Rogue AP Detection in the Wireless LAN for Large Scale Deployment

Sang-Eon Kim, Byung-Soo Chang, Sang Hong Lee
KT
17 Woomyeon-dong, Seocho-gu, Seoul 137-792, Korea

and

Dae Young Kim
Department of InfoComm Engineering, Chungnam National University
220 Gung-dong, Yusung-gu, Daejeon 305-764, Korea

ABSTRACT

The wireless LAN standard, also known as WiFi, has begun to use commercial purposes. This paper describes access network architecture of wireless LAN for large scale deployment to provide public service. A metro Ethernet and digital subscriber line access network can be used for wireless LAN with access point. In this network architecture, access point plays interface between wireless node and network infrastructure. It is important to maintain access point without any failure and problems to public users. This paper proposes definition of rogue access point and classifies based on functional problem to access the Internet. After that, rogue access point detection scheme is described based on classification over the wireless LAN. The rogue access point detector can greatly improve the network availability to network service provider of wireless LAN.

Keywords: WLAN, AP, xDSL, Metro Ethernet, DHCP

1. INTRODUCTION

Wireless LAN (WLAN) has become the preferred technology for wireless local area networking in both business and home environment. To provide commercial WLAN service, several requirements including [1, 2, 3] should be met. Users can enjoy Internet access using mobile device such as laptop, pocket PC and PDA with WLAN technology. As subscribers are increase, a service provider has to extend service areas such as airports, bus terminals, shopping malls, railway stations, parking lots, campuses and so on. The standards for WLAN have three kinds of specifications: IEEE 802.11a, 802.11b and 802.11g. IEEE 802.11b, also known as WiFi, are widely deployed and deploying. Also, advanced technologies related to wireless LAN are developing. Wi-Fi typically includes both network adapters and access points. The network adapter is available several kinds of devices such as external card, internal card and USB devices [4]. The network adapter includes a transmitter, receiver, antenna and hardware that provide data interface to the mobile nodes. The access point is a base station which is mounted in a fixed position and connected to a wired LAN. The access point includes transmitter, receiver, antenna and bridge that allow network adapter-equipped mobile nodes to communicate with wired LAN.

Each access point has a radio range [4], from approximately 20 to more than 100m, depending on the specific product, antennas, and operating environment. The access points provide an interface to IEEE 802.3 wired LAN.

Many access points have to be installed for public service due to its limited coverage. These access points should be managed to provide wireless Internet access. A rogue access point can not connect Internet. It can cause many problems from security holes to customers complain. Therefore it is important to manage access point by network management system (NMS) of service provider. A detection of rogue access point is one of the problems to be resolved [2] for commercial deployment with large scale.

In this paper we first present network architecture for public service. Section 3 proposes rogue access point and classifies based on functional problem to access the Internet. After that, section 4 describes the detailed detection scheme for implementation. The rogue access point detector can integrate network management system (NMS) [3].

2. NETWORK ARCHITECTURE

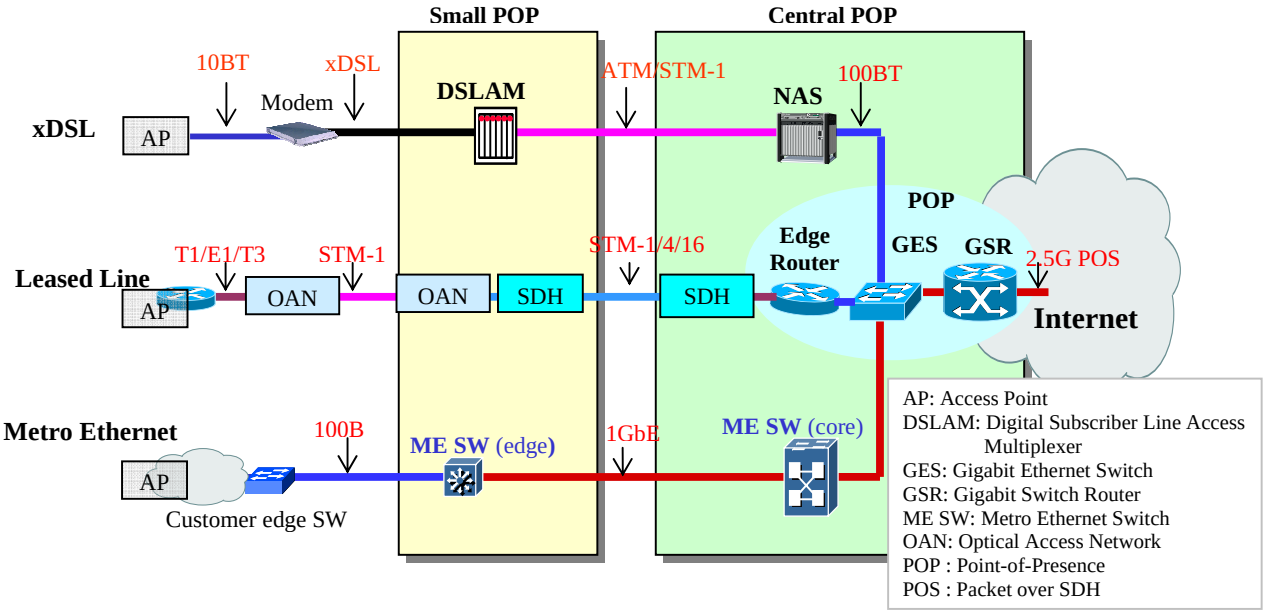
The WLAN standard [10] defines two basic modes of operation: the infrastructure network and the ad hoc network [11].

