Available online at www.sciencedirect.com
SCIENCE DIRECT®
The Journal of Systems and Software 76 (2005) 297–309
The Journal of Systems and Software
www.elsevier.com/locate/jss

Implementation of wireless network environments supporting inter access point protocol and dual packet filtering

Liang-Yi Hwang [a], Mei-Ling Chiang [b,*], Ruei-Chuan Chang [a]

[a] Department of Computer and Information Science, National Chiao-Tung University, Hsinchu, Taiwan, ROC
[b] Department of Information Management, National Chi-Nan University, Puli, Taiwan, ROC

Received 16 August 2002; received in revised form 13 June 2004; accepted 21 June 2004
Available online 26 August 2004

Abstract

With advances in wireless technologies, future internetworks will include large numbers of mobile hosts roaming across wireless cells. The goal of this paper is to provide a wireless network communication environment, in which mobile hosts can roam among various access points (wireless cells) and across different subnets. For this purpose, we develop methods to implement and integrate the communication mechanisms of Mobile IP and Inter Access Point Protocol (IAPP). For efficient transmission, we also devise a dual packet filtering technique to filter out unnecessary packet transmission, thereby reducing traffic on wireless networks. Such filtering is especially important because of the limited bandwidth of wireless links. Our work can serve as the reference once IAPP has been approved as standard.

Keywords: IAPP; Mobile IP; Packet filtering; Wireless LAN; Access point

1. Introduction

Due to advances in wireless technologies, together with the explosive growth of notebooks and handheld devices, future internetworks will include many mobile hosts roaming across wireless cells since wireless transmission provides the advantages of mobility and flexibility. However, the limited transmission bandwidth and low transmission quality are shortcomings to be overcome.

In a wireless LAN environment, users of mobile hosts can transmit data to each other through wireless links, and they can also communicate with other hosts on wired networks via access points. Thus, the access points act as bridges for communication between wireless and wired networks. The coverage for the wireless transmission area of an access point is called a cell or a basic service set (BSS).

Because they are mobile, users can carry mobile devices across cell boundaries and enter the area covered by another cell, which is referred to as roaming. A handoff mechanism is often used to solve the problem of termination of transmission or data loss when mobile hosts roam across cell boundaries. In addition, a mobile host may also roam to a different subnet, at which point its original IP address cannot be used in the new subnet and the on-going data transfer cannot be continued. Thus, the *Mobile IP* mechanism (Dixit and Gupta, 1996; Imielinski and Korth, 1996; Perkins, 1996) was developed to solve this problem.

The Mobile IP standard (Perkins, 1996) as defined by the Internet Engineering Task Force (IETF) is used to solve the above problem and let mobile hosts continue their on-going data transfer while roaming to different subnets. Mobile IP employs a home agent in each subnet

* Corresponding author. Tel.: +886 49 2910960; fax: +886 49 2915205.
E-mail addresses: joanna@ncnu.edu.tw (M.-L. Chiang), rc@cc.nctu.edu.tw (R.-C. Chang).

0164-1212/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2004.06.019

to keep track of the current location of the mobile host. Whenever a mobile host roams to another subnet, its home agent will encapsulate all the packets destined for the mobile host sent to the original subnet, and then forward the encapsulated packets to the mobile host according to its new location. In this way, the mobile host can roam among various subnets and can still receive and transmit data as usual. Thus, even if mobile hosts roam to another subnets, their on-going data transfer can still proceed. So Mobile IP specifies how a mobile host registers with its home agent and how the home agent routes datagrams to the mobile host through a tunnel.

However, Mobile IP cannot handle the problem that occurs when a mobile host roams to a different cell but remains in the same subnet. Without a handoff mechanism, access points act only as the bridges for communication between wired networks and wireless networks. This is because an access point would forward whatever packets it receives from wired interface to its wireless interface, regardless of whether or not the target mobile host resides in its BSS. This unnecessary packet transmission causes the waste of wireless bandwidth. Thus, Lucent Technologies, Digital Ocean, and Aironet Wireless Communications have collaborated to develop the *Inter Access Point Protocol (IAPP)* specification (Menri et al., 1998) to resolve this problem. This protocol is an IEEE 802.11 (1997) compliant wireless multi-vendor interoperatability protocol. Its primary function is to specify the handoff protocol for access points, such that their on-going data transferring can proceed while mobile hosts are roaming to different BSSs in the same subnet. By conforming to the IAPP, access points made by different manufacturers can cooperate in wireless networks.

