Enabling Location-Based Services on Wireless LANs

Yen-Cheng Chen, Yao-Jung Chan, and Cheung-Wo She
Department of Information Management
National Chi Nan University
Puli, 545 Nantou, Taiwan
ycchen@ncnu.edu.tw

***Abstract*- The wide deployment of IEEE 802.11 Wireless Local Area Networks (WLANs) has made possible the development of application services on WLANs. Due to the small cell size in WLANs, it is practical to develop location dependent services based upon the awareness of the WLAN access points (AP) that mobile devices currently access. In this paper, we propose a location determination technique using the inherent SNMP support in WLAN APs. It is shown that the location of a mobile device can be determined effectively from the SNMP traps sent by APs. Our SNMP-based approach doesn't need any particular software or hardware in mobile devices. This paper also considers how to determine the location of a mobile device by its IP address. In general, only the IP address of a mobile device can be seen by location-based services. However, APs identify each mobile device by its MAC address. Hence, we propose effective techniques for the mappings between IP addresses and MAC addresses. Through the address mappings, the location of a mobile device can be determined by its current IP address. We further propose a web service framework to enable WLAN location-based services in WWW environments. To verify our approach, we also develop a location-based campus map service based on the web service framework.**

I. Introduction

IEEE 802.11 [1] wireless local area networks (WLANs) have been successfully deployed in corporate networks and campus networks. Recently, Internet service providers (ISPs) start to provide Internet wireless access services by installing WLAN access points (APs) in public hotspot areas, such as airports, coffee shops, and conference centers. Therefore, as in cellular telecommunication systems, there is an increasing demand for location-based services on WLANs. That is, any IEEE 802.11-enabled mobile device can obtain location dependent information based on its current location within a WLAN. Currently, there are no standard solutions for location management in IEEE 802.11 WLAN infrastructures. Therefore, to provide location-based services on WLANs, we need to develop an effective technique for determining the location of any mobile device.

In indoor environments, the coverage area of a typical IEEE 802.11 AP is usually small, compared with the size of cells in cellular telecommunication systems. Therefore, if we can identify the AP that a mobile device accesses currently, we can determine that the mobile device is in the neighborhood of the AP. Hence, it is practical to provide location dependent information to the mobile device based on the location of the AP. In this paper, we will show that the inherent Simple Network Management Protocol (SNMP) [2] supported in each AP can be used to determine which AP a mobile device is currently connected to. As known, most WLAN APs support SNMP for network management purposes. In an IEEE 802.11 WLAN, when a mobile device attempts to access the network, the device will first make an association with its nearest AP. For effective management of association services, many APs are capable of sending association notifications to their network manager via SNMP traps. That is, whenever a mobile device successfully makes an association with an AP, the AP will immediately send an SNMP association trap to notify its management station. Similarly, the re-associations and disassociations between mobile devices and APs will also trigger the transmissions of re-association traps and disassociation traps, respectively. By receiving the SNMP traps sent from APs, we can know which mobile device is entering or leaving the coverage area of an AP. As a result, the approximate location of a mobile device can be determined as soon as its migration to the coverage area of an AP. In this paper, we will develop an effective location determination technique by means of the SNMP supported in APs. By our approach, no any particular hardware and software is required in mobile devices. In the wired network, only a location server is needed to receive SNMP traps from APs and to perform location determinations. Since SNMP traps are sent immediately after associations are made, we will show that location determination via SNMP traps can achieve shorter response time and higher accuracy than previous approaches.

Many Internet application services are designed to be web-based. This paper also aims to enable WLAN location-based services in WWW environments. If a location-based service can be implemented as a web application, the web browser in a mobile device will be the only required software to access location dependent information Previous location determination approaches use particular hardware or software in mobile devices to perform location detection. These approaches were not appropriate for use in WWW environments. Since we assume that the web browser is the only software used in a mobile client, what we can use for location determination will be only the IP address of the mobile device, which can be retrieved from HTTP requests. Although Java applets can be embedded in most web browsers, it is not allowed to retrieve the MAC address or other identification information of the mobile client via Java applets due to security and privacy concern. On the other hand, most APs use MAC addresses to identify mobile devices. Therefore, as we obtain the IP address of a mobile device, we still need to get the MAC address corresponding to the IP address. To support location-based services in WWW environments, our location determination approach will also involve the mapping between IP addresses and MAC addresses. Accordingly, by our location determination approach, location-based services can use the IP address of a mobile device to determine its current location. To further facilitate the development of location-based services in WWW environments, we will propose a generalized web service framework for location-based services on WLANs.