The infrastructure network is meant to extend the range of the wired LAN to wireless cells. A laptop can move cell to cell while keeping access to the resources on the wired LAN. A cell is the area covered by an access point and is called basic service set (BSS). The collection of all cells of an infrastructure network is called an extended service set (ESS). The ad hoc network mode is meant to easily interconnect laptops that are in the same area, for example in a meeting room. It is an island for independent networking.

The interconnected stations in ad hoc network mode are forming an independent basic service set (IBSS). These two operation modes are for a user interface to the network.

A network architecture for service providers depends on their environments such as mobile operator [12], large scale Internet service providers [13, 14], and access network architecture [15, 16, 17, 18]. The network architecture can be divided into backbone and access. In this paper we focus on access network which connects WLAN with infrastructure mode.

The network architecture to connect millions of customer with access point is shown in Figure 1. In fact, several ISPs have deployed metro Ethernet to a residential and enterprise customer without access point. Also, digital subscriber line (DSL) technologies are already deployed to dense residential area, for example apartment complex, without access points. WLAN service can be provided by attached access point at the end of the metro Ethernet and xDSL modem which has embedded IEEE 802.11b protocol stacks.



(Figure 1) Access network architecture for large scale deployment of WLAN

xDSL Architecture with Wireless LAN

An xDSL stands for various kinds of DSL technologies including asymmetric DSL (ADSL), high-speed DSL (HDSL), very high-speed DSL (VDSL) and so on [20]. Basic rate access DSL, just DSL, is 160 Kbps one-pair full-duplex for data service to provide access to the Integrated Services Digital Network (ISDN). HDSL is subscriber line technology for 1.544 Mbps or 2.048 Mbps two-pair full duplex system using 2B1Q coding and echo cancellation with 0.5mm twisted pair up to 4Km. ADSL system is a subscriber line technology to transmit downstream and upstream data rates up to 6.8 Mbps and 64 Kbps, respectively, within a radius of approximately 5.4Km without repeater. VDSL is used with fiber to the curb and uses between optical network units and customer premises. Its data rate is from approximately 58 Mbps to 13 Mbps within a 300m and 1.5Km, respectively.

The architecture of the DSLAM may determine the entire design of the ADSL network. Some DSLAMs handle only asynchronous transfer mode (ATM) over ADSL; others support a variety of DSLs with both ATM and frame-based transport. The protocol stack for link layer over xDSL depends on the customer premises configuration. The following protocols are possible: integrated network interface card for G.992.2, single user via bridging such as 10BaseT, universal serial bus, ATM25 and multiple users via routing such as 10 Base T, IEEE 1394.

Several premises architectures are possible. First, it is based on broadband media access protocol. Second, point-to-point protocol (PPP) over Ethernet (PPPOE) specify in ADSL Forum. Third, frame-based UNI (FUNI) over Ethernet specify in ATM Forum. Finally, layer 2 tunneling protocol (L2TP) is an [25].

PPPOE assumes an IEEE 802.3/Ethernet interface with no ATM stack in the PC. It is the widely used model in Korea.

In case of ATM over ADSL, users are connected to a network service provider via virtual circuits. Three ATM protocol stacks for ATM over ADSL are possible: RFC 1483 encapsulation/bridging, PPP over ATM and native ATM.

The advantages of ADSL are both service provider and users as following due to solve two problems simultaneously. First, it provides more bandwidth to end users: both residential and small- to medium-size business. This is increasingly important for Internet access, remote access to corporate servers and transparent LAN interconnection. Second, it enables service provider to offer value-added, high-speed networking services, without massive investment, by leveraging the copper loop.

In the xDSL architecture, service provider can provide WLAN service with access point based on [4] specification to public users. The interface between access point and xDSL modem prefer Ethernet to ATM.

Metro Ethernet Architecture with Wireless LAN

An Ethernet service is that customer equipment attaches to the network at the user-network interface using a standard 10Mbps, 100Mbps, 1Gbps or 10Gbps Ethernet interface. The metro Ethernet is an Ethernet-based metropolitan area network.

The metropolitan area networks comprise last big unreconstructed part of service provider. In the network architecture point, metro network lies between enterprise LAN and carrier WAN and plays a crucial role in carriers' abilities to provide the services enterprises want. Many infrastructure vendors are scrambling to promote a raft of new technologies as solutions to the carriers' problems and to their enterprise customers' needs.

Though advanced networking technologies such as SNA, Ring Net, ATM, FDDI and Ethernet are emerged, the major data networks of the customer are Ethernet [21] that means Ethernet series including fast Ethernet, gigabit Ethernet and 10 gigabit Ethernet. The metro Ethernet is an expansion of Ethernet from local area network to metropolitan area network by combination of Ethernet technology as a link layer and uses optics which transports frames without any transformation of protocol and frame. The protocol layering is Ethernet over dark fiber model which covers up to 150km in case of gigabit Ethernet and 40km at 10 gigabit Ethernet. The metro Ethernet constructs either gigabit switch or gigabit router with ring or star topologies.

