 Scan result of Nmap. 9

2.2 Using AirSnare to monitor MAC addresses of devices in LAN. . . . 12

2.3 Using NetStumbler to discover APs in WLAN. 15

2.4 Using Kismet to discover APs in WLAN. 16

3.1 System Architecture. 20

3.2 State machine of AP. 22

3.3 Message flows between AP and AR. 25

3.4 Flowchart of certificate-based detection procedure. 26

3.5 AP7 can not be detected by AR. 33

3.6 The distance between rogue AP and AP1/AP2. 35

4.1 Experiment Environment. 38

4.2 Management program after querying the scan results. 40

4.3 Detection time of certificate-based detection and Nmap. 41

4.4 Detection time in different Challenge Interval. 42

4.5 The relation between periodically scan behavior and throughput. . 43

4.6 The relation between random scan behavior and throughput. . . . 44

Chapter 1

Introduction

For the past few years, increasing number of wireless local area networks (WLANs), based on the IEEE 802.11, have been deployed in various types of places, including schools, enterprises, airports, coffee shops, as well as many other locations. One of the primary advantages of WLAN is its ability to provide wireless connectivity to portable devices, such as laptops, personal digital assistants (PDAs).

As users realize the benefits of wireless networking, they begin to desire the same mobility and flexibility in the workplace. Rather than waiting for their network administrators in their company to install a WLAN, the employees install one by themselves. This kind of unauthorized access points (APs), not deployed by network administrator, we called rogue APs. These rogue APs expose the intranet to a breach of security because they are typically connected to a network port behind the corporate firewall. Furthermore, employees rarely enable any security settings on rogue APs or just use the default manufacturing security setting.

The most rogue APs are well-intentioned, installed by authorized users for convenient purpose. However, unauthorized users may connect to rogue APs and do some malicious actions. The most likely major impact is that an unauthorized intruder can associate with the rogue AP and gain the ability to access network resources. Otherwise, an unauthorized user can use the rogue AP and easily eavesdrop on enterprise network traffic.

In this thesis, we proposed a system that can detect and locate the rogue APs in the WLANs. There are two main parts of our proposed rogue APs detection system: certificate-based detection and scan-based detection. In certificate-based detection, the central server, access router (AR), takes charge of determining an AP is rogue or not. Rogue APs can be detected during the phase that AR verify legality of this AP by checking its MAC address and certificate. After verifying a legal AP, AR will challenge the AP periodically to avoid that a rogue AP cracks the legal AP and then masquerade to a legal one by using its MAC address.

But the certificate-based rogue APs detection has a drawback so that maybe some rogue APs can evade detecting by AR. So we conceive the scan-based detection to cooperate with certificate-based detection to make up its defect. The scan-based detection utilizes the legal APs that verified via AR to scan beacon frames broadcasted from other APs in all channel. According to the MAC addresses of beacon frames, we can determine if the AP is rogue or not by comparing its MAC address with the legal APs list in AR.

However, the general APs do not have scanning capability, i.e. APs are not required to receive beacon frames from other APs. In our experiment, we use the HostAP daemon and HostAP driver [1] to implement an AP. We modified the source code of HostAP driver to enable AP can receive beacon frames. The modified APs scan all channels to collect beacon frames from other APs and send the scan results to network manager to compare with the legal APs list in AR. Once a rogue AP is detected, we estimate the location of this rogue AP base on its signal strength received at the legal APs.

The remainder of the paper is organized as follows: In section 2, we discuss current approaches of detecting and locating method. In section 3, we describe our proposed detection and location method in detail. And evaluate the performance of our proposed system in section 4. In section 5, we give the conclusion and a discussion of future work.

Chapter 2

Related Works

In this chapter, we will introduce the current approaches for detecting and locating rogue access points (APs). We classify the detection methods according to their detecting techniques are operated on wired or wireless network. Based on this classification strategy, the detection approaches can be separated into wired-based and wireless-based detection. Once a rogue AP is detected, the network administrators have to remove the rogue AP as fast as possible. The detecting system in order to inform the network administrators about the location of the rogue AP, the system must have ability to calculate the location of the rogue AP. WLAN-based indoor positioning methods nowadays mostly depend on signal strength utilization. We classify the location method base on what kinds of device that measure signal strength. There are two main kinds of indoor positioning in WLAN: client-based location and sniffer-based location.

2.1 Rogue Access Point Detection

The current approaches for detecting rogue APs can be categorized into two main categories. The first category is using traditional wired LAN to discover the rogue APs. Such approaches include TCP/IP fingerprinting, SNMP scanning, packet sniffing, and observation of traffic characteristics. The second category of detection approaches is utilizing wireless radio link to find out rogue APs. This kind of detection such as active probing and RF monitoring.

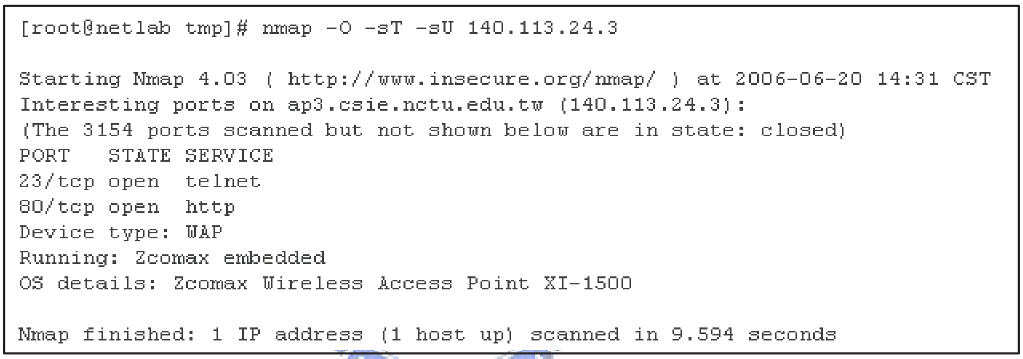
2.1.1 Wired Detection Approaches

There are certain of techniques and tools available for determining information about devices that are connected to the wired network. These tools and techniques are based on two primary approaches for collecting information: (1) Query-Response and (2) Traffic-Monitoring. We will introduce four kinds of wired detection approaches. In these four methods, TCP/IP fingerprinting and SNMP scanning belong to Query-Response approach to gather information of devices. Another two wired detection approaches, packet sniffing and observation of traffic characteristics, obtain information about network devices by Traffic-Monitoring.

A. TCP/IP Fingerprinting

Because of implementation of TCP/IP stack in every operating system (OS) is different, we can use TCP/IP fingerprinting to guess the OS running on the target machine. There are many techniques which can be used to fingerprint TCP/IP stacks. Basically, you just notice and record the differences in TCP/IP payload in each OS. If you gather enough information of these, you can guess the OS of target machine very accurately. The network administrators can use TCP/IP fingerprinting to discover rogue APs by scanning entire network and seek if any machine its OS is recognized as an 802.11 AP.

The most popular tool using TCP/IP fingerprinting is Nmap [2]. It can run under Windows and Unix-like system. When you execute Nmap with the parameter "-O", the program will use TCP/IP fingerprinting to guess remote operating system. Only the users have root privilege can do this function. Figure 2.1 displays the result of Nmap. The outcome reveals the hostname of target machine is *ap3* and the OS is *Zcomax Wireless Access Point XI-1500*. According to these clues, we can firmly believe that machine is an AP.



```
[root@netlab tmp]# nmap -O -sT -sU 140.113.24.3

Starting Nmap 4.03 ( http://www.insecure.org/nmap/ ) at 2006-06-20 14:31 CST
Interesting ports on ap3.csie.nctu.edu.tw (140.113.24.3):
(The 3154 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
Device type: WAP
Running: Zcomax embedded
OS details: Zcomax Wireless Access Point XI-1500

Nmap finished: 1 IP address (1 host up) scanned in 9.594 seconds
```

Figure 2.1: Scan result of Nmap.

The advantages of TCP/IP fingerprinting is that the network administrators can simply start up a tool such as Nmap which performs TCP/IP fingerprinting and let it scan entire network while they deal with other work, i.e. the network administrators do not need concentrate their attention on Nmap while it is scanning.

The disadvantages of this method are illustrated as follows:

1. If the network of enterprise is large, it could take a long time to scan entire

network.

2. The behavior of determining the operating system is intrusive. If target machine has firewall or intrusion detection system (IDS), the scan will fail.

3. TCP/IP fingerprinting is not 100% accurate. Detection tools such as Nmap use information of TCP/IP fingerprinting to guess operating system running on target machine, it might be bring a false-positive or false-negative result.

B. SNMP Scanning

The idea of SNMP scanning is similar to TCP/IP fingerprinting. SNMP scanning utilize information obtained by using the SNMP protocol instead of observing the differences in the TCP/IP fingerprinting. If a machine its UDP port 161 is open, it represents that machine is running the SNMP service.

In SNMP protocol, the management information base (MIB) is a database that records the information of network devices. Tools like snmpwalk [3] is an SNMP application that uses SNMP GETNEXT requests to query a network device for a tree of management information. Network administrators can tell this device operating system by the SNMP variable, *system.sysDescr*, from SNMP GETNEXT response from this network device.

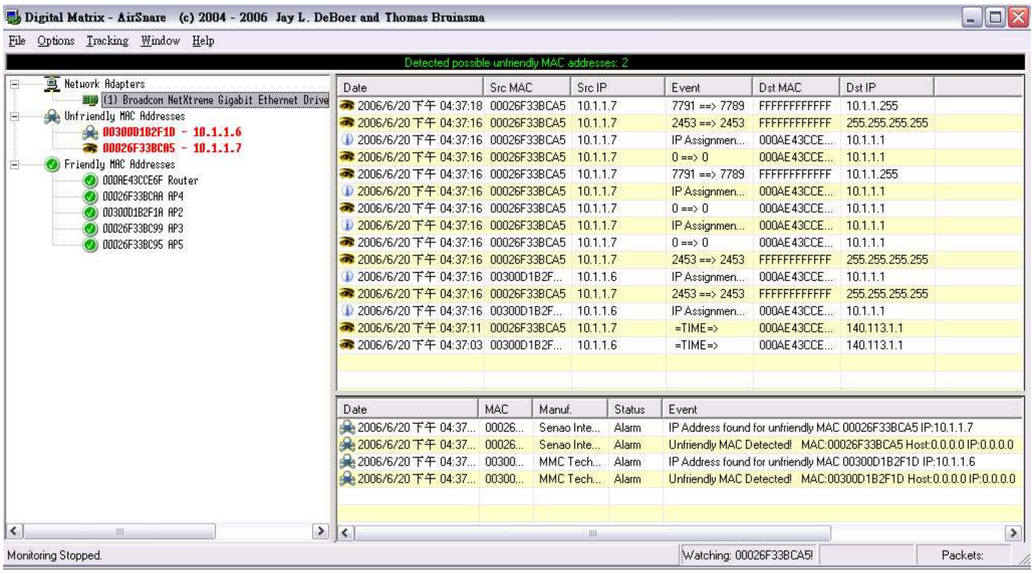
One advantage of SNMP scanning is similar to TCP/IP fingerprinting. Network administrators can simply start up a tool such as snmpwalk which performs SNMP scanning and let it scan entire network while they deal with other work. Other advantage that SNMP scanning is more accuracy than TCP/IP fingerprinting. Because SNMP scanning determines the system information is using the information acquired from MIB. But TCP/IP fingerprinting is using the difference in field of packet to guess the operating system of target machine.