The remainder of this paper is organized as follows. Section II is a review of previous location determination techniques on IEEE 802.11 WLANs. In section III, we will describe our location determination approach based on the SNMP protocol. In section IV, we will present a web service framework for WLAN location-based services in WWW environments. Section V describes an implementation of a location-based campus map service based on the web service framework. Finally, the conclusion and future work are given in section VI.

II. Related Work

Location determination techniques for cellular systems have been developed in recent years. The interested reader may refer to [3] for details. In addition, there are a number of location sensing systems that require particular sensor hardware such as radio frequency (RF) and GPS components. A comprehensive survey of such location systems can be found in [4]. In this section, we focus on previous work that determines the location of a mobile device simply by the IEEE 802.11 WLAN infrastructure.

A. RSS-Based Approaches

Several previous studies [5]-[7] make use of the strengths of signals received by a mobile device to infer its current location. Triangulation [8] is the most common technology for those location determination approaches based on received signal strengths (RSSs). Theoretically, triangulation can be used to accurately determine the geographical location of a mobile device, if the distances between the mobile device and APs can be precisely estimated from the signal strengths. Unfortunately, probably due to obstructions and multipath fading effects in indoor environments, there is a considerable variation in the strengths of signals received by a mobile device at the same spatial point. Therefore, triangulation based on variable signal strengths may give inaccurate results. The deficiency can be possibly overcome by the use of a database of signal strength data, measured earlier in each possible location. Then, the location of a mobile user can be inferred by finding the most likely location whose corresponding signal strength data in the database best match received signal strengths. This kind of location determination technique is called RSS-based location fingerprinting [9]. To build the database of signal strengths, RSS-based location fingerprinting needs tedious measurements of signal strengths in the all coverage areas of WLANs. In addition, both triangulation and RSS-based location fingerprinting also require denser installation of APs to ensure that each location is within the converge areas of three APs. Both techniques also require additional software in each mobile device to collect signal strengths from different APs.

B. Network-Based Approaches

Unlike the previous RSS-based techniques, there are several approaches that determine the location of a mobile device by finding the AP that the mobile device is associated with. S.G.M. Koo et al. in [10] proposed a network-based approach, called the RADIUS approach, based on the use of a centralized RADIUS server. Remote Authentication Dial-In User Service (RADIUS) [11] is a service to provide centralized authentication, authorization, and accounting for network access. The RADIUS approach assumes that a RADIUS server is used for authenticating WLAN users. Each mobile device attempting to access the WLAN will send an authentication request to an AP. The AP then forwards the request to the RADIUS server. In case of a successful authentication, the time, the ID of the AP, and the MAC address of the mobile device will be recorded in the log file of the RADIUS server. By inspecting the log file, the RADIUS approach can determine which AP a mobile device is currently associated with. For performance considerations, it was recommended that location determination be implemented in the RADIUS server. Since the format of the RADIUS log file is not standardized, the log format may vary in different RADIUS servers. Therefore, the implementation of the RADIUS approach depends on the RADIUS server used.

Also in [10], an SNMP approach was proposed to provide a standard and platform-independent solution for location determination. In the SNMP approach, an SNMP polling program is used to periodically query each AP in a WLAN to obtain the MAC addresses observed by the AP. Essentially, APs are configured as transparent bridges. For forwarding frames, the MAC addresses listened by an AP will be stored in the forwarding table of the AP. In general, an MAC address can be stored in the forwarding table for 15 to 20 minutes even if the corresponding device has stopped an association with the AP. As a result, it is possible that the same MAC address may appear in several APs. This complicates the location determination process using the SNMP approach. In addition, the periodic polling by SNMP may consume considerable network resources and may result in longer response time than the RADIUS approach.