However, the Mobile IP and IAPP are defined based on different network layers. Therefore, it is desirable to provide a method and system for integrating the IP-based (Postel, 1981) Mobile IP and UDP-based (Postel, 1980) IAPP communication mechanisms.

Currently, the IAPP protocol is under discussion in the IEEE 802.11 Task Group F for wireless LANs. Recently, IEEE 802.11f working group has come out a recommended practice for implementation of an Inter-Access Point Protocol on a Distribution System supporting wireless LAN (IEEE, 2003). Besides the same goal to ensure mobile hosts' roaming between access points from different vendors, this recommended practice is also designed for secure exchange of mobile hosts' security contexts between access points during handoff period. IAPP can use a RADIUS (Rigney et al., 2000) server for authentication. Systems implementing the original IAPP protocol can be thought of systems implementing the IAPP recommended practice with security level 1 (IEEE, 2003) that has no administrative or security support.

The goal of this current paper is to build a seamless wireless communication environment, in which mobile hosts can roam across different subnets and among various BSSs in the same subnet. We used Linux (Bovet and Cesati, 2002) as our experimental environment due to its popularity and its advantages of stability, reliability, high performance, and comprehensive documentation. Our system implements the original IAPP protocol (Menri et al., 1998) and uses it to solve the handover problem that occurs when a mobile host roams among different BSSs in the same subnet. Moreover, the system integrates the IAPP and the existing Mobile IP technology (Dixit and Gupta, 1996) to allow the mobile hosts to roam across different subnets. We also devise a dual packet filtering technique to reduce unnecessary or redundant traffic of packet transmission, thus increasing the bandwidth utilization of the wireless networks. Such filtering is especially important because of the limited bandwidth of wireless links.

Empirical results show that mobile hosts can successfully roam among various wireless cells and across different subnets, receiving and transmitting data as usual. A primitive performance evaluation also shows that the dual packet filtering technique can greatly improve transmission performance.

The rest of this paper is organized as follows. Section 2 briefly introduces the IEEE 802.11 wireless LAN, the Mobile IP, and the IAPP protocol. Related work is also discussed in this section. Section 3 presents our proposed system and its architecture, including the implementation of access point and IAPP management program for handling IAPP related events. Section 4 presents the implementation of our dual packet filtering mechanism. Section 5 reports the experimental results of the implementation, and Section 6 presents conclusions.

2. Background and related work

This section begins with the introduction of wireless LAN and related services defined by IEEE 802.11, then describing the Mobile IP specification in Section 2.2 and IAPP protocol in Section 2.3. Related work is discussed in Section 2.4.

2.1. Wireless LAN architecture and related IEEE 802.11 services

In IEEE 802.11 standard (1997), a wireless LAN consists of one or several basic service sets (BSS) and a BSS is composed of several mobile hosts. A wireless transmission environment is either an ad hoc network or an infrastructure network. An ad hoc network consists of independent BSSs, in which a BSS forms a self-contained network and no access to a distribution system

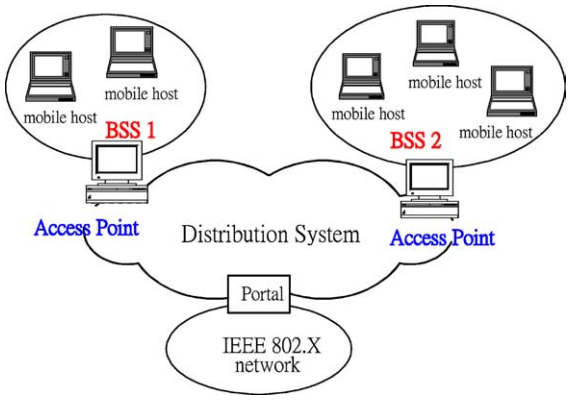

Fig. 1. Wireless LAN architecture.

is available. A distribution system interconnects multiple cells via access points to extend the wireless coverage area. In contrast, an infrastructure network consists of one or more BSSs and each BSS can make use of an access point to communicate with other networks through a distribution system. An access point serves as the interface between its covered wireless network and attached wired network, and it also plays the role of management center for an individual BSS. Fig. 1 shows the wireless LAN environment of the infrastructure network.