The main disadvantage of SNMP scanning is that not all APs support SNMP or some APs may be turned off SNMP service. In those situations, it is impossible to get information of devices by SNMP scanning.

C. Packet Sniffing

The manner of packet sniffing is to configure a wired network device to run in promiscuous mode. In an Ethernet local area network (LAN), promiscuous mode is a mode of operation in which every data packet transmitted through LAN can be received and read by a network adapter. The devices that operate in promiscuous mode capture all data packets in the LAN and analyze the Ethernet headers of packets to check the MAC addresses are authorized MAC addresses or not.

An example of a tool that monitors MAC addresses of packets is AirSnare [4]. AirSnare is a free program that captures all packets in LAN and checks the MAC addresses whether they are authorized or not. At first, the network administrators have to specify a list of friendly trusted MAC addresses. If an unknown MAC address is found, the program will take this MAC address is unfriendly and send an alert to the network administrators. A screenshot of AirSnare is displayed in figure 2.2.


Digital Matrix - AirSnare (c) 2004 - 2006 Jay L. DeBoer and Thomas Bruinsma
File Options Tracking Window Help

Detected possible unfriendly MAC addresses: 2

- Network Adapters
  - (1) Broadcom NetXtreme Gigabit Ethernet Drive
- Unfriendly MAC Addresses
  - 00300D1B2F1D - 10.1.1.6
  - 00026F33BCA5 - 10.1.1.7
- Friendly MAC Addresses
  - 000AE43CCE6F Router
  - 00026F33BCAA AP4
  - 00300D1B2F1A AP2
  - 00026F33BC99 AP3
  - 00026F33BC95 AP5

Date	Src MAC	Src IP	Event	Dst MAC	Dst IP
2006/6/20 下午 04:37:18	00026F33BCA5	10.1.1.7	7791 ==> 7789	FFFFFFFFFFFF	10.1.1.255
2006/6/20 下午 04:37:16	00026F33BCA5	10.1.1.7	2453 ==> 2453	FFFFFFFFFFFF	255.255.255.255
2006/6/20 下午 04:37:16	00026F33BCA5	10.1.1.7	IP Assignmen...	000AE43CCE...	10.1.1.1
2006/6/20 下午 04:37:16	00026F33BCA5	10.1.1.7	0 ==> 0	000AE43CCE...	10.1.1.1
2006/6/20 下午 04:37:16	00026F33BCA5	10.1.1.7	7791 ==> 7789	FFFFFFFFFFFF	10.1.1.255
2006/6/20 下午 04:37:16	00026F33BCA5	10.1.1.7	IP Assignmen...	000AE43CCE...	10.1.1.1
2006/6/20 下午 04:37:16	00026F33BCA5	10.1.1.7	0 ==> 0	000AE43CCE...	10.1.1.1
2006/6/20 下午 04:37:16	00026F33BCA5	10.1.1.7	IP Assignmen...	000AE43CCE...	10.1.1.1
2006/6/20 下午 04:37:16	00026F33BCA5	10.1.1.7	0 ==> 0	000AE43CCE...	10.1.1.1
2006/6/20 下午 04:37:16	00026F33BCA5	10.1.1.7	2453 ==> 2453	FFFFFFFFFFFF	255.255.255.255
2006/6/20 下午 04:37:16	00300D1B2F...	10.1.1.6	IP Assignmen...	000AE43CCE...	10.1.1.1
2006/6/20 下午 04:37:16	00026F33BCA5	10.1.1.7	2453 ==> 2453	FFFFFFFFFFFF	255.255.255.255
2006/6/20 下午 04:37:16	00300D1B2F...	10.1.1.6	IP Assignmen...	000AE43CCE...	10.1.1.1
2006/6/20 下午 04:37:11	00026F33BCA5	10.1.1.7	=TIME=>	000AE43CCE...	140.113.1.1
2006/6/20 下午 04:37:03	00300D1B2F...	10.1.1.6	=TIME=>	000AE43CCE...	140.113.1.1

Date	MAC	Manuf.	Status	Event
2006/6/20 下午 04:37...	00026...	Senao Inte...	Alarm	IP Address found for unfriendly MAC 00026F33BCA5 IP:10.1.1.7
2006/6/20 下午 04:37...	00026...	Senao Inte...	Alarm	Unfriendly MAC Detected! MAC:00026F33BCA5 Host:0.0.0.0 IP:0.0.0.0
2006/6/20 下午 04:37...	00300...	MMC Tech...	Alarm	IP Address found for unfriendly MAC 00300D1B2F1D IP:10.1.1.6
2006/6/20 下午 04:37...	00300...	MMC Tech...	Alarm	Unfriendly MAC Detected! MAC:00300D1B2F1D Host:0.0.0.0 IP:0.0.0.0

Monitoring Stopped. Watching: 00026F33BCA5! Packets:

Figure 2.2: Using AirSnare to monitor MAC addresses of devices in LAN.

The main advantage of this method is that monitor action is continuous. The monitor constantly captures and analyzes any data in LAN. Once a rogue AP connects to the network and transmits any packet, the monitor can detect this rogue AP immediately.

The primary shortcoming of sniffing traffic is suffered from MAC spoofing. A device can easily cheat the detection system by changing its MAC address to an authorized one. There is also the problem of processing capacity. If the network is a high speed network it may be hard to process high volumes of traffic and perform the analysis.

D. Observation of traffic characteristics

Raheem Beyah et al. purposed a method that used temporal traffic characteristics to detect rogue APs at a central location [5]. A wireless link in a network path of multiple links would cause a more random and temporally different spreading of packets, as compared to a path that has only wired links. Every switch port will analyze inter-packet spacing over time. If the statistics of inter-packet spacing crosses a threshold, it is possible that there is a wireless link in LAN. But the flaw of observing traffic characteristics is that method only can detect rogue AP appearing in enterprise where the network is pure wired. Otherwise, inter-packet spacing may also increase in pure wired while the traffic is heavy in LAN. In this situation, the detection system will make an erroneous judgement.

2.1.2 Wireless Detection Approaches

In this section, we will introduce two kinds of wireless detection approaches. One of these two approaches, active probing, finds out the surrounding rogue APs actively. On the contrary, the other wireless detection approach, RF monitoring, is more passive than active probing. It only monitors the wireless traffic passively to discovery rogue APs.

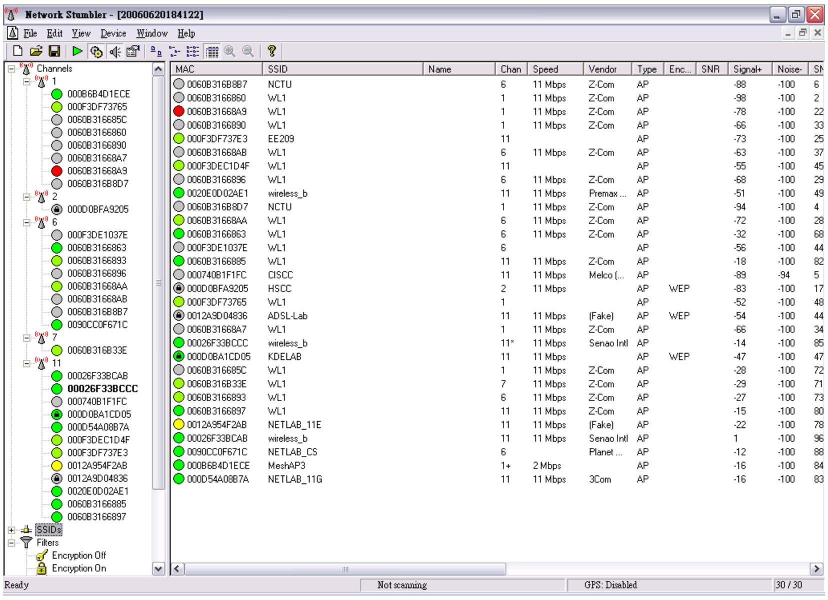
A. Active Probing

The active probing means that wireless stations send probe request frames on each channel actively. When an AP receives a probe request frame, it will reply a probe response frame with its MAC address, ESSID, etc. But this detection method will not be able to discover rogue APs that are configured not to advertise their ESSID or not to respond to probe requests. Once the station receives a probe request frame from AP, the next step is to identify whether it is a rogue or not. One way to do this is to use pre-configure authorized list of APs. Any detected AP that not on the authorized list would be identified it is rogue. Some of different ways to configure the authorized list:

- Permitted MAC address
- Permitted ESSID
- Permitted vendor
- Permitted Radio Media Type
- Permitted Channel

Tools like NetStumbler [6] lets network administrators to walk the halls of the enterprise or campus searching for rogue APs. NetStumbler works by sending out probe request frames and then listens for probe response frames from APs. Figure 2.3 shows the executing window of NetStumbler. The results of NetStumbler indicate some information about surrounding APs: what channel they were using, its vender, if WEP was enabled, etc.

If network administrators attempt to detect the rogue APs by using active probing, they must walk around the building with a laptop or a handheld device equipped analyzer tools. The periodic walk through is the only way to gather all APs in the building and check for unauthorized access points. It is an ineffectively detection method. It consumes a lot of time and manpower. Besides, this method is also easy to elude, since a rogue AP can easily be unplugged when the scan takes place.