Both the RADIUS approach and the SNMP approach use the MAC addresses of mobile devices to perform location determination. As described previously, only the IP addresses of mobile devices can be obtained by the location-based services in WWW environments. Therefore, IP-to-MAC address mappings are required, in addition to the previous location determination approaches that, in fact, provide MAC-To-AP mappings. In [12], two approaches for the IP-to-MAC mapping were proposed: the DHCP approach and the SNMP approach. In the DHCP approach, the log of the DHCP server for a WLAN is used to provide address mappings. Whenever the DHCP successfully assigns an IP address to a mobile device, the IP address as well as the MAC address of the mobile device will be recorded in the log file. Therefore, IP-to-MAC mappings can be obtained by inspecting the log file. Since there is no standard format for the log file of a DHCP server, the DHCP approach also depends on a particular implementation of the DHCP server. One advantage of the DHCP approach is that the DHCP log can also provide MAC-to-IP mappings, which will be useful for instant messaging or paging applications on WLANs. In the SNMP approach, SNMP queries are sent to the default gateway of a mobile device to retrieve the cached MAC address corresponding to a given IP address. In the default gateway, the mappings of IP addresses and MAC addresses can be found in the Address Resolution Protocol (ARP) table, namely the *ipNetToMediaTable* in the standard MIB II [13]. The SNMP approach was applied in a single LAN or a set of Virtual LANs (VLANs). In case of VLANs, the default gateway of each VLAN should be known in advance for performing SNMP queries. Compared with the DHCP approach, the SNMP approach cannot provide MAC-to-IP address mappings.

III. A New SNMP Approach

Platform independence is an important factor to facilitate the wide use of location-based services on WLANs. Since RSS-based approaches for location determination require specialized software in mobile clients, they are platform dependent. Such specialized software is not needed in the RADIUS approach. However, the RADIUS approach can only be adopted in WLANs using RADIUS authentications. Furthermore, it is also platform dependent, since it should be integrated with a particular implementation of a RADIUS server. Among previous approaches, the SNMP approach is the most promised one to achieve platform independence. However, as described in the previous section, the periodic polling by SNMP may generate heavy signaling traffic and results in poor performance. In this section, we will propose an alternative solution for location determination based on the trap mechanism of SNMP. We will show that no any periodic polling is required if APs have the capability of sending SNMP traps to report the association related events in the APs.

A. SNMP Trap Approach

Before a mobile device is allowed to send data messages via an AP, the mobile device shall first become associated with the AP. This can be accomplished by the association service specified by IEEE 802.11. IEEE 802.11 also specifies the reassociation service and the disassociation service. The reassociation service is invoked to enable a current association to be transferred from one AP to another. The disassociation service is invoked whenever an existing association is to be terminated. IEEE 802.11 recommends that an SNMP trap should be sent when a disassociation occurs. For effective management of associations, many enterprise-level APs [14]-[17] will also send out SNMP traps after associations and reassociations take place. Thus, sending association-related traps is a common feature found in most APs. The information carried in an association-related trap includes the MAC address of the mobile device involved in an association-related service. The IP address of the AP sending the trap is also in the agent address field of an SNMP trap message. As a result, by interpreting the traps sent from all APs, we can determine which AP a mobile device is currently connected to or disconnected from. Fig. 1 illustrates our SNMP trap approach.

In the SNMP trap approach, only a location server is required in the wired network. The location server is responsible for receiving traps and performing location determinations. Each AP is configured so that all traps are sent to the location server. In the location server, a trap listener program runs as a daemon process to receive and handle incoming traps. The location server also contains a location database to store location information. In the location database, an AP table is used to store the information about each AP, including its identifier (ID), IP address, and a textual location description. The location database also contains an association table. A record in the association table consists of the MAC address of a mobile device and the ID of the AP that the mobile device is currently associated with. The association table is updated according to the types of traps received:

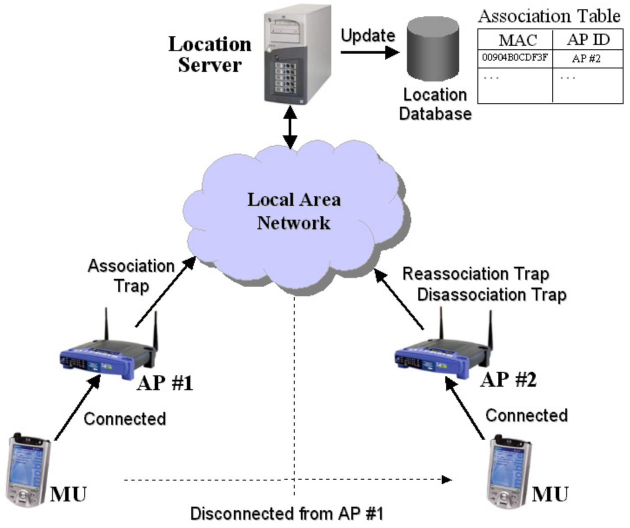


Fig. 1. The SNMP trap approach.