The advantages of metro Ethernet for large scale deployment can be considered as following. First, metro Ethernet can be

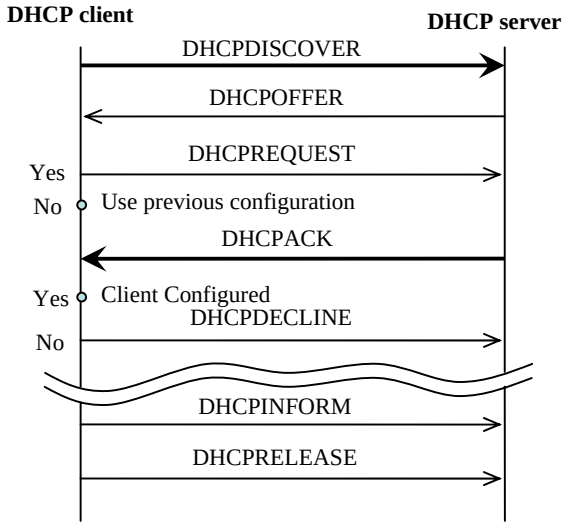
internetworking with synchronous optical network (SONET) to utilize existing network equipment and configure native Ethernet in case of new network. Second, metro Ethernet can easily configure the network without high cost router or transmission facilities. Third, metro Ethernet can share the bandwidth due to packet technology and reduce cost per bandwidth compared to SONET. Therefore, it can improve network operation because the network is simple.
In the metro Ethernet architecture, service provider can provide WLAN service with access point based on [4] specification to public users.

Leased Line with Wireless LAN
A leased line is a dedicated private connection to the Internet that is for a direct connection between the two locations. It provides a fast link to the Internet and ensures uninterrupted, private voice and data transfer.
The advantages of leased line are guaranteed service, bandwidth on demand, security, service level agreement and so on. However, leased line is not suitable for public WLAN because of its private purpose.

3. INTERNET ACCESS WITH ACCESS POINT

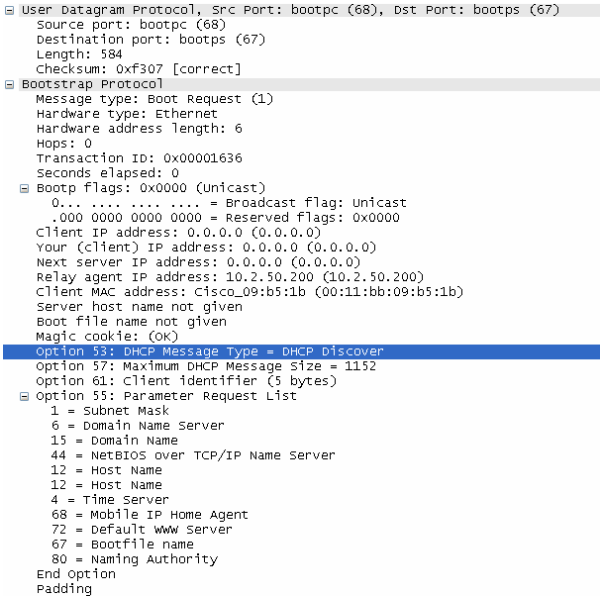
Access Point for WLAN
Access point can be divided into two categories: good and rogue access point. Good access points provide Internet access to the user who has a network adapter equipped wireless nodes. The wireless node requires network information to access the Internet via access point. The network information is: IP address, network mask that divides bits for network and host, default route and IP address of domain name system (DNS) server.
There are two methods to get the network information: manual and automatic. Users have to set up the network information by hand to their wireless node. However, it is difficult to the user who does not know all network information. Moreover, the network information is different place to place where the access point installed. Therefore, service providers are usually deployed with automatic network configuration by dynamic host configuration protocol (DHCP) [5].
The DHCP provides a framework for passing configuration information to wireless node via access point. DHCP is based on the BOOTP protocol, adding the capability of automatic allocation of reusable network addresses and additional configuration options such as network mask, default route and IP address of DNS server. The identical information in a single coverage of access point is IP address, network mask and default route. This information changes in accordance with location of the access point as described in network architecture at section 2. The IP address of DNS server can use whether the access point is changed or not.
Rogue access point can not provide Internet access service. When someone installs rogue access point without any permission of network provider with provider's SSID, public users can not access the Internet.
Network provider has to find rogue access point and resolve the problem as soon as possible. However access points are installed from hundreds of access point to millions of access point depend on a service area called hot spot such as hotels, airports, railway stations, bus terminals, campus, and so on. Also, it difficult to detect a rogue access point under the public service environment. It is an important issue that how to detect rogue access point to service providers. To resolve this problem, network operator patrols service areas of wireless LAN to detect rogue access points.