- Channels
  - 1
    - 000B6B4D1ECE
    - 000F3DF73765
    - 0060B316685C
    - 0060B3166860
    - 0060B3166890
    - 0060B31668A7
    - 0060B31668A9
    - 0060B316B8D7
  - 2
    - 000D0BFA9205
  - 6
    - 000F3DE1037E
    - 0060B3166863
    - 0060B3166893
    - 0060B3166896
    - 0060B31668AA
    - 0060B31668AB
    - 0060B316B8B7
    - 0090CC0F671C
  - 7
    - 0060B316B33E
  - 11
    - 00026F33BCAB
    - **00026F33BCCC**
    - 000740B1F1FC
    - 000D0BA1CD05
    - 000D54A08B7A
    - 000F3DEC1D4F
    - 000F3DF737E3
    - 0012A954F2AB
    - 0012A9D04836
    - 0020E0D02AE1
    - 0060B3166885
    - 0060B3166897
- SSIDs
- Filters
  - Encryption Off
  - Encryption On

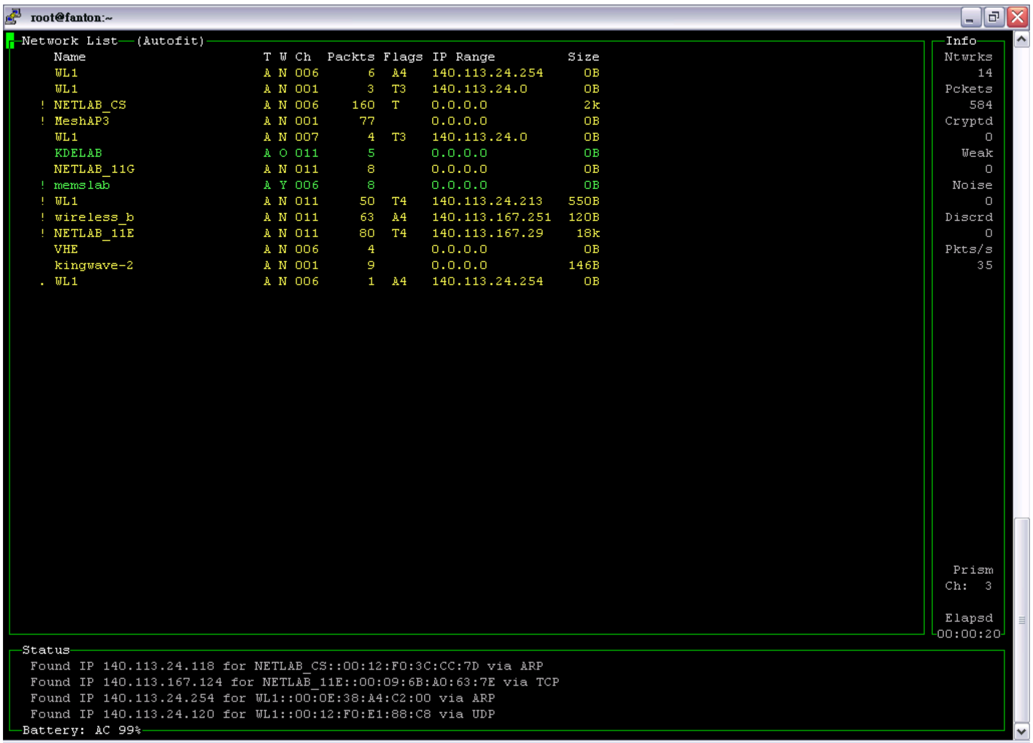
MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SN
0060B316B8B7	NCTU		6	11 Mbps	Z-Com	AP			-88	-100	6
0060B3166860	WL1		1	11 Mbps	Z-Com	AP			-98	-100	2
0060B31668A9	WL1		1	11 Mbps	Z-Com	AP			-78	-100	22
0060B3166890	WL1		1	11 Mbps	Z-Com	AP			-66	-100	33
000F3DF737E3	EE209		11			AP			-73	-100	25
0060B31668AB	WL1		6	11 Mbps	Z-Com	AP			-63	-100	37
000F3DEC1D4F	WL1		11			AP			-55	-100	45
0060B3166896	WL1		6	11 Mbps	Z-Com	AP			-68	-100	29
0020E0D02AE1	wireless_b		11	11 Mbps	Premax ...	AP			-51	-100	49
0060B316B8D7	NCTU		1	11 Mbps	Z-Com	AP			-94	-100	4
0060B31668AA	WL1		6	11 Mbps	Z-Com	AP			-72	-100	28
0060B3166863	WL1		6	11 Mbps	Z-Com	AP			-32	-100	68
000F3DE1037E	WL1		6			AP			-56	-100	44
0060B3166885	WL1		11	11 Mbps	Z-Com	AP			-18	-100	82
000740B1F1FC	CISCC		11	11 Mbps	Melco (...	AP			-89	-94	5
000D0BFA9205	HSCC		2	11 Mbps		AP	WEP		-83	-100	17
000F3DF73765	WL1		1			AP			-52	-100	48
0012A9D04836	ADSL-Lab		11	11 Mbps	(Fake)	AP	WEP		-54	-100	44
0060B31668A7	WL1		1	11 Mbps	Z-Com	AP			-66	-100	34
00026F33BCCC	wireless_b		11*	11 Mbps	Senao Intl	AP			-14	-100	85
000D0BA1CD05	KDELAB		11	11 Mbps		AP	WEP		-47	-100	47
0060B316685C	WL1		1	11 Mbps	Z-Com	AP			-28	-100	72
0060B316B33E	WL1		7	11 Mbps	Z-Com	AP			-29	-100	71
0060B3166893	WL1		6	11 Mbps	Z-Com	AP			-27	-100	73
0060B3166897	WL1		11	11 Mbps	Z-Com	AP			-15	-100	80
0012A954F2AB	NETLAB_11E		11	11 Mbps	(Fake)	AP			-22	-100	78
00026F33BCAB	wireless_b		11	11 Mbps	Senao Intl	AP			1	-100	96
0090CC0F671C	NETLAB_CS		6		Planet ...	AP			-12	-100	88
000B6B4D1ECE	MeshAP3		1+	2 Mbps		AP			-16	-100	84
000D54A08B7A	NETLAB_11G		11	11 Mbps	3Com	AP			-16	-100	83

Ready | Not scanning | GPS: Disabled | 30 / 30

Figure 2.3: Using NetStumbler to discover APs in WLAN.

B. RF monitoring

There is a lot of research in detecting rogue APs used RF monitoring [7][8][9]. RF monitoring is a completely passive method of wireless LAN discovery known as radio frequency monitoring (RFMON). A client with a wireless card that is configured in RFMON mode will be able to capture all RF signals on the channels to which it is configured to listen. This method can detect rogue APs by monitoring 802.11 frames transmitted from AP such as beacon frames. Each time a beacon frame is sniffed, the sniffer could compare the source MAC address of the frame with a list of registered APs. If the MAC address doesn't match with any record in the list, the sniffer would consider the AP to be a rouge one. Kismet [10] is a kind of tools using RF monitoring to detect network behavior. A screenshot of Kismet can be seen in figure 2.4.



```
root@fanton:~
Network List (Autofit)                                                       Info
    Name                        T W Ch  Packts Flags IP Range          Size  Ntwrks
    WL1                         A N 006      6  A4   140.113.24.254      0B      14
    WL1                         A N 001      3  T3   140.113.24.0        0B  Pckets
  ! NETLAB_CS                   A N 006    160  T    0.0.0.0             2k     584
  ! MeshAP3                     A N 001     77       0.0.0.0             0B  Cryptd
    WL1                         A N 007      4  T3   140.113.24.0        0B       0
    KDELAB                      A O 011      5       0.0.0.0             0B    Weak
    NETLAB_11G                  A N 011      8       0.0.0.0             0B       0
  ! memslab                     A Y 006      8       0.0.0.0             0B   Noise
  ! WL1                         A N 011     50  T4   140.113.24.213    550B       0
  ! wireless_b                  A N 011     63  A4   140.113.167.251   120B  Discrd
  ! NETLAB_11E                  A N 011     80  T4   140.113.167.29     18k       0
    VHE                         A N 006      4       0.0.0.0             0B  Pkts/s
    kingwave-2                  A N 001      9       0.0.0.0           146B      35
  . WL1                         A N 006      1  A4   140.113.24.254      0B

                                                                                  Prism
                                                                                 Ch:  3

                                                                                 Elapsd
                                                                               00:00:20
Status
 Found IP 140.113.24.118 for NETLAB_CS::00:12:F0:3C:CC:7D via ARP
 Found IP 140.113.167.124 for NETLAB_11E::00:09:6B:A0:63:7E via TCP
 Found IP 140.113.24.254 for WL1::00:0E:38:A4:C2:00 via ARP
 Found IP 140.113.24.120 for WL1::00:12:F0:E1:88:C8 via UDP
Battery: AC 99%
```

Figure 2.4: Using Kismet to discover APs in WLAN.

An advantage of RFMON is no limitation of only getting information from probe response frames. Further, wired packet sniffing and wireless RF monitoring are similar. They both detect rogue APs by sniffing and analyzing the packets on network. But the RF monitoring has less traffic to analysis in WLAN than LAN.

RFMON is a receive-only mode. While in RFMON mode, station are unable to transmit any frames; their cards are only able to receive, and therefore capture traffic. Another disadvantage of RF monitoring is similar to active probing. In order to scan all the AP in the building, IT personnel have to walk around with the laptop and handheld device that operates in RFMON.

2.2 Rogue Access Point Location

Nowadays indoor positioning solutions for WLAN mostly depend on signal strength utilization. We categorize WLAN-based indoor positioning into two main kinds: client-based and sniffer based. This classification bases on what kinds of devices takes charge to measure signal strength.

2.2.1 Client-Based Location

A basic design of client-based location utilizes two phases. First, in the offline phase, a model is constructed based on received signal strength at a finite number of locations within a target area. Second, during online operation in the target area, mobile stations report the signal strength received from each AP and the system determines the best match between online observations and the offline model. The best matching location is reported as the estimated position.

The main disadvantage of client-based location method is that spends a lot of time on constructing a pattern model. For examples, if we want to locate a device in a large building by using client-based location method. We need to walk to several locations in each floor and do signal strength measurement. This is an inefficient work. Another shortcoming of client-based location method is that mobile station need to reports the signal strength from each AP, this action have to modify the mobile station. It is impractical.

2.2.2 Sniffer-Based Location

To ease the burden of system maintenance, many enterprises prefer sniffer-based location method which simple sniffers monitor client activity and measure the signal strength of transmissions received from clients. The locations of sniffers are fixed and operate in a passive scanning mode to sense transmissions on all channels with sniffing software. The sniffers then put together signal strength measurement and using positioning algorithm to calculate the position.

The sniffer-based location method doesn't have to pre-construct the signal strength pattern. It's more effective than client-based location method. In sniffer-based location method, mobile stations don't need to report the received signal strength from each AP.

There are more advantages of sniffer-based location than client-based location, so we choose the former to be our location method to locate the rogue AP in this thesis.