1) *Association Trap*: Insert a new record to store the MAC address of a mobile device and the ID of the AP that sent the trap.

2) *Reassociation Trap*: Update the AP ID field of the record that has an MAC address same as the one shown in the reassociation trap.

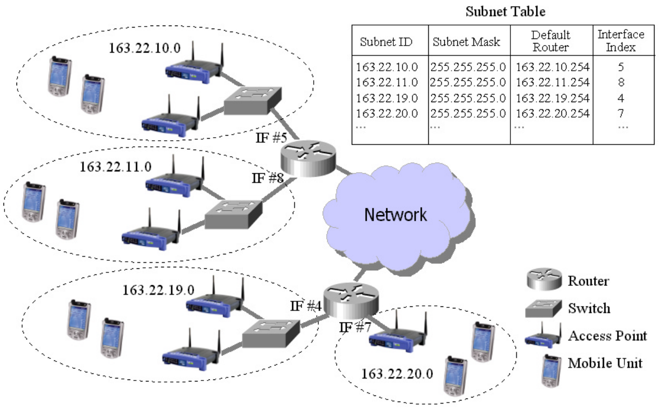
3) *Disassociation Trap*: Delete the record that has an MAC address same as the one shown in the disassociation trap.

By the above traps, we can effectively maintain MAC-to-AP mappings in the association table without introducing additional network traffic as incurred in the previous SNMP polling approach. Furthermore, unlike the use of ARP caches in previous approaches, the MAC-to-AP mappings derived from SNMP traps are always most up-to-date. Therefore, the location of a mobile device can be determined correctly.

B. Address Mappings

Essentially, WLAN APs are layer 2 devices. They identify each mobile device by its MAC address. However, location-based services are usually located at the application layer. In general, only the IP address of a mobile device can be seen by these services. Therefore, to enable location-based services at the application layer, we further need the mappings between MAC addresses and IP addresses. Before presenting our mapping methods, we first study how IP addresses are used in location-based services. In general, a location-based service can be pull-based or push-based. Location-based pull services provide services in an on-demand manner. Location-based web applications fall into this category. As a mobile device "pulls" a location-based service, the location-based service obtains the IP address of the mobile device and then determines the AP that the mobile client is currently associated with. Since MAC-to-AP mappings have been available in the association table, we further need IP-to-MAC mappings to finally obtain IP-to-AP mappings. On the other hand, location-based push services send location dependent information to a mobile device without any explicit request from the device. Instant messaging services are typical push-based services. When a location-based push service attempts to "push" a message to a mobile device, the location-based service must know the IP address currently used by the mobile device. We can obtain the MAC address of a mobile device from the association table. Therefore, we further need MAC-to-IP mappings to get the IP address of a mobile device. In summary, we conclude that IP-to-MAC and MAC-to-IP address mappings are necessary for location-based pull services and push services respectively. In the following, we will show how both mappings can be obtained via SNMP.

To support address mappings via SNMP, we first prepare a subnet table in the location database. The subnet table consists of four fields: Subnet ID, Subnet Mask, Default Router, and Interface Index. Each record in the subnet table corresponds to a subnet that could contain mobile devices. In general, when a mobile device accesses a network via an AP, the mobile device is in a subnet that also contains the AP. Therefore, the subnets containing APs will also be those ones that can contain mobile devices. By the AP table, we can know which APs are involved in the location-based services. Therefore, we can find the subnets from the APs. For each AP, we send an SNMP get-request to the AP to get its subnet mask, which will be stored in the Subnet Mask field of the subnet table. The subnet mask is available in the *ipAdEntNetMask* object of the *ipAddrTable* table, defined in MIB II. After the Subnet Mask is determined, the Subnet ID can be obtained by the bit-wised AND of the Subnet Mask and the IP address of the AP. The Default Router field indicates the default router of the mobile devices in a subnet. In fact, the default router of an AP is also the one of the mobile devices in the same subnet. For an AP, the IP address of its default router can be obtained in the *ipRouteTable* table of MIB II. In *ipRouteTable*, the entry with a value of 0.0.0.0 in the *ipRouteDest* object indicates a default route. The *ipRouteNextHop* object in the default route entry will be the IP address of the default router. The Interface Index field indicates the index number of a network interface in the default router. The network interface is used to connect to a subnet that can contain mobile devices. We can determine the index number of the network interface from the *ipAdEntIfIndex* object in the *ipAddrTable* table of MII II. Fig. 2 shows a typical WLAN configuration with its corresponding subnet table.