Configuration for Network Information
DHCP is one of the basic requirements for good access point to provide Internet access. To do this, access point should support either DHCP server function or DHCP relay function to the wireless nodes.
DHCP server can be located in the network. The access point should reach to DHCP server through the network. The wireless node can get network information from the DHCP via access point. We can consider centralized DHCP server or distributed DHCP server. DHCP server configuration depends on the policy of the provider, network architecture of access and backbone. Also, it takes into consideration on the operation and maintenance capability of the provider.
Wireless node should support DHCP client functions.



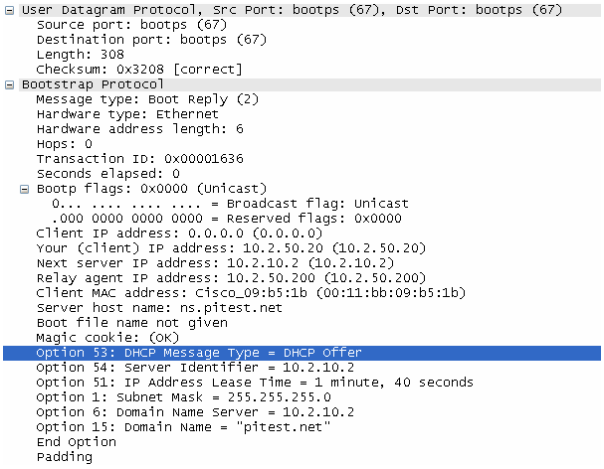
(Figure 2) DHCP client and server interaction

Figure 2 shows operational procedures to get the network information [22]. The client broadcasts the DHCPDISCOVER message to solicit offers from all reachable DHCP servers on the network.
The DHCPDISCOVER message is used when the client is configuring its interface using DHCP for the first time, or when it is has been unable to reuse a previously assigned address.
The client broadcasts the DHCPDISCOVER message as shown in Figure 3. i.e., source IP address and destination IP address is 0.0.0.0 and 255.255.255.255, respectively. It is to solicit offers from all reachable DHCP servers on the network.
The DHCPDISCOVER message may include options [23]. It is mandatory parameters such as subnet mask (option 1), router (option 3) and domain name server (option 6) among the option. The others are required for their purposes such as initial www server (option72), time server (option 4) and so on.
A server sends the DHCPOFFER message in response to the DHCPDISCOVER message from the client as shown in Figure 4. If the server has no suitable IP address available, it will not respond to the client's request. The IP address, mask, domain name, lease intervals, and other options are contained in the DHCPOFFER message. DHCP servers may temporarily reserve any offered IP addresses, so they will not be offered to several DHCP clients at the same time.



(Figure 3) Example of DHCPDISCOVER message

The servers may record the address as offered to the client to prevent the same address being offered to other clients in the event of further DHCPDISCOVER messages being received before the client has completed its configuration. The source and destination IP addresses of the DHCPOFFER message in the IP packet header are IP address of the DHCP server and 255.255.255.255, respectively. Even if the optional messages are requested from DHCPDISCOVER, the optional messages may not delivered by DHCPOFFER. When the DHCP server does not have requested optional information, server can not respond.

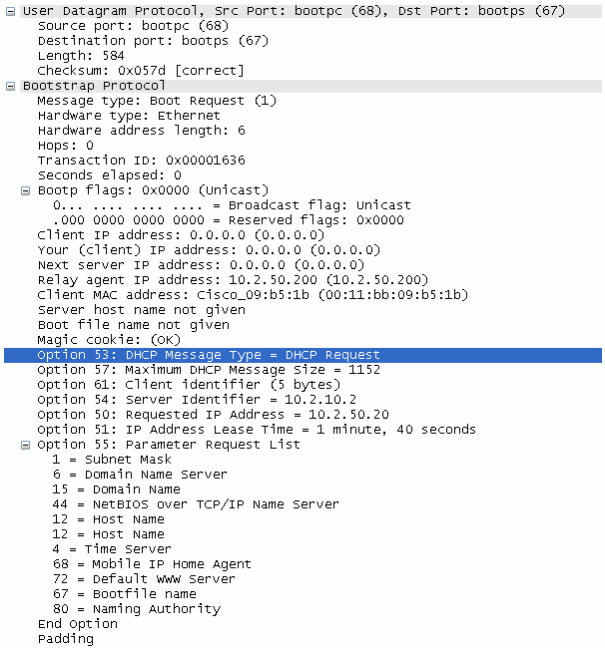


(Figure 4) Example of DHCPOFFER message

The client receives DHCPOFFER messages from multiple servers. The server identifier is the IP address of the DHCP server whose offer is being accepted. The DHCPREQUEST message is sent as a broadcast packet. All servers that had sent an offer receive the message. A client accepts parameters from one server and rejects other offers with a DHCPREQUEST message. The client chooses one based on the configuration parameters offered and broadcasts a DHCPREQUEST message as shown in Figure 5.

The DHCPREQUEST message includes the server identifier option to indicate which message it has selected and the requested IP address option, taken from your IP address in the selected offer. The client identifier may use MAC address of the network interface. The essential requested parameters are subnet mask, router and domain name server in the DHCPREQUEST message.

When the client receives no DHCPOFFER message, the client may reuse previous configuration until the lease expires, if its release is valid.