Chapter 3

System Design

In this chapter, we will introduce our proposed detection method and the location method. The rogue APs detection methods we proposed can be separated into certificate-based and scan-based. The certificate-based detection can find out most rogue APs in target area. But there is a drawback of certificate-based detection, some rogue APs might evade detecting by using this drawback of certificate-based detection. For making up this shortcoming, we proposed scan-based detection to cooperate with certificate-based detection. Therefore, our proposed detection method can discovery all rogue APs in environment.

3.1 Certificate-Based Detection

The certificate-based detection is based on centralized system architecture. APs have to connect to a centralized server called access router (AR). This AR takes charge to determine AP is legal or rogue. In the section, we will first illustrate the whole system architecture and the function of each component in the system. The major detection procedure will describe in detail by message flow between AR and AP.

3.1.1 System Architecture

Figure 3.1 displays the whole system architecture. There are five kinds of devices: mobile station (STA), access point (AP), switch, access router (AR) and RADIUS server. The main device is AR. AR connects to Internet through public network and connects to APs through private network. In order to let AR determines the APs are rogue or legal and easily manage APs, all APs must access network through AR. Otherwise, AR utilizes firewall to restrict the data from APs.

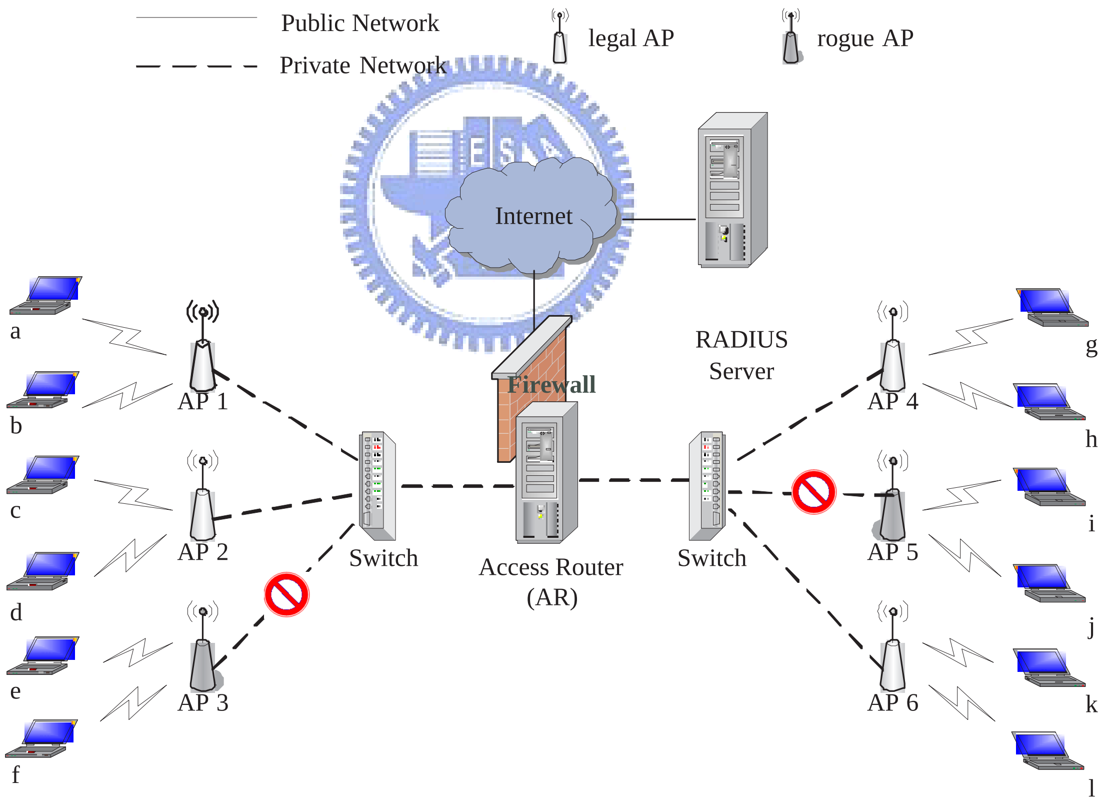


Figure 3.1: System Architecture.

3.1.2 System Components

There are four major components in detection system: mobile station (STA), access point (AP), access router (AR) and RADIUS server. Each component plays a different role in the detection system. We give a description of each component as follows:

1. Mobile station (STA)

STA is any portable device such as laptop or personal digital assistant (PDA) that equipped wireless network interface card (NIC). STA must associate with an AP to gain network access capability. STAs generally choose the AP that signal strength is the strongest to connect, they don't know the AP is rogue or not. If STAs connect to a rogue AP, they will transmit data through an unauthorized AP. Because STAs can not prevent connecting to a rogue AP, so the detection system architecture must be well designed to against rogue APs.

2. Access point (AP)

In our system architecture, all APs directly connect to AR to access Internet. In this system architecture, APs can not function like general APs, because they have to work with AR. This kind of APs they can not operate individually, it must cooperates with and be verified by AR. The detailed operation of AP will introduce in section 3.1.3.

3. Access Router (AR)

AR plays the major role in rogue detection system. Because of the centralized architecture, AR can gather information from each AP and check the AP is rogue or not. AR will determine an AP by its MAC address and certificate. If the

AP is legal, the firewall on AR will pass all data from this AP. On the contrary, the firewall on AR will drop all data from rogue AP. AR also cooperates with a RADIUS server to achieve user (STA) authentication.

4. **RADIUS server**

RADIUS server is used to authenticate users by checking the identity and password of user.

3.1.3 Main State Machine

In our system architecture, all APs must connect to AR. Because of this system design, AP don't function like tradition one. In order to let AP cooperates with AR, we have to do some modification of functionality of AP. We learn this concept from Light Weight Access Point Protocol (LWAPP) [11] and do some modification of state machine of AP defined in LWAPP. Figure 3.2 illustrates the main state machine of AP in our system.

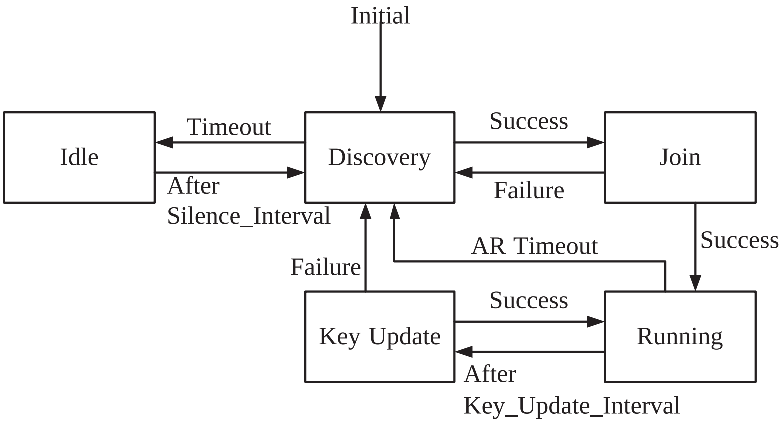


Figure 3.2: State machine of AP.

We specify every state in detail as follows:

1. At the beginning, an AP turns on its power, it enters the Discovery state. In the Discovery state, AP attempts to find out any AR in the network. If AP finds out an AR, it enters the Join state immediately. If AP doesn't receive any response from AR, it enters the Idle state.

2. When AP in the idle state, AP do nothing and just idle. After a silence interval, AP enters the Discovery state again to find out any AR.

3. AR verifies the identity of AP is the main goal of the Join state. If AP passes the verification by AR, it will enter the Running state. Otherwise, AP will go back to Discovery state. (After AR check the validity of AP, AR will generate a session key that to secure some message transmitted between AP and AR)

4. In the Running state, AP has network access ability so it can serve mobile stations with wireless transmission. AP will check the connection with AR by sending echo message periodically. If AR doesn't response, AP determines the connection with AR is disconnected. In this situation, AP will go back to Discovery state to find out another AR.

5. In the Running state, AP will use the session key to encrypt or decrypt some messages. As far as security concern, the session key must update periodically. This action try to avoid that attacker collects plenty encrypted messages and then breaks the session key. For this reason, when the session key expires (after a key update interval), AP will enter the Key Update state to get a new session key.

6. In the Key Update state, AR will generate a new session key to AP. If key update procedure is failure, AP will return to the Discovery state.

3.1.4 Detection Procedure

In this section, we will describe how AR verifies an AP and detect a rogue AP by illustrating the entire message flows. Figure 3.3 displays the message flows between AP and AR.

1. *Discovery Request / Response*

   AP attempts to seek any AR in the network by sending Discovery Request. Once AR receives a Discovery Request, AR will reply Discovery Response to the address in the source address of the received Discovery Request.

2. *Join Request / Response*

   Join Request is sent by an AP in the Join state after receiving Discover Response from AR. The Join Request is used by an AP to inform an AR that it wishes to gain access ability through AR. When an AR receives a Join Request it will reply a Join Response. The AR will check the MAC address and verify the certificate found in the request. If the MAC address and certificate are valid, the AR generates a session key which will be used to secure the connection between AR and AP.