Subnet Table

Subnet ID	Subnet Mask	Default Router	Interface Index
163.22.10.0	255.255.255.0	163.22.10.254	5
163.22.11.0	255.255.255.0	163.22.11.254	8
163.22.19.0	255.255.255.0	163.22.19.254	4
163.22.20.0	255.255.255.0	163.22.20.254	7
…	…	…	…

Fig. 2. A WLAN configuration and its subnet table.

1) *IP-to-MAC Address Mapping*:

Given the IP address of a mobile device, we need to determine the MAC address of the mobile device. By using the subnet table, we obtain IP-to-MAC address mapping as follows. Firstly, we search the subnet table to find the subnet containing the given IP address. After the subnet is found, we identify the default router, whose ARP cache will contain the MAC address of the mobile device. The ARP table is corresponding to the *ipNetToMediaTable* table in MIB II. The *ipNetToMediaTable* table is indexed by interface index and IP address. Therefore, by using the *Interface Index* value in the subnet table and the known IP address as the instance identifier, we retrieve the *ipNetToMediaPhysAddress* object in the *ipNetToMediaTable* table. The returned value is the MAC address of the mobile device observed by the default router. In summary, the IP-to-MAC address mapping can be accomplished via a simple table lookup followed with a single SNMP query. Therefore, the IP-to-MAC address mappings can be performed efficiently.

2) *MAC-to-IP Address Mapping*:

Given the MAC address of a mobile device, we need to know the current IP address assigned to the device. Firstly, we determine the AP that the MAC address is associated with. This information is available in the association table. Using the IP address the AP, we search the subnet table to find the subnet that contains the AP. After the subnet is found, we identify the default router, whose ARP cache will contain the IP address of the mobile device. Note that the *ipNetToMediaTable* table is indexed by interface index and IP address. The interface index has been known from the subnet table. Obviously, the IP address is unknown. Therefore, we cannot determine the IP address of the mobile device in a single SNMP request. To avoid retrieving the entire *ipNetToMediaTable* table, we use *Interface Index* and the *Subnet ID* of the subnet table as the start instance identifier of SNMP queries. Then, we can quickly find the resulting IP address in a few SNMP get-next requests. As a result, only a very limited part of the *ipNetToMediaTable* should be retrieved. If SNMPv2 is supported in the router, the use of get-bulk requests can further reduce the SNMP traffic.

IV. A Web Service Framework for Location-Based Services on WLANs

Undoubtedly, web browsing is the most convenient way to access information in the Internet. Therefore, it will be popular to provide WLAN location-based services in WWW environments. That is, location-based services are deployed on web servers located in the wired network. Thus, a mobile device can obtain location dependent information through a web browser. In this section, we consider how the SNMP trap approach and address mappings by SNMP can be used together for location-based services in WWW environments.

To provide a standard way to develop location-based services in WWW environments, we propose a web service framework for location-based services on WLANs. The web service framework, as shown in Fig. 3, is composed by mobile units, WLAN APs with default routers, web servers, and a location server with a location database. Mobile units are those mobile devices that request location-based services through web browsers. The WLAN APs with their default routers together provide necessary management information for location determinations. Location-based services are located in web servers. The location server is the place where location determinations are performed. All location information is stored in the location database. To provide a standard way to access location information, we design a web service in the location server. The web service provides location query services using the Simple Object Access Protocol (SOAP) [18]. Web servers can obtain location information via SOAP messages.

SOAP is an XML-based protocol for exchange of information in web environments. The SOAP protocol between web servers and the location server is implemented over HTTP. In the proposed web service framework, two SOAP messages are defined. The *LocationRequest* SOAP message, sent from web servers, contains a single parameter *muIP* to carry the IP address of a mobile unit whose location is to be determined. The *LocationResponse* SOAP message, sent from the location server, is used to return the result of a previous location request. The *LocationResponse* SOAP message includes two parameters: *muIP* and *location*. The muIP parameter is the same as in the *LocationRequest* SOAP message. The *location* parameter indicates the current location of the mobile unit.

The interactions among the components of the web service framework are described in the following typical scenario, as illustrated in Fig. 3.