(Figure 5) Example of DHCPREQUEST message

The servers receive the DHCPREQUEST broadcast from the client. Those servers not selected by the DHCPREQUEST message use the message as notification that the client has declined that server's offer. The server selected in the DHCPREQUEST message commits the binding for the client to persistent storage and responds with a DHCPACK message as shown in Figure 6.

The DHCPACK message contains the configuration parameters for the client. The combination of client MAC address and your (client) IP address constitute a unique identifier for the client's lease. This identifier is used by both client and server to identify a lease referred to in any DHCP messages. The your IP address field in the DHCPACK messages is configured to client's network address.

The client receives the DHCPACK message with configuration parameters. The client checks on the parameters, for example with ARP for allocated network address, duration of the lease and the lease identification cookie specified in the DHCPACK message. At this point, the client is configured.

If the client detects a problem with the parameters in the DHCPACK message for example, the address is already in use on the network, the client sends a DHCPDECLINE message to the server and restarts the configuration process. The client should wait a minimum of ten seconds before restarting the configuration process to avoid excessive network traffic to prevent from looping. On receipt of a DHCPDECLINE, the

server must mark the offered address as unavailable and inform the system administrator that there is a configuration problem.
If the client receives a DHCPNAK message, the client restarts the configuration process.

```
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
    Source port: bootps (67)
    Destination port: bootps (67)
    Length: 308
    Checksum: 0x2f08 [correct]
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00001636
    Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 10.2.50.20 (10.2.50.20)
    Next server IP address: 10.2.10.2 (10.2.10.2)
    Relay agent IP address: 10.2.50.200 (10.2.50.200)
    Client MAC address: Cisco_09:b5:1b (00:11:bb:09:b5:1b)
    Server host name: ns.pitest.net
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP ACK
    Option 54: Server Identifier = 10.2.10.2
    Option 51: IP Address Lease Time = 1 minute, 40 seconds
    Option 1: Subnet Mask = 255.255.255.0
    Option 6: Domain Name Server = 10.2.10.2
    Option 15: Domain Name = "pitest.net"
    End Option
    Padding
```

(Figure 6) Example of DHCPACK message

A client that has already configured network information may use DHCPINFORM message as shown Figure 7 to request additional configuration parameters from the DHCP server.

```
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 308
    Checksum: 0x3a94 [correct]
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0f89c93a
    Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 211.48.1.212 (211.48.1.212)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: AsustekC_5b:2c:08 (00:13:d4:5b:2c:08)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Inform
  Option 61: Client identifier
      Hardware type: Ethernet
      Client MAC address: AsustekC_5b:2c:08 (00:13:d4:5b:2c:08)
    Option 12: Host Name = "your-9ea8c53aff"
    Option 60: Vendor class identifier = "MSFT 5.0"
  Option 55: Parameter Request List
      1 = Subnet Mask
      15 = Domain Name
      3 = Router
      6 = Domain Name Server
      44 = NetBIOS over TCP/IP Name Server
      46 = NetBIOS over TCP/IP Node Type
      47 = NetBIOS over TCP/IP Scope
      31 = Perform Router Discover
      33 = Static Route
      249 = Classless static routes
      43 = Vendor-Specific Information
      252 = Proxy autodiscovery
    End Option
    Padding
```

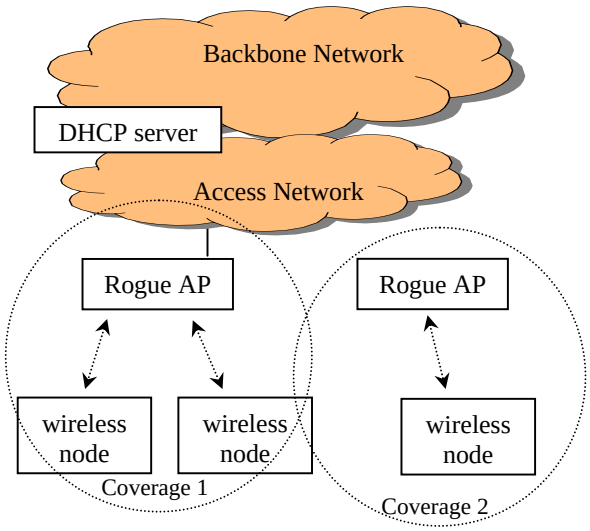
(Figure 7) Example of DHCPINFORM message

The DHCPRELEASE message is used by clients to cancel their lease as shown in Figure 8. When the clients are ending a session, the rest of the leased time (option 51) is not zero. The server can manage IP address pools efficiently, if the clients send DHCPRELEASE message when it shutdown communication session. However, most clients do not send DHCPRELEASE message during a shutdown so that they may attempt to use the same IP address when they are rebooted.
The 4 message exchanges are inefficient in some conditions that one DHCP server operates or mobile environments. The DHCP rapid commit [24] are used. It uses DHCPDISCOVER and DHCPACK messages instead of DHCPDISCOVER, DHCPOFFER, DHCPREQUEST and DHCPACK. The thick arrows indicate rapid commit in Figure 2.

```
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 308
    Checksum: 0x2a87 [correct]
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xb19a617d
    Seconds elapsed: 1280
  Bootp flags: 0x8000 (Broadcast)
      1... .... .... .... = Broadcast flag: Broadcast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 222.106.137.242 (222.106.137.242)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Ipone_50:29:19 (00:07:13:50:29:19)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Release
    Option 54: Server Identifier = 222.106.137.129
  Option 61: Client identifier
      Hardware type: Ethernet
      Client MAC address: Ipone_50:29:19 (00:07:13:50:29:19)
    End Option
    Padding
```