The IEEE 802.11 standard specifies the following distribution system services as the communication between an access point and mobile hosts or distribution system:

- Association
  When a mobile host initially starts, it receives the beacon from an access point, and then sends out association request to inform the access point of its entrance into the BSS. After confirmation, the mobile host can then communicate with other networks via this access point.
- Disassociation
  This service is used to notify the access point that the mobile host has left the BSS served by it.
- Reassociation
  When a mobile host roams into another BSS served by a new access point, it then sends out a reassociation request to inform the new access point of its entrance into the BSS. Again, after confirmation, the mobile host can then communicate with other networks via this new access point.
- Distribution
  This service is used when an access point wants to use a distribution system to communicate with other networks.
- Integration
  This service is used for a non-802.11 wireless network to communicate with a distribution system.

2.2. Mobile IP specification

The Mobile IP standard (Perkins, 1996) is defined by the Internet Engineering Task Force (IETF), and it enables mobile hosts to continue their on-going data transferring while roaming to different subnets. Mobile IP uses home agents and foreign agents to achieve the functions of handoff and data forwarding. Each agent will periodically broadcast information about itself, so that mobile hosts can know their current positions. Every mobile host must register its permanent IP address to its agent (i.e. home agent) at the initial time. This home agent is then responsible for keeping track of the current location of the mobile host after registering it.

Two different network architectures are defined in Mobile IP standard, as shown in Fig. 2 and illustrated as follows:

1. Network architecture with foreign agents
   When a mobile host roams into another subnet, its home agent will encapsulate all packets destined for the mobile host and then send them to the foreign agent of the mobile host. After receiving these encapsulated packets, the foreign agent will decapsulate these packets and then send them to the mobile host. This way of forwarding is called tunneling, as shown in Fig. 2(a).
   To support roaming, this method needs not change the IP address of a roaming mobile host, and a mobile host needs not the capability of decapsulation. However, this network architecture must have foreign agents to support the roaming of mobile hosts.
2. Network architecture without foreign agents
   As shown in Fig. 2(b), foreign agents are not needed at all in this network architecture. When a mobile host roams into another subnet, it gets a new IP address belonging to the new subnet and then informs

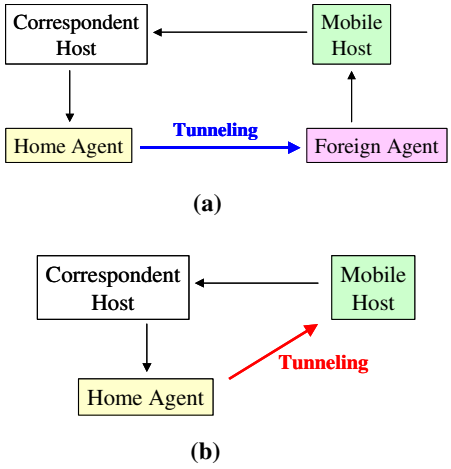

Fig. 2. Mobile IP protocol: (a) with foreign agents; (b) without foreign agents.

its home agent of its new IP address. Its home agent will encapsulate all packets destined for the mobile host and then send them to the mobile host. After receiving these packets, the mobile host must decapsulate them.

The advantage of this method is that the network architecture needs not have foreign agents. Therefore, mobile hosts can roam among existing networks that do not have any foreign agents. However, mobile hosts must have the capability of packet decapsulation.

2.3. Inter access point protocol

The current IEEE 802.11 standard addresses the physical and media access control layers of the OSI reference model for wireless LANs. IEEE 802.11 does not support handover, neither does it support coordination among access points. Besides, it has no exposed interface to the Distribution System. The Inter Access Point Protocol (IAPP) (Menri et al., 1998), originally proposed by the team of Lucent Technologies, Aironet Corporation, and Digital Ocean, mainly defines how access points from different vendors communicate with each other and the support of mobile hosts roaming across cells.