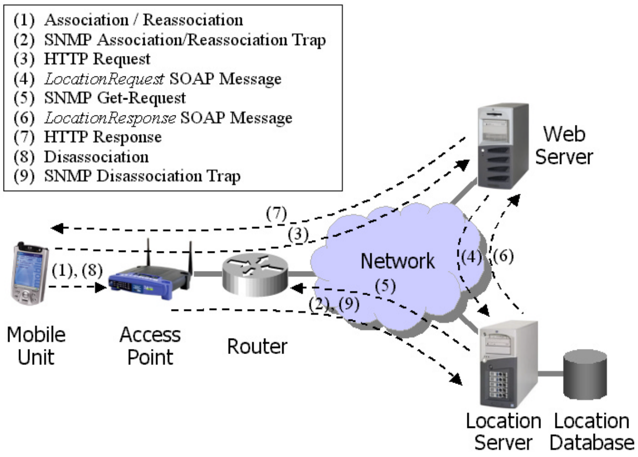


Fig. 3. A web service framework for WLAN location-based services.

1) A mobile unit makes an association (reassociation) with an AP.

2) After the association (reassociation) is made, the AP sends an SNMP association (reassociation) trap to the location server. The location server stores the MAC address of the mobile unit with the ID of the AP in the association table of the location database.

3) The mobile unit uses a web browser to access a location-based service in a web server. The request of a location-based service is sent via an HTTP request.

4) The web server extracts the IP address of the mobile unit from the HTTP request and then sends a *LocationRequest* SOAP message to the location server.

5) Upon receiving a *LocationRequest* SOAP message, the location server first refers to the subnet table in the location database to determine the default router of the mobile unit. Then, the location server sends an SNMP get-request to the default router to get the MAC address of the mobile unit.

6) After the MAC address of the mobile unit is obtained, the location server refers to the association table to determine the AP that the mobile unit is associated with. Then, the location server sends the determined location information to the web server via a *LocationResponse* SOAP message.

7) The web server obtains the location information from the received SOAP message and then prepares location dependent information for the mobile unit in a web page. The web page is then sent to the mobile unit via an HTTP response.

8) The mobile unit is disassociated from the AP.

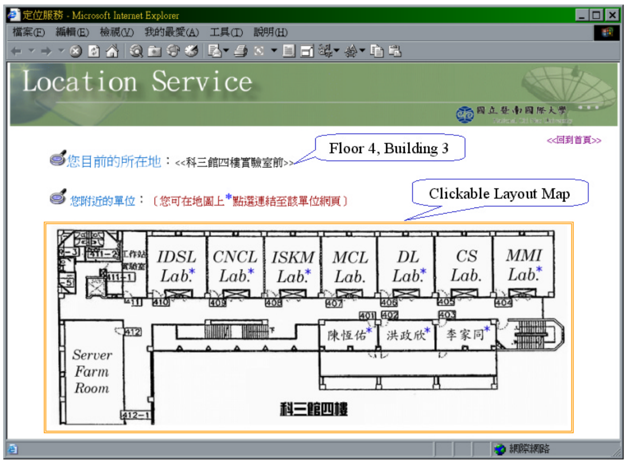
9) The AP sends an SNMP disassociation trap to the location server. The location server then deletes the record for the mobile unit in the association table.

The web service framework for WLAN location-based services doesn’ t need the support of additional services, such as RADIUS and DHCP servers in previous approaches. In addition, the framework provides a uniform approach for accessing location information by the use of a standard SOAP interface. Therefore, location-based services can be developed independently without considering the details of location determinations.

V. IMPLEMENTATION

In order to verify the proposed web service framework, we have implemented a location server in a university campus network to support location-based services on the WLAN of the campus. The WLAN is composed by fifteen 802.11b Cisco Aironet 350 APs [14]. Three routers are used to connect the APs. Since our location determination approach also involves the auto-discovery of default routers, in fact we don’ t need any knowledge of how those APs are connected to routers. For each AP, we specify a textual identification of a location in the AP’ s *sysLocation* object, which is defined in the *system* group of MIB II. The value of this object can be retrieved via SNMP for the identification of a location. In addition to the setting of the *sysLocation* object, we configure each AP so that all traps can be sent to the location server. The location server consists of an SNMP trap listener to receive traps and an HTTP server to receive location queries in SOAP messages. The location server stores location related information in the location database.