(Figure 8) Example of DHCPRELEASE message

Classification of Rogue Access Point
A rogue access point can not provide Internet access to the wireless node. It can be classified by three types of rogue access point according to the problem to access Internet as shown in figure 9. A circle shows radio coverage of access point. Wireless node communicates each other or accesses to the Internet through access point in the coverage.



(Figure 9) Classification of Rogue Access Point

In type I, rogue access point can provide Internet access to wireless, but it gives network operators the serious problem such as exposure of the network information to the attackers. The network information can be divided in to user and service provider aspects.
There are user's aspect information such as IP address of the mobile node, network mask, IP address of DNS and default route. This information is essential to provide Internet access.
The provider's information is also important including network security policy, location of the access point and so on. The

wireless LAN service provider maintains access points and its location including simple network management protocol (SNMP) community. If the network provider does not manage SNMP community of the access points, attackers can acquire information by SNMP. These kinds of rogue access points can be a source of denial of service attack or change configuration by SNMP.

In type II, rogue access point can not provide Internet access within its radio coverage due to failure connecting DHCP server or no route to forward packets. With this access point at coverage 1 in Figure 9, it is impossible to configure network parameters such as IP address, mask, DNS server and default router. However user can communicate each other in the coverage and its wired sub-network which has the same network mask.

In type III, rogue access point runs completely ad hoc network mode as depicted coverage 2 in Figure 9. These access points can not use in public service because of its no route to Internet.

Table 1 summarizes the types of rogue access point and its characteristics.

<Table 1> Types of Rogue Access Point

Functions	Rogue Access Point		
	Type I	Type II	Type III
DHCP support	Yes	Yes/No	No
Default route	Yes	No	No
AP's IP address	Yes	yes	No
Operation problem	Yes	yes	Yes

4. DETECTION FOR ROGUE ACCESS POINT

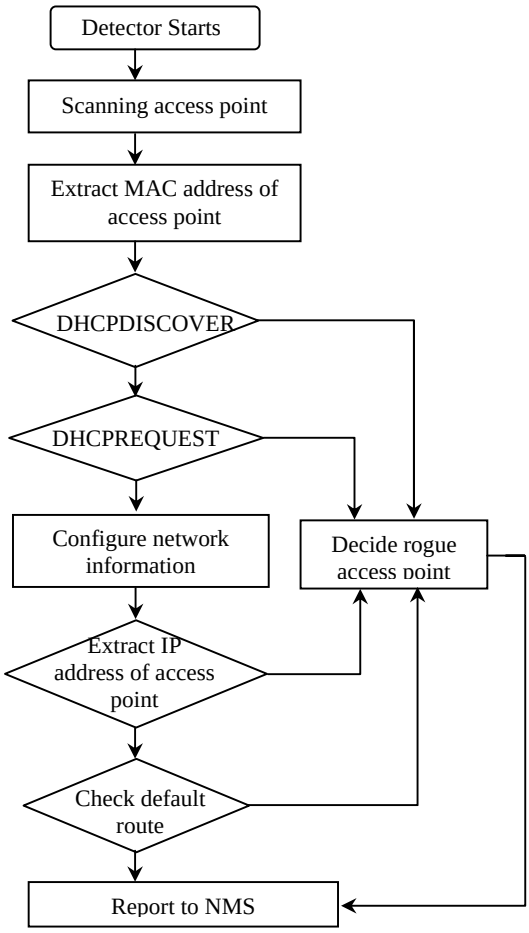
Detection Algorithm

It is important to operate and maintain without any rogue access point. For the purpose of secure and stable operation, provider has to detect rogue access point and can remove it to protect network resources.

We propose rogue access point detection scheme as shown in Figure 10. A tool is turned on searching any kinds of access points around the access point detector. There are two methods to find an access point called scanning: passive and active scanning [6]. In passive scanning the detector listens to beacons in each channel. A beacon messages consist of timestamp, beacon interval, capability information, service set identifier (SSID), supported rate, frequency hopping parameter set, direct sequence parameter set, IBSS parameter set, traffic indication message (TIM) and so on. This beacon messages are sent for networks with a several channels by beacon intervals. Active scanning is a faster process. In this scheme the detector sends a probe into each channel and waits for a response. A probe request message includes SSID, supported rate and a probe response message has a same message as beacon except for TIM information.

When the detector finds access point successfully, it extracts media access control (MAC) address from SSID of beacon or probe response messages. After that the detector tries to acquire IP address for its interface with DHCP protocol. The detector sends DHCPDISCOVER message to configure network between the detector and new access point. In this phase the detector can not configure network through type II or III rogue access point because the detector can not reach to DHCP server. The detector can get network information via good access point or type I rogue access point.