The proposed IAPP specification builds on the baseline capabilities of the IEEE 802.11 standard and is an extension of the IEEE 802.11 standard to support interoperability, mobility, handover, and coordination among access points of wireless LAN. This IAPP is implemented using IEEE 802.11 management frames (i.e. association packets and reassociation packets) and UDP/IP transmission. Since UDP/IP transmission is used, each access point should have an IP address. This IAPP mainly defines the protocol header of each IAPP packet and two handling procedures that are detailed in the Section 2.3.1.

The IAPP protocol is currently under discussion in the IEEE 802.11 Task Group F for wireless LANs. Recently, IEEE 802.11f working group has come out a recommended practice for implementation of IAPP (IEEE, 2003). In addition to ensure roaming between access points from different vendors, the system architecture also uses a RADIUS (Rigney et al., 2000) server for encryption and authentication.

Though the original IAPP and the IAPP recommended practice have different names for service primitives, and the original IAPP provides less number of service primitives, the counterpart of each service primitive in the original IAPP can be found in the IAPP recommended practice. Our system implementing the original IAPP protocol can be thought of the system implementing the IAPP recommended practice with security level 1 (IEEE, 2003) that has no administrative or security support. Section 2.3.2 briefly highlights the difference between the IAPP recommended practice and the original IAPP.

2.3.1. Original IAPP protocol

This protocol mainly defines the protocol header of each IAPP packet and two handling procedures: the announce procedure and the handover procedure.

The announce protocol is used mainly when a new access point is initially activated and the new access point needs to notify other access points about its existence. Access points can also use this protocol to exchange information about themselves or mobile hosts. In general, there are three scenarios for the announce protocol:

- When a new access point is initially activated, it should send out an announce request to notify other access points of its existence. Other access points must then respond with announce response packets upon receiving the announce request. When receiving responses from other access points, this new access point should also respond with announce response packets, as shown in Fig. 3.
- Every access point must periodically broadcast an announce request packet to notify other access points that it is still active.
- Access points can use this protocol to exchange information about themselves or their associated mobile hosts.

To complete the announce procedure, each access point must include the following data: when sending the announce request packet, it requires the Station Service ID (SSID) to indicate the BSS of the mobile host, the BSS, the channel number to show the frequency of the access point, and the physical communication type indicating the wireless communication type used by the mobile host, including direct sequence or frequency hopping.

In sending an announce response, it requires the SSID, the BSS, the physical communication type, the announce cycle for recording the intervals (120 s as default) between each announce response for the access

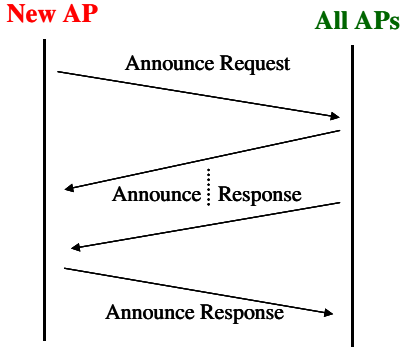

Fig. 3. Announce protocol.

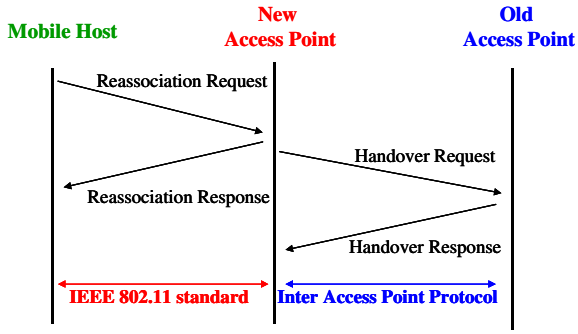

Fig. 4. Handover protocol.

point, the beacon cycle for recording intervals between each beacon, the handover timeout for indicating the time for completing the handover procedure (500 ms as default), and the channel number.

The handover protocol is used mainly when a mobile host roams to another BSS which is served by another access point, at which time the mobile host will send a reassociation request to the new access point. Then, the new access point will send out a handover request to the original access point of the mobile host to notify it about the roaming of the mobile host, and wait for the corresponding handover response, as shown in Fig. 4. This completes a handover procedure, which will allow the new access point to replace the role of the original access point and provide services for the mobile host.