We have also developed a location-based campus map service on the WLAN. The location-based campus map service provides layout maps of the campus in web pages according to the current locations of mobile devices. When any mobile device uses a web browser to access the campus map service, the campus map service will obtain location information from the location server. Then, a web page containing the map image of the location is sent to the mobile unit. The map image is clickable to provide more information about the location. Fig. 4 shows a resulting web page. In the implementation, web pages can be shown correctly in less than 5 seconds. Since no any periodic SNMP polling is required, the location server performs well without a heavy processing load.



您目前的所在地：<<科三館四樓實驗室前>>

您附近的單位：（您可在地圖上*點選連結至該單位網頁）

Fig. 4. A location-based campus map service on the WLAN of a campus.

VI. Conclusion and Future Work

Previous studies [7], [10] indicated that the MAC addresses of mobile devices cached in APs might be invalid for location determinations. Instead of the use of the cache, we have proposed an effective approach based on the use of SNMP traps to obtain most up-to-date mappings of MAC addresses and APs. We have also proposed an effective approach for address mappings. Consequently, the location of a mobile device can be determined by its IP address. Hence, WLAN location-based services can be developed in WWW environments.

We have presented a practical web service framework for WLAN location-based services in WWW environments. Thus, location-based services can be developed in a standard way. Our future work is the study of location-based push services on WLANs. Location-based push services require an effective mechanism to monitor the movements of mobile devices. In fact, SNMP traps can also be used for the purpose. In addition, the MAC-to-IP address mapping method already proposed in this paper are essential for push services. We need to further study how SNMP traps and the MAC-to-IP address mapping can be used together for supporting location-based push services. A standard web service framework is to be developed for enabling location-based push services on WLANs.

References

[1] IEEE Computer Society LAN MAN Standards Committee, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11 1999. The Institute of Electrical and Electronics Engineers, 1999.

[2] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", RFC 1157, May 1990.

[3] "Location Technologies for GSM, GPRS and WCDMA Networks," White Paper, SnapTrack, A QUALCOMM Company, November 4, 2001.

[4] Jeffrey Hightower and Gaetano Borriello, "A Survey and Taxonomy of Location Systems for Ubiquitous Computing," Extended paper from Computer, 34(8) p57-66, August 2001.

[5] P. Bahl, V. N. Padmanabhan, "RADAR: An In –Building RF-Based User Location and Tracking System," in *Proc. IEEE INFOCOM* 2000, Vol. 2, pp. 775-784, March 2000.

[6] Paul Castro, Patrick Chiu, Ted Kremenek, and Richard Muntz. "A probabilistic location service for wireless network environments," in *Proc. Ubicomp* 2001, pp. 18-24., September 2001.

[7] Smailagic, A., Kogan, D. "Location Sensing and Privacy in a Context-Aware Computing Environment," *IEEE Wireless Communications*, vol. 9, no. 5, Oct 2002

[8] K. Pahlavan and P. Krishnamurthy, *Principles of Wireless Networks: A Unified Approach*, Prentice Hall PTR, 2002.

[9] P. Prasithsangaree, P. Krishnamurthy, and P. K. Chrysanthis. "On Indoor Position Location with Wireless LANs," in *Proc. the 13th IEEE Int'l Symposium on Personal, Indoor, and Mobile Radio Communications*, Lisbon, Portugal, Sept. 2002.

[10] S. G. M. Koo, C. Rosenberg, H. -H. Chan, and Y. C. Lee. "Location Discovery in Enterprise-based Wireless Networks: Implementation and Applications," in *Proc. the 2nd IEEE Workshop on Applications and Services in Wireless Networks* (ASWN 2002), Paris, France, Jul 3-5, 2002.

[11] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial in User Service (RADIUS)", RFC 2865, June 2000.

[12] S. G. M. Koo, C. Rosenberg, H. Chan, and Y. C. Lee. "Location Discovery in Enterprise-based Wireless Networks: Case Studies and Applications," *Annals of Telecommunications*, to be published.

[13] K. McCloghrie, T. Rose, "Management Information Base for Network Management of TCP/IP –based internets," RFC 1213, March 1991.

[14] Cisco Aironet 350 Series Access Points, http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/

[15] Symbol Technologies' Spectrum24 4131 Access Point http://www.symbol.com/products/wireless/ap4131.html

[16] Intel PRO/Wireless 2011B LAN Access Point http://www.intel.com/network/connectivity/products/2011_lan_access.htm

[17] WAP11 - Instant Wireless Network Access Point ftp://ftp.linksys.com/datasheet/wapIIds.pdf

[18] Simple Object Access Protocol, http://www.w3.org/TR/SOAP/