If the detector is in the coverage of type II or III rogue access point, detector starts to identify the problems. For this, detector sends reverse address resolution protocol (RARP) [7] request message to get IP address of the rogue access point. The RARP request message includes hardware type, protocol type, hardware address length, protocol address length and so on. The type II rogue access point has an IP address. However, it can not access to DHCP server because of network instability or no default routing table and other problems. Therefore detector can receive response message from type II rogue access point but can not receive any response from type III. The detector saves above information to report to network management system when it moves to other area where the Internet can access.



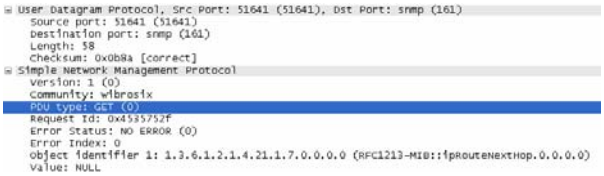
(Figure 10) Detection scheme for rogue access point

The type II rogue access point can be classified into problem based on whether the access point has default route information or not. When the rogue access point supports DHCP server, the detector can configure network information such as IP address, network mask, IP address of DNS server and default route. However, the rogue access point can not provide the default route and DNS server information to the detector.

If the access point performs DHCP relay and can not reach to the DHCP server, the detector can not configure network information.

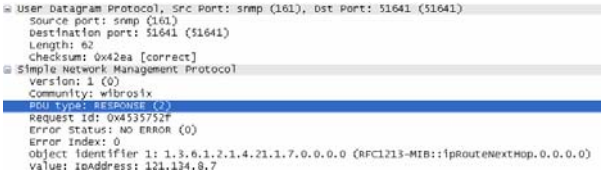
The detector decides a problem based on DHCP operation, default route and DNS information. The detector can sends SNMPGET message [8] to check default route as shown in

Figure 11. The SNMPGET message includes “ipRouteNext Hop.0.0.0.0” [9] which is object identifier for default route information.



(Figure 11) Example of SNMPGET message

If detector receives SNMPRESPONSE message as shown in Figure 12 via type II rogue access points, the rogue access point has default route information. The detector can check to default route with this information by “ping” command. Otherwise, type II rogue access points do not have default route information for DHCP server and Internet access.



(Figure 12) Example of SNMPRESPONSE message

When the detector configures network information through the access point, these kinds of access points are good or type I rogue access point. The SNMP can be used once again to decide good or rogue access point. The detector sends arbitrary object identifier for SNMP with publicly known community. If the detector receives response message from the access point, this access point is open to attackers. Service providers usually manage SNMP communities to prevent their resource from intruders or attackers. Therefore, it means that SNMP communities are not managed when it receives SNMP response with default community.

The operator with a detector moves everywhere to find rogue access point and can detect a large number of access points: good and rogue access point. The access points are important resource to provide public wireless service of service provider. To manage this resource, collected information from detector will be used in the NMS. For that purpose, the detector saves all information and reports to the NMS. This information includes time and date, location, and detailed access point types based on this proposed scheme.

Performance Analysis

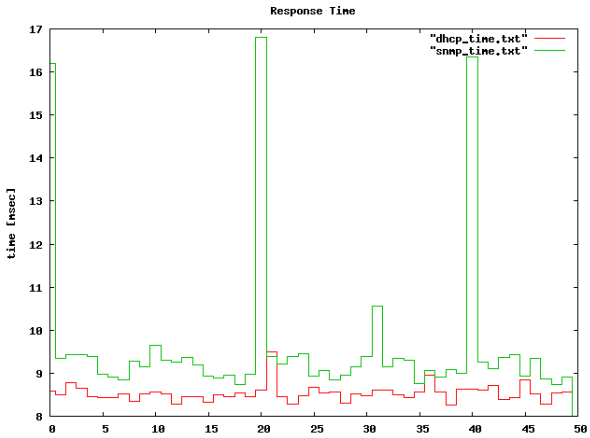
One of the main performance metric of the detector is overall detection time of the rogue access point. The detection time depends on detection scheme. i.e., scan time, DHCP response time and SNMP response time.

The scan time begins with channel sensing by either sensing a carrier signal in the wireless medium or checking the network allocation vector (NAV). The network allocation vector set by the station on detecting a short packet exchange between the intended transmitter and receiver.

A DHCP and SNMP response time can be variable in accordance with network environments. We measure the response time under the real environments. The DHCP and SNMP messages exchanged between the node and the network. Figure 13 shows the results of the measurements. We measure 50 times to acquire accurate data collection. The DHCP response time varies from 8.2 msec to 9.5 msec. The SNMP response time varies from 8.7 msec to 16.8 msec. The variation of the response time for SNMP is larger than its DHCP. It can be considered that load of the SNMP manager influences SNMP response.

The detector can be decided rogue access point within the T_{detect}. Where, $T_{detect} = NAV_{max} + T_{dhcp\_max} + T_{snmp\_max}$.

NAV_{max} is a maximum carrier scan time. T_{dhcp_max} is a maximum DHCP response time and T_{snmp_max} is a maximum SNMP response time, respectively. In our case, T_{dhcp_max} value is 9.5 msec and T_{snmp_max} value is 16.8 msec.