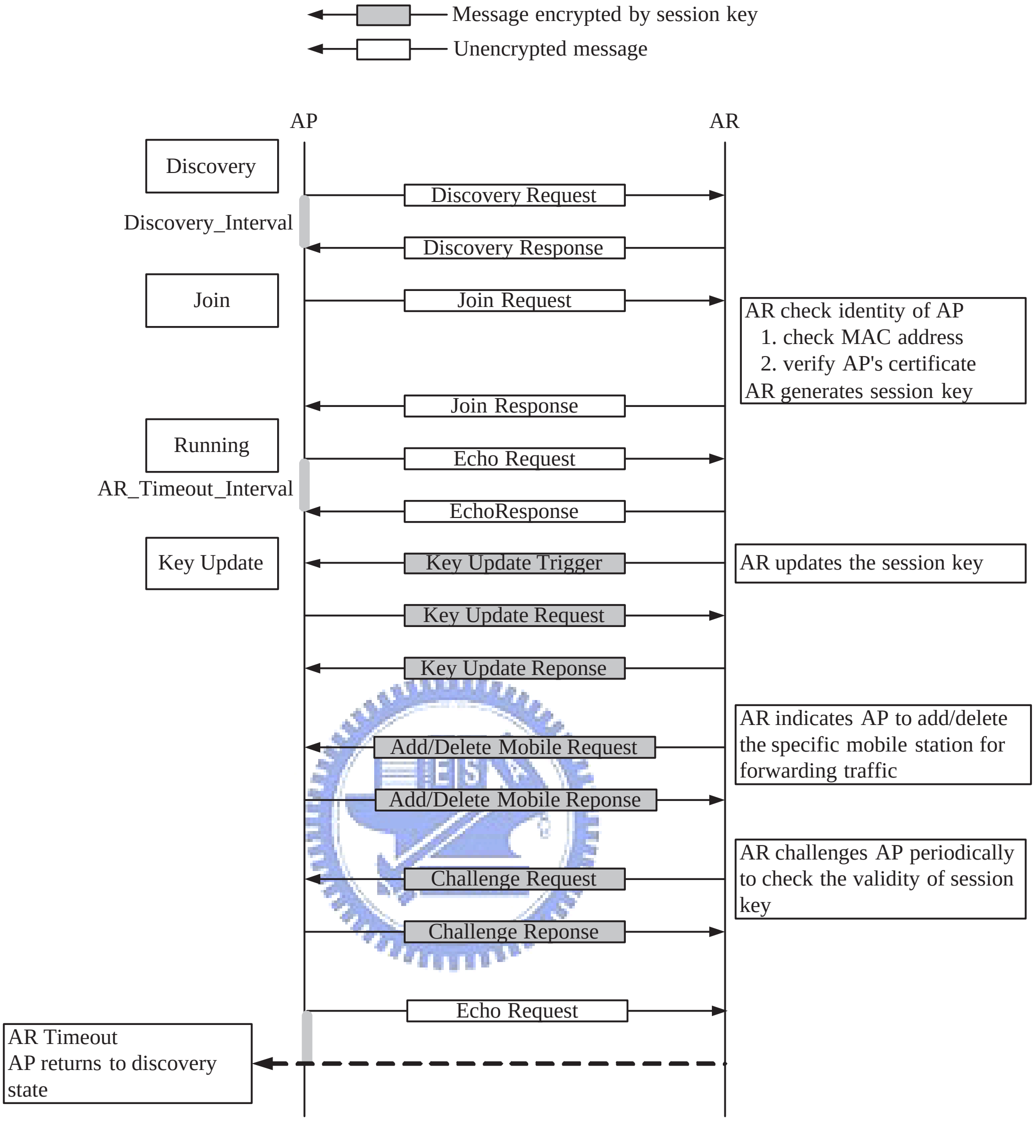


Figure 3.3: Message flows between AP and AR.

The AR can validate the identity of AP and detect it is rogue or not in a single round trip using the Join Request/Response. Figure 3.4 displays the detection flowchart. The detail validation and detection procedure is described below.

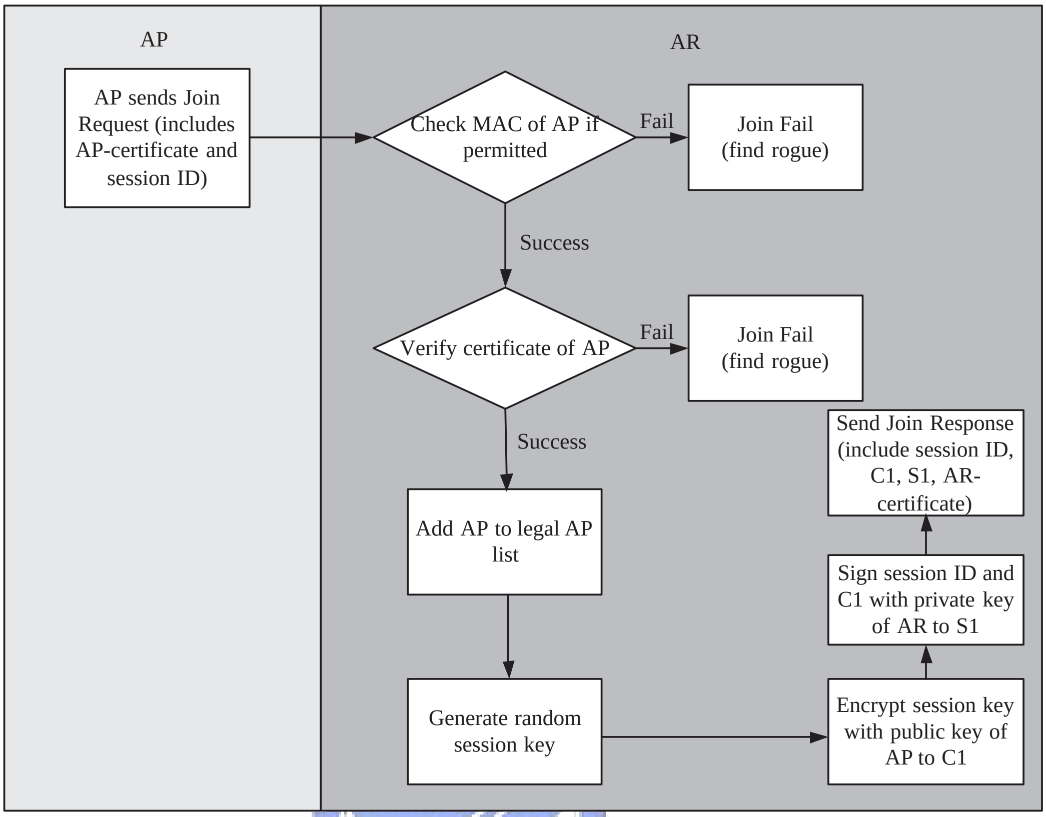

AP
AR
AP sends Join Request (includes AP-certificate and session ID)
Check MAC of AP if permitted
Fail
Join Fail (find rogue)
Success
Verify certificate of AP
Fail
Join Fail (find rogue)
Success
Add AP to legal AP list
Generate random session key
Encrypt session key with public key of AP to C1
Sign session ID and C1 with private key of AR to S1
Send Join Response (include session ID, C1, S1, AR-certificate)

Figure 3.4: Flowchart of certificate-based detection procedure.

(a) *Check the MAC address of AP*

AR has a list established by network administrators that records the permitted MAC addresses. When users want to install an AP in enterprise network, they must inform network administrators about its MAC address and then network administrators will add this MAC address into list. After AR receiving a Join Request, it will compare the MAC address of received request with the records in the list. Only the MAC address appears on the list, AR progress to next check procedure. Otherwise, the AP will be treated as a rogue one.

(b) *Verify the certificate of AP*

AR determines that AP is legal or rogue by its MAC address is not enough. Because MAC address can be easily modified by attacker. Attacker can sniff the traffic on the network and trace the MAC address of authorized AP. Then attacker can masquerade to a legal AP by modified its MAC address. So our detection approach not only checks MAC address but also verifies certificate of an AP.

In the Join request, AP includes its identity certificate and a randomly generated session ID which functions as a nonce to avoid replay attack. After AR checking the MAC address of AP, it will further verify the certificate of AP. If the certificate of AP is invalid, this AP is treated as a rouge AP. If the certificate of AP is valid, AR will record the information (ex: MAC address, SSID, IP, etc.) of this AP into a *legal APs list*. AR constructs the payload of Join Response as follows:

- Randomly generate a session key. Encrypt this session key with the public key of AP to C1, so that only the AP can decrypt it and determine the session key. (public key of AP can find in its certificate)
- Compute the AR's digital signature over the concatenation of the session ID and C1 to S1. This digital signature is encrypted with the private key of AR and can be verified by using the public key of AR. The purpose of this signature want to prove this frame is produced by the AR.

AR replies the Join Response with its certificate, C1, S1, and session ID to AP. When AP receives the Join Response, it will first check the session ID whether match an outstanding request. Then AP will verify the certificate of AR and use its pubic key and private key of AR to decrypt C1 and S1. During these procedures, if any examination or computation is failed, AP will consider the AR is illegal and then return to Discovery state.

AR can determine an AP if rogue or not by verifying corresponding payload of the Join Request. Otherwise, after exchanging the Join Request and Response, AP and AR will accomplish mutual authentication and a session key exchange.

3. *Echo Request / Response*

The purpose of sending Echo Request and Response is to determine the connection between AR and AP is still alive. AP will send Echo Request periodically. If AP doesn't receive any Echo Response after sending Echo Request, AP determines the AR is dead and goes back to Discovery state. On the other hand, if AR doesn't receive any echo request in a specific period, AR thinks the connection with AP is broken or AP is dead and then AR will delete this AP in legal APs list.

4. *Key Update Trigger / Request / Response (Encrypted)*

   As far as security concern, the session key must update periodically. This action try to avoid that attacker collects plenty encrypted messages and then break the session key. Key update procedure initiates by AR sending Key Update Trigger to AP. After AP receives a Key Update Trigger, the rest of message exchange is similar to Join Request and Response without certificate verification. AP will generate a new random session ID and include this new session ID to Key Update Request. When the AR receives Key Update Request with new session ID it constructs the Key Update Response payload as same as Join Response.

5. *Add / Delete Mobile Request / Response (Encrypted)*

   In our system, AR cooperates with RADIUS server to achieve STA authentication. If the STA is authenticated, AR will send the Add Mobile Request to inform an AP that it should forward traffic from this particular mobile station. If the STA authenticate of RADIUS server is failed, AR will send the Delete Mobile Request to inform the AP to terminate service to the particular mobile station.

6. *Challenge Request / Response (Encrypted)*

   The intention of sending encrypted Challenge Request to AP is to prevent unauthorized AP utilizing MAC spoofing. For instance, an authorized AP gains network access ability through AR after checking MAC address and verifying certificate. The attacker cracks this authorized AP and make the

AP can not work anymore. After that, attacker pretends to the authorized AP using MAC address of this authorized AP. If there is no policy to check this situation, it might exist some rouge AP masquerades to an authorized one and access network information.

To solve MAC address spoofing, AR will periodically send encrypted Challenge Request to AP. Although the rogue AP pretends to a legal AP by spoofing the MAC address, they don't have correct session key. Therefore, the rogue AP can not decrypt the Challenge Request correctly. If message doesn't decrypt successfully, the AP can not recognize this message and send the corresponding response to AR. Once AR doesn't receive any Challenge Response, it determines the MAC address spoofing happened and threat this AP as a rogue AP.

3.1.5 Firewall

In certificate-based detection, we utilize AR to check MAC address of AP, verify certificate of AP and periodically challenge AP to detect rogue APs. Besides, we apply firewall system on AR to restrict the network access ability of AP. Only authorized AP can access network, the firewall will drop any packets from rogue APs.