(Figure 13) Response Time for Detector

5. CONCLUSION

It is important to detect rogue access point in the wireless LAN environment that is for public service. This paper proposes access network architecture for large scale deployment of wireless LAN for the purpose of public service. A metro Ethernet and xDSL access network [19] can be used for wireless LAN with access point.

We propose the rogue access point classification based on the problem to connect Internet and detection scheme of rogue access point. The rogue access point detector can be used by service provider for operation and maintenance.

The detector stores collected data to report NMS. It will be ultimately contribute to the network provider to enhance to Internet availability. A network operator can easily find out rogue access point and resolve the problem by walk around with the detector.

6. REFERENCES

[1] Stallings, W., “IEEE 802.11: moving closer to practical wireless LANs”, **IT Professional**, Vol. 3, no. 3, May-June 2001, pp. 17 – 23

[2] Henry, P.S., Hui Luo, “WiFi: what's next?”, **IEEE Communications Magazine**, Vol. 40, No. 12, December 2002, pp. 66 – 72

[3] Boo-Sun Jeon, Eun-Jin Ko, Gil-Haeng Lee, “Network management system for wireless LAN service”**, 10th International Conference on Telecommunications,** Vol. 2 , 23 Feb.-1 March 2003, pp.948 - 953

[4] IEEE Std. 802.11b-1999, **"Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications: Higher-speed Physical Layer Extension In The 2.4 GHz Band"**, IEEE, Sep. 1999
[5] T. Lemon, S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", **RFC 3396**, November 2002
[6] Neeli Prasad, Anand Prasad, "**WLAN Systems & Wireless IP for Next Generation Communications**", Artech House, January 2002
[7] Ross Finlayson, Timothy Mann, Jeffrey Mogul, Marvin Theimer, "A Reverse Address Resolution Protocol", **RFC 903**, June 1984
[8] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol (SNMP)", **RFC 1157**, May 1990
[9] K. McCloghrie, M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", **RFC 1213**, March 1991
[10] IEEE Std. 802.11-1997, "Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications", IEEE Press, June. 1997
[11] Brian P. Crow, Indra Widjaja, Jeong Geun Kim, Prescott T. Sakai, "IEEE 802.11 Wireless Local Area Networks", **IEEE Communications Magazine**, Vol. 35, no. 9, Sep 1997, pp. 116-126
[12] Juha Ala-Laurila, Jouni Mikkonen, and Jyri Rinnemaa, "Wireless LAN access network architecture for mobile operators", **IEEE Communications Magazine**, Vol. 39, No. 11, November 2001 pp.82 - 89
[13] Bala Rajagopalan, Dimitrios Pendarakis, Debanjan Saha, Ramu S. Ramamoorthy, Krishna Bala, "IP over optical networks: architectural aspects", **IEEE** Communications Magazine, Vol. 38, no 9, September 2000, pp.94 – 102
[14] Stefano Baroni, M. Alber Qureshi, Antonio Rodriguez-Moral and David Sugerman, "Backbone network architectures for IP optical networking", **Optical Fiber Communication Conference**, Vol. 1 , 7-10 March 2000 pp.159 - 161
[15] Koichi Asatani, Yoichi Maeda, "Access network architectural issues for future telecommunication networks", **IEEE Communications Magazine**, Vol. 36, no 8, August 1998, pp.10 - 114
[16] Nicholas Madamopoulos, mark D. Vaughn, Leo Nederlof and R. E. Wagner, "Metro network architecture scenarios, equipment requirements and implications for carriers", **Optical Fiber Communication Conference and Exhibit**, 2001, Vol. 3, pp.WL2-1 - WL2-3
[17] Guen-Bum Kwon, Boo-Young Chung, "Access network architecture and economics for Internet", International Conference on Communication Technology Proceedings, 1998. **ICCT '98**, Vol. 2, pp. S46-10-1 – S46-10-5
[18] Frank Brockners, Norman Finn and Steve Phillips, "Metro ethernet - deploying the extended campus using ethernet technology", Proceedings. **28th Annual IEEE International Conference on Local Computer Networks**, 20-24 Oct. 2003, pp.594 – 604
[19] Yong-Kyung Lee and Dongmyun Lee, "Broadband Access in Korea: Experience and Future perspective" , **IEEE Communication Magazine**, Vol. 41, No. 12 December 2003, pp.30 – 36
[20] John A. C. Bingham, **ADSL, VDSL and Multicarrier Modulation**, John Wiley and Sons, Inc. 2000, pp1 – 19
[21] IEEE Std. 802.3-2002, **"Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications",** IEEE, March 2002
[22] R. Droms, "Dynamic Host Configuration Protocol", **RFC 2131**, March 1997
[23] BOOTP AND DHCP PARAMETERS, http://www.iana.org/assignments/bootp-dhcp-parameters
[24] S. Park, P. Kim and B. Volz, "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)" **RFC 4039**, March 2005
[25] W. Townsley, et al. "Layer Two Tunneling Protocol "L2TP"", **RFC 2661**, August 1999