Firewall on AR adds *DROP* rule in following situation:

- AR turns on

Firewall on AR adds *ACCEPT* rule in following situation:

- Check MAC address and verify certificate of AP succeed
- Receive Add Mobile Request

Firewall on AR deletes *ACCEPT* rule in following situation:

- Session key of AP is error
- AP timeout
- Receive Delete Mobile Request

3.1.6 Summary of Certificate-Based Detection

In this section, we explain the certificate-based detection in detail. The contents included system architecture, system components, main state machine of AP, detection procedure, and firewall. The key features of certificate-based detection are listed below:

1. Centralized system architecture
2. AR takes charge of detecting rogue APs
3. AR determines an AP is legal or rogue by checking its MAC address and certificate
4. AR restricts ability of APs to access network by applying firewall, AR only forward data from legal APs
5. AR can find out MAC address spoofing of APs by periodically sending encrypted Challenge Request

3.2 Scan-Based Detection

In section 3.1, we introduced a certificate-based detection. The certificate-based detection can manage and detect most APs in enterprise network. There is one shortcoming of certificate-based detection design, some APs can not be found by certificate-based detection in a particular situation. We will describe how this situation happened in section 3.2.1. For making up the drawback of certificate-based detection, we propose a scan-based detection to function together with certificate-based detection. When certificate-based detection cooperates with scan-based detection, we can detect all rogue APs in the environment.

3.2.1 Drawback of Certificate-Based Detection

In certificate-based detection, we assume all APs connect to AR directly. But maybe there are some APs to gain network access ability by connecting backbone not AR. In this situation, AR can not manage AP and verify its identity. Therefore, AR can not detect these AP is rogue or legal. Figure 3.5 displays that AP7 directly connects to backbone network so AR can not know the existence of this AP.

3.2.2 Design of Scan-Based Detection

Maybe some APs connect to backbone network directly to evade detecting by certificate-based detection. But we can scan all the channels to listen beacons broadcasted from APs for checking MAC address whether authorized or not. For this kind detection, network administrators must walk around the building with a

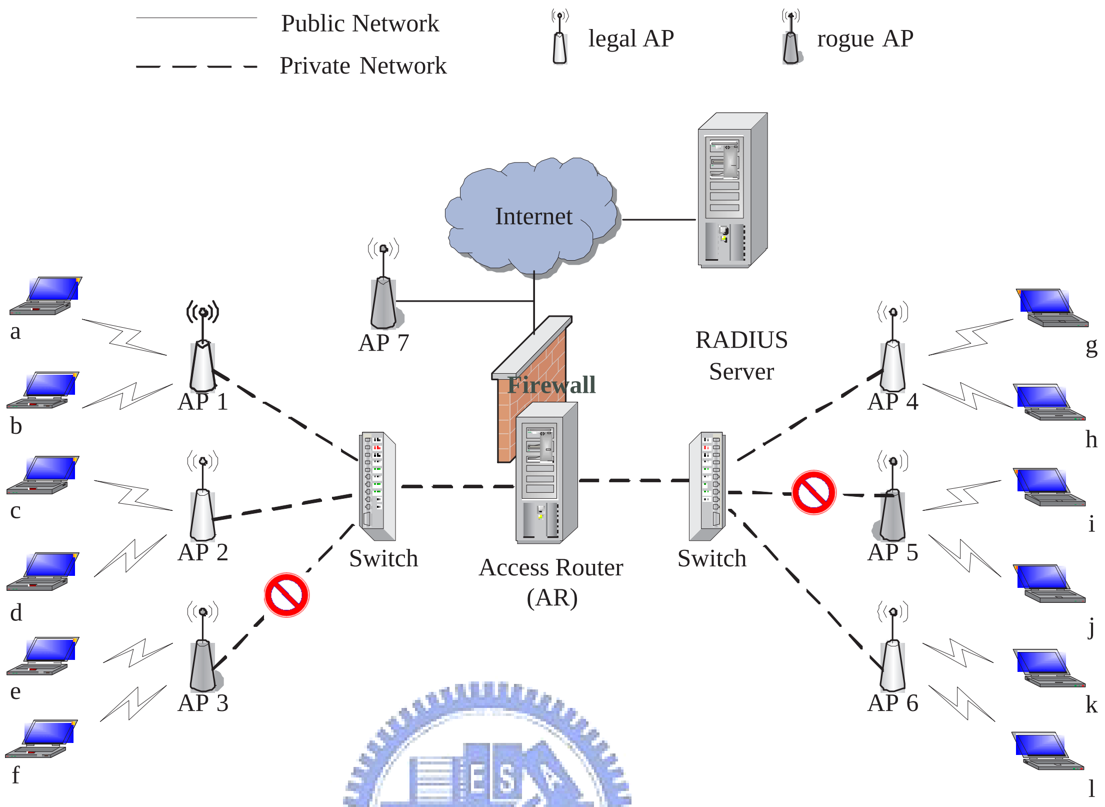


Figure 3.5: AP7 can not be detected by AR.

laptop or a handheld device equipped sniffer tools. The periodic walk through is to check for unauthorized access points. But the drawback of this detection method is ineffective. It consumes a lot of time and manpower. Besides, this method is also easy to elude, since a rogue AP can easily be unplugged when the scan takes place.

In scan-based detection, we also need devices to listen beacons in all channels. But the difference is that we utilize legal APs to scan not general handheld devices equipped with sniffer that must walk around the building.

Most of APs are designed not to process received beacon frames from other APs. When wireless NIC of APs receive any beacon frame from other APs, the driver of wireless NIC will discard immediately. So we want to legal APs to help us scan beacon frames, we need to modify the source code of access point to enable that AP can receive beacon frames from other APs and reports the scanned results to network administrator periodically.

The legal APs periodically scan beacon frames in all channels and then report the results to network administrators. The scan result includes source MAC addresses, SSID of beacon frames and the signal strength that legal AP received the beacon frame. When network administrators receive the scan results from legal APs, AR will compare the records in scan results with the legal APs list in AR. The network administrators can find out a rogue AP if there is a record in scan result but not in the legal APs list stored in AR.

The legal APs periodically scan the channels to gather beacon frames from other APs. The action, periodically scan, means that scan action is taken at every fixed interval. We called this interval *fixed scan interval.* If users who set up rogue APs know about this interval, they can elude detecting from our scan-based detection by turning off rogue APs at every fixed scan interval. To deal with this situation, we made the scan interval different in each round. The advantage of *random scan interval* is that users are difficult to let their rouge APs evade detecting because the intangible scan interval is hard to obtain. Therefore, the scan-based detection with random scan interval can prevent the users, who know the fixed random interval, let their rogue APs eschew detecting.

3.3 Sniffer-Based Location

The sniffer-based location method is chosen in this thesis. In sniffer-based location, the network administrators develop several sniffers with fixed location. These sniffers take charge to measure the signal strength received from object devices. In our system, the legal APs play roles as these sniffer and the object devices are the detected rogue APs.

The position algorithm that we choose is based on radio propagation model (Eq. 3.1). The following equation calculates the received signal power at distance d from the transmitter.

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \tag{3.1}$$

P_t is the transmitted signal power. G_t and G_r are the antenna gains of the transmitter and receiver respectively. L (L $\geq$ 1) is the system loss and λ is the wavelength. We assume P_t, G_t and G_r of each AP is the same.

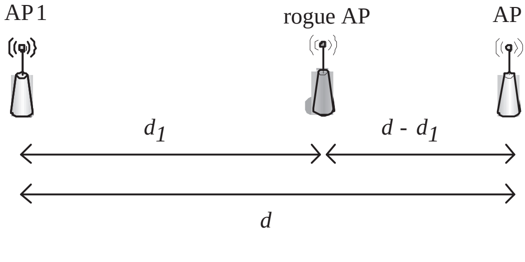


Figure 3.6: The distance between rogue AP and AP1/AP2.

We choose two legal APs which both received the beacon from the same rogue AP, see figure 3.6. P_{r1} and P_{r2} are the received signal strength at the legal AP1 and AP2. We measure the distance d between these two legal APs. We make the notation d_1 that represents the distance between rogue AP and the legal AP1; $d - d_1$ represents the distance between rogue AP and the legal AP2. We can computer the d_1 by Eq. 3.2.

$$\frac{P_{r1}}{P_{r2}} = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 {d_1}^2 L} \times \frac{(4\pi)^2 (d - d_1)^2 L}{P_t G_t G_r \lambda^2} = \frac{(d - d_1)^2}{{d_1}^2} \tag{3.2}$$

The P_{r1}, P_{r2} and d are known number, so we can calculate the d from Eq. 3.2.

Chapter 4

Implementation and Performance Evaluation

In this section, we describe our experimental environment and the rogue AP management program of scan-based detection in section 4.1 and 4.2 respectively. In section 4.3, we show the performance of our detection system.

4.1 Experimental Environment

The experimental environment of rogue AP detection system is shown in figure 4.1. We had installed three access points: AP1, AP2, and AP3 on the fourth floor in the Engineering Building III of NCTU. These three APs all connect to AR and pass the identity check with their certificates by AR. The following paragraphs describe each component in more detail.

A. Access Router (AR):

We used Fedora Core 4 as the OS and iptables as the firewall of the AR. (Iptables is the Linux packet filtering tool). There are two wired network interface

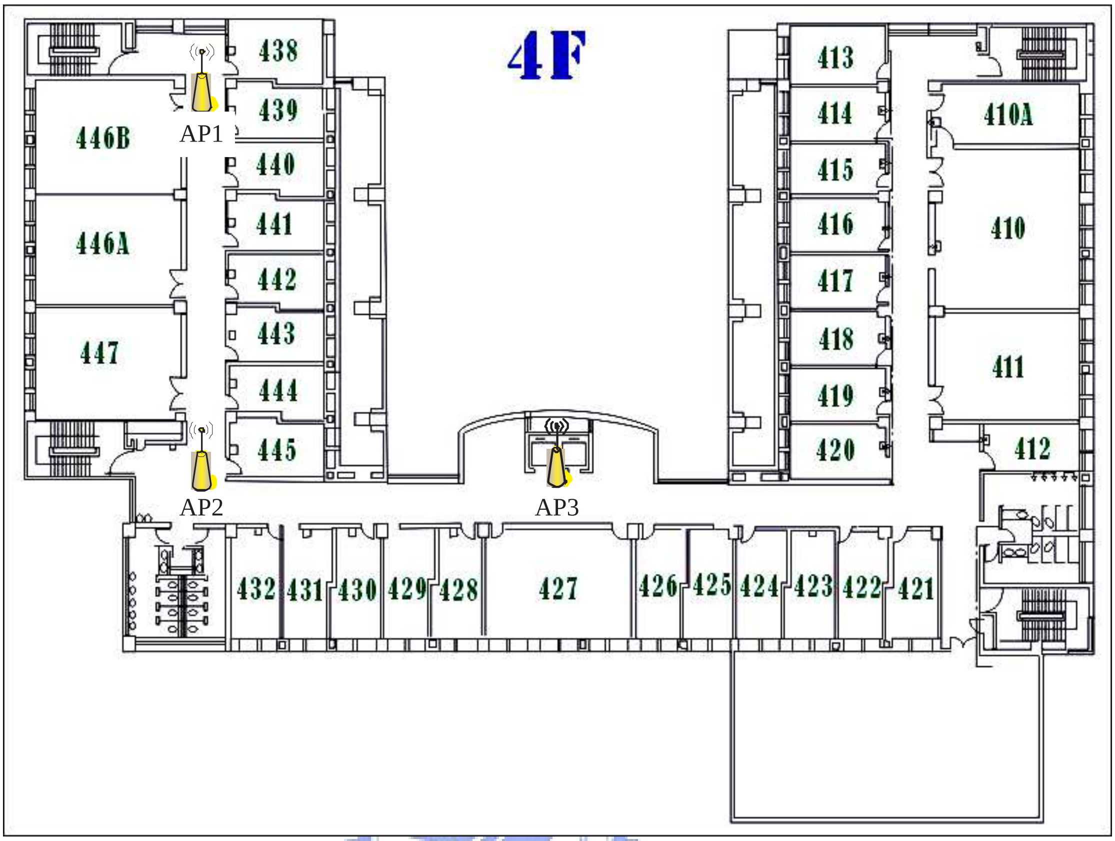


Figure 4.1: Experiment Environment.

cards (NIC) on the AR. One is connect to Ethernet with public IP and the other one is connected to AP with private IP.

B. Access Point (AP):

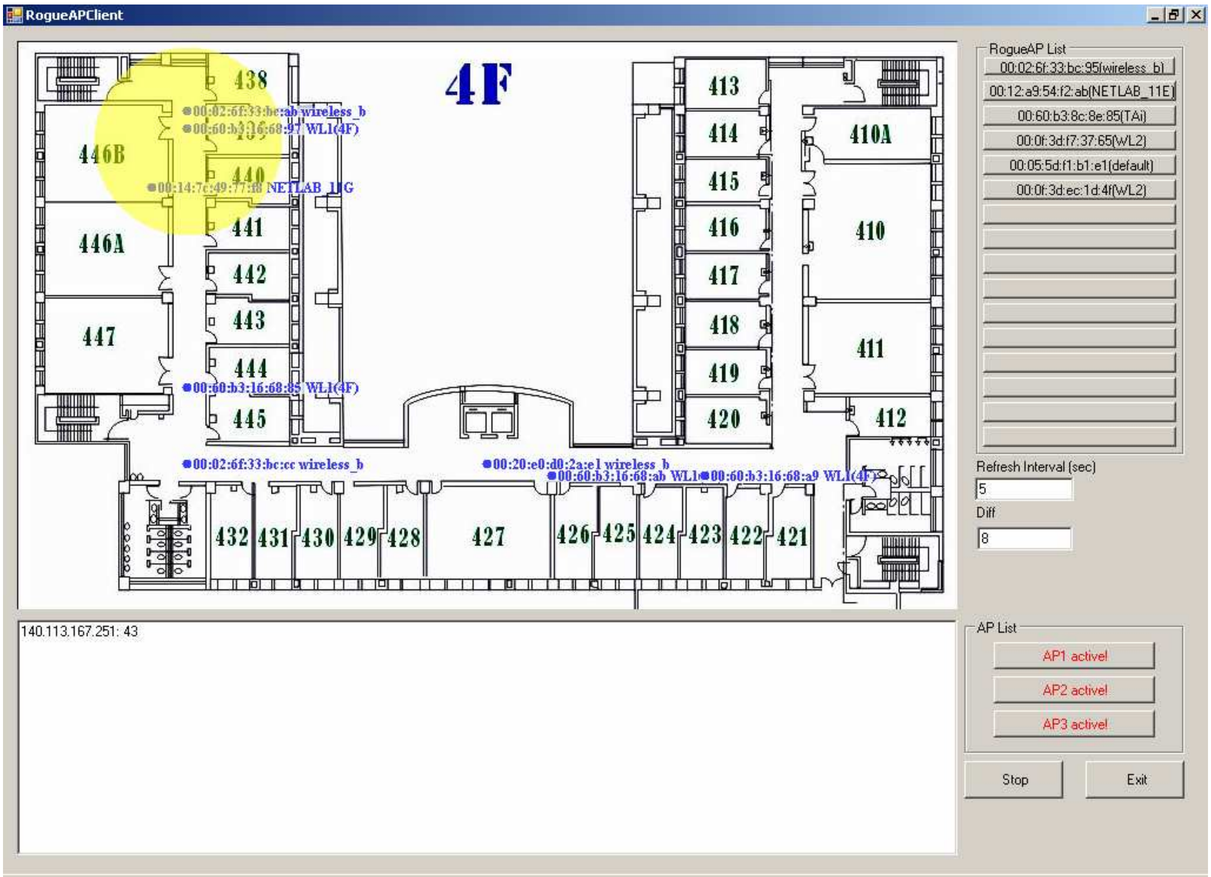
We use InterEpoch access point [12] as the platform. The chipset of this kind of AP is Intersil's Prism2.5 which can work with the HostAP driver [1] to emulate the access point. We modified the source code of HostAP to enable AP can communicate with AR and scan beacon frames from other APs.

C. Network Manager:

We used Windows XP as the platform. The network manager can gather the scan results from legal APs and compare with the legal APs list in AR by the management program. The program can show the information and the location of detected rogue AP.

4.2 Rogue AP management program of scan-based detection

The management program is displayed in figure 4.2. After the legal APs transmitted the scan results to network manager, the network manager can detect a rogue AP by comparing with the legal APs list in AR. The legal APs are shown on the left-hand map and the rogue APs are shown on the right-hand button. The network administrator can click the button and the program will display the location of the rogue AP on the left-hand map. The location of rogue AP is calculated by the location method we discussed in section 3.3.


RogueAPClient
4F
438
439
440
441
442
443
444
445
446B
446A
447
432
431
430
429
428
427
426
425
424
423
422
421
413
414
415
416
417
418
419
420
410A
410
411
412
00:02:6f:33:bc:ab wireless_b
00:60:b3:16:68:97 WL1(4F)
00:14:7c:49:77:f8 NETLAB_11G
00:60:b3:16:68:85 WL1(4F)
00:02:6f:33:bc:cc wireless_b
00:20:e0:d0:2a:e1 wireless_b
00:60:b3:16:68:ab WL1
00:60:b3:16:68:a9 WL1(4F)
Stop
Exit

RogueAP List

- 00:02:6f:33:bc:95(wireless_b)
- 00:12:a9:54:f2:ab(NETLAB_11E)
- 00:60:b3:8c:8e:85(TAi)
- 00:0f:3d:f7:37:65(WL2)
- 00:05:5d:f1:b1:e1(default)
- 00:0f:3d:ec:1d:4f(WL2)

Refresh Interval (sec): 5

Diff: 8

```
140.113.167.251: 43
```

AP List

- AP1 active!
- AP2 active!
- AP3 active!

Figure 4.2: Management program after querying the scan results.

4.3 System Performance Evaluation

The certificate-based detection belongs to wired rogue AP detection method. We want to prove our certificate-based detection method that can find out rogue APs faster than other wired detection method. So, we took Nmap, one of wired detection method we discussed in chapter 2, compares with certificate-based detection. In figure 4.3, we can see that more APs in the environment, the less time that certificate-based detection spent.

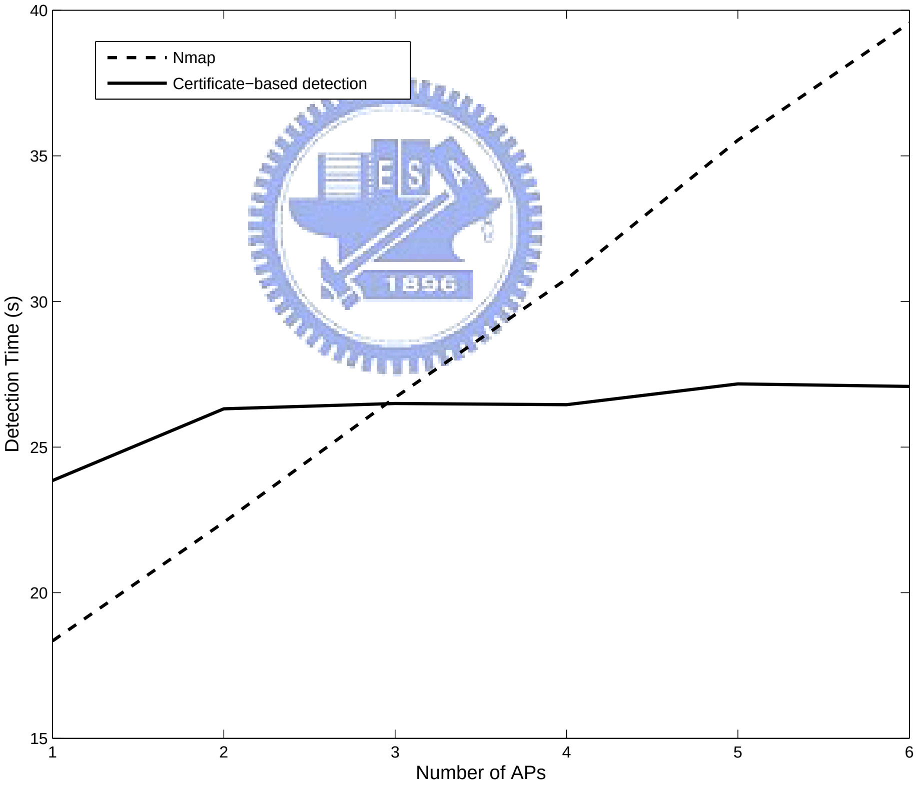


Figure 4.3: Detection time of certificate-based detection and Nmap.

Our detection method can detect the rogue AP with MAC spoofing by sending encrypted challenge message periodically. We set a parameter, Challenge Interval, to calculate when AR sends the next challenge message to AP. In the figure 4.4, we show the AR how long to detect MAC spoofing in difference Challenge Interval. From the result, the spending time of AR detected a rogue AP with MAC spoofing is approximate half Challenge Interval.

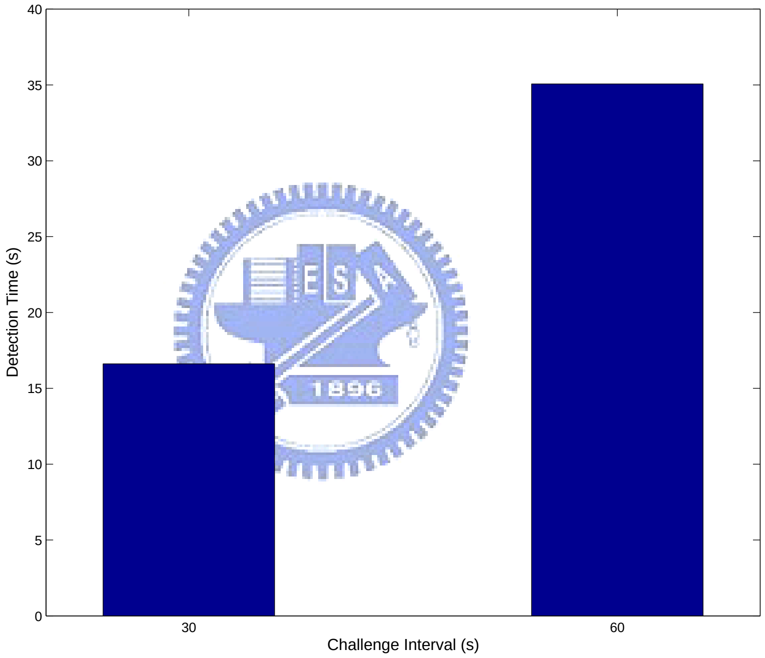


Figure 4.4: Detection time in different Challenge Interval.

In scan-based detection with fixed scan interval, AP has to scan periodically. In this situation, AP can not transmit any frame while it scans the channel. Figure 4.5 illustrates the relation between scan behavior and data throughput. In this evaluation, we use the software, NetIQ Chariot [13], to test the network performance. One station associated with the certificate-based AP or scan-based AP and then transmits 200M bytes data 100 times. The fixed scan interval of scan-based AP is 10 seconds. We can learn that throughput will drop in each 10 seconds while the scan takes place. Otherwise, the rest performance of scan-based AP is similar to certificate-based AP.

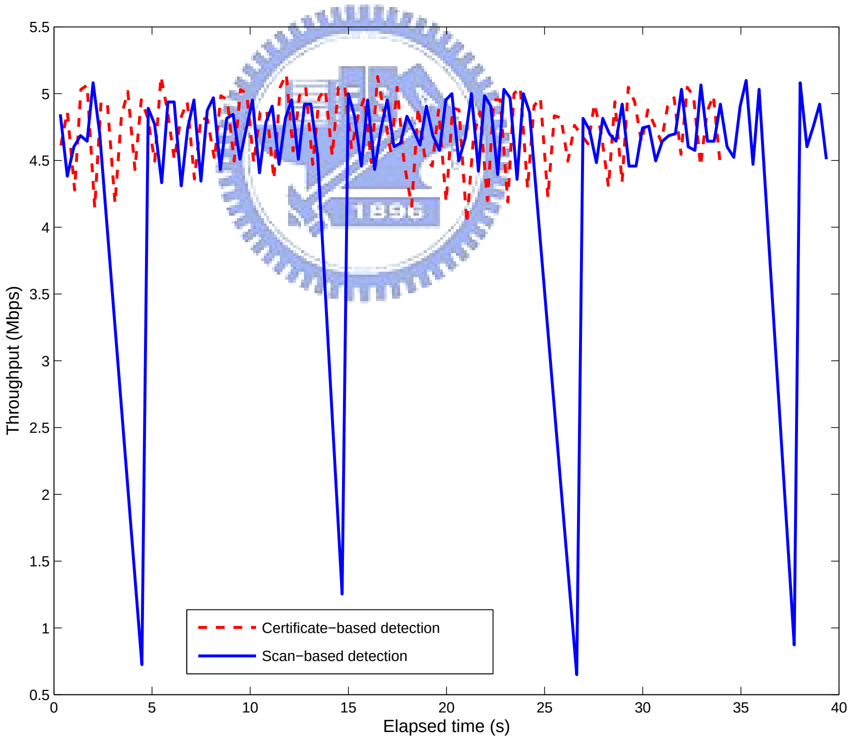


Figure 4.5: The relation between periodically scan behavior and throughput.

Figure 4.6 illustrates the relation between random scan interval and network throughput. The experiment parameters are the same with figure 4.5, but the scan interval is random, not fixed. We random choose a number from 1 10 to be next scan interval. We can notice that interval between each throughput drop is different.

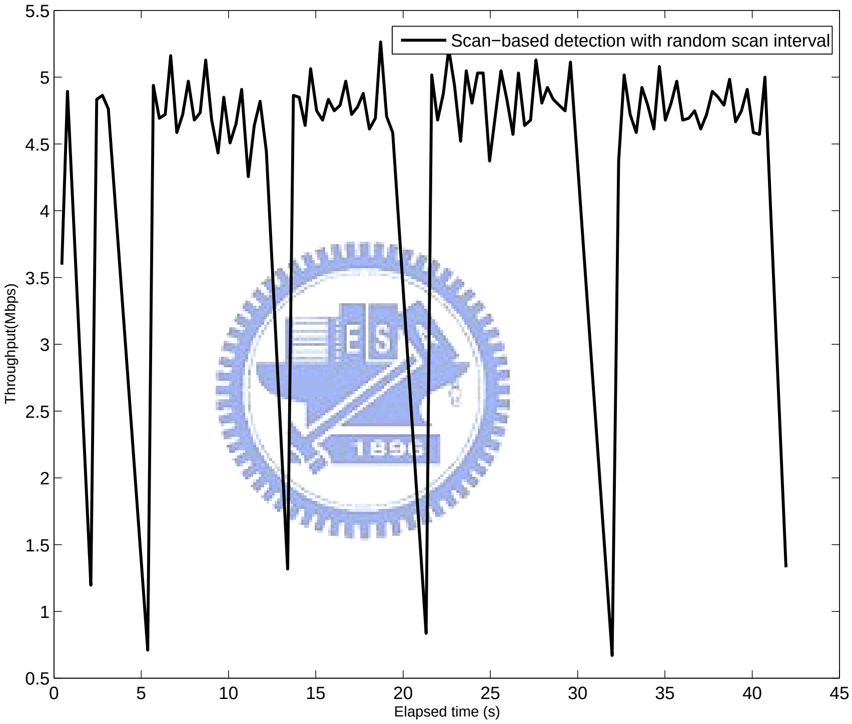


Figure 4.6: The relation between random scan behavior and throughput.

From these performance analyses, we can conclude some superiority of our detection system as follows:

- The detection is constantly, rogue APs can be detected immediately.
- The scan-based detection utilizes legal APs to scan beacon frames from other APs. Network administrators don't need walk around the building to scan. It's more efficient and hard to evade.
- AR can detect rogue APs with MAC spoofing by periodically sending encrypted challenge message to AP.
- We determine an AP is rogue by its information not just use traffic characteristic or OS information to guess. It is more accuracy.

Chapter 5

Conclusions and Future Work

In this thesis, we proposed a system that can detect and locate the rogue APs in WLNAs. First, we proposed the certificate-based detection method in centralized system architecture. The main role of certificate-based detection is the access route (AR). APs must connect to AR to be verified its certificate and then gain network access ability. There is an extraordinary advantage of certificate-based detection that deserves to be mentioned. Most of current detection approaches can not avoid MAC address spoofing, but AR can detect a rogue AP that masquerades an authorized one with MAC address spoofing by sending encrypted challenge message periodically. Although, the rogue AP change its MAC address to the authorized one from legal AP. They still don't have the session key so they do not have ability to correctly decrypt the challenge.

Nevertheless, there is one drawback of certificate-based detection. AR can not find out the rogue AP which connects to backbone directly not AR. For solving this shortcoming of certificate-based detection, we brought up the other detection method, scan-based detection, to cooperate with certificate-based detection. In scan-based detection, we modified the source code of AP to make AP can receive beacon frames from other APs. The legal APs will scan all the channels at fixed or random interval, and then send the scan results to the network manager. The network manager gathers the scan results from legal APs and compare with the legal APs list in the AR. If there is one MAC address that does not belong to legal APs list but appears in the scan result, the network manager will determine this AP is rogue.

The scan result contains the signal strength received at this legal AP. According to the signal strength, the network manager can calculated the location of the rogue AP and show this AP in map. Because radio transmission has propagation character, the signal strength will decrease while the distance between transceiver and receiver increase. We used this feature to calculate approximate location based on propagation model. In the future, we are going to considering more accurate poisoning method to locate a rogue AP more delicate.

Bibliography

[1] HostAP. A Linux driver for wireless LAN cards takes care of IEEE 802.11 management functions in the host computer and acts as an access point. [Online]. Available: http://hostap.epitest.fi/

[2] Nmap. A free open source utility is used for network exploration or security auditing. [Online]. Available: http://www.insecure.org/nmap/

[3] Snmpwalk. A SNMP application that uses SNMP GETNEXT requests to query a network entity for a tree of information. [Online]. Availiable: http://net-snmp.sourceforge.net/docs/man/snmpwalk.html

[4] AirSnare. A tool that monitors network traffic for unfriendly MAC addresses and alerts you when a MAC address is found that isn't on the friendly list. [Online]. Availiable: http://home.comcast.net/ jay.deboer/airsnare/

[5] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, "A Rogue Access Point Detection using Temporal Traffic Characteristics", In *Proc. of IEEE Global Telecommunications Conference (GLOBECOM)*, vol.4, pp. 2271-2275, Nov 2004.

[6] NetStumbler. A tool can monitor and analyze network traffic. [Online]. Available: http://www.netstumbler.com/

[7] M. K. Chirumamilla and B. Ramamurthy, ”Agent Based Intrusion Detection and Response System for Wireless LANs”, In *Proc. of IEEE International Conference on Communications (ICC)*, vol.1, pp. 492-496, May 2003.

[8] A. Adya, P. Bahl, R. Chandra, and L. Qiu, ”Architecture and Techniques for Diagnosing Faults in IEEE 802.11 Infrastructure Networks”, In *Proc. of ACM International Conference on Mobile Computing and Networking (MobiCom)*, pp. 30-44, Sept 2004.

[9] J. W. Branch, N. L. Petroni, L. V. Doorn, and S. David, ”Autonomic 802.11 Wireless LAN Security Auditing”, In *IEEE Security and Privacy Magazine*, vol.2, pp.56-65, May/June 2004.

[10] Kismet. An 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. [Online]. Available: http://www.kismetwireless.net/

[11] P. Calhoun, B. O’Hara, R. Suri, N. C. Winget, S. Kelly, M. Williams, and S. Hares, ”Leight Weight Access Point protocol”, *IETF Internet-Draft of Network Working Group*, June 2005.

[12] IWE2100-A. An 802.11a/g AP produced by InterEpoch Inc. [Online]. Available: http://www.interepoch.com.tw/products/datasheets/IWE2100-A.pdf

[13] NetIQ Chariot. A tool to test Network Performance. [Online]. Available: http://www.netiq.com/default.asp