To complete the handover procedure, each access point must include the following data for handover request packets: the SSID, the BSS, previous BSSID, the physical address of the mobile host, and the message ID to distinguish messages and prevent repeated forwarding of the same messages. The data required to complete the handover response procedure is the same as that required to process the handover request packet.

2.3.2. IAPP recommended practice

This protocol mainly consists of three protocol sequences: the add procedure, the move procedure, and the cache procedure. A RADIUS (Rigney et al., 2000) server can be applied for authentication and maintaining mapping of BSSID to IP addresses. This means that the new access point can discover the IP address of the old access point via RADIUS server and obtain the security information to secure the communication. TCP or UDP is used for communication between access points and UDP is used for communication between RADIUS server and access point. This protocol also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

The add protocol is used mainly when a mobile host registers to a new access point by an associate request. Once an access point receives an associate request, it should send out the broadcast add request for other access points to remove stale associations if they exist.

The move protocol is like the handover protocol in the original IAPP protocol. However, on receipt of a reassociate request, the new access point should use the RADIUS protocol for authentication and encryption, and to get the IP address of the old access point. Then the new access point sends a move request to the old access point, and then the old access point responds with the mobile host's Context block (IEEE, 2003). The Context block is used for removing the need for reauthentication.

The cache protocol implementing the proactive caching (Mishra et al., 2004) is used to avoid long handoff delay caused by IAPP communication between two access points as well as RADIUS server and access point. With proactive caching, current access point uses the cache request to distribute the security context of the mobile host to its neighboring access points before the mobile host actually handoffs.

Three security levels are possible with the IAPP capabilities. For level 1, the RADIUS server is not used, so that no administrative or security support exist. Then each access point should be configured with the mapping of BSSID to IP addresses for other access points. For level 2, the RADIUS server is responsible for maintaining the mapping of BSSID to IP addresses. For level 3, the RADIUS server supports encryption and authentication of IAPP messages.

2.4. Related work

To provide integrated networking service, Helal et al. (2000) presented an architecture for integration between wireless LANs and wireless WANs. Similarly, their architecture uses Mobile IP as an integrative layer atop different LAN/WAN networks. However, reducing the handoff latency is not discussed in their paper.

Several studies have focused on reducing the handoff latency for mobile hosts to roam across IP networks or across access points in various aspects. Fikouras et al. (2001) proposed a method using the link-layer information to accelerate Mobile IP handoff. Through link-layer information such as the 802.11b Service Set Identifier (SSID) that provides the identity of Mobile IP agent, Mobile IP mechanisms for movement detection and periodic Mobile IP agent broadcast advertisements are not necessary. Therefore, faster Mobile IP hand-offs can be achieved. However, this method should assume that the link-layer is capable of delivering information to Mobile IP layer regarding the identity of Mobile IP agent. In contrast, our approach maintains the layer independence and uses packet filter in access point's bridge program to reduce unnecessary broadcast advertisements from Mobile IP agent.

Mishra et al. (2004) proposed proactive caching to avoid handoff delay caused by IAPP communication between two access points as well as access point and

RADIUS server. Current access point of a mobile host distributes the security context of the mobile host to its neighboring access points in advance. So that when the mobile host is reassociating to its neighboring access point, context transfer from old access point to new access point is not needed. They also devised an efficient data structure, neighbor graphs (Mishra et al., 2004), to dynamically determine the set of potential neighboring access points without examining network topology and manually creating the set. Currently, the proposed proactive caching is included in the IAPP recommended practice (IEEE, 2003).

Similar to our implementation, their IAPP implementation is inside the wireless LAN card driver and a stand-alone IAPP daemon program. Similarly, those two components use system calls and signals to communicate to each other, whereas, proactive caching is implemented in their driver. However, our system does not rely on RADIUS server to maintain mapping of MAC addresses to IP addresses for all access points. Nor does our system need to transfer this mapping information from old access points. Instead, this mapping information is maintained in our IAPP management program, which is constructed during the announce procedure when an access point is initiated. For a trusted environment in which authentication is not an issue, our approach does not reed a RADIUS server for obtaining old access point's IP address to fulfill the handover procedure. More reliability and efficiency can be achieved.

Shin et al. (2004) devised a discovery method using neighbor graphs and non-overlap graphs in the probing process to find a new access point with the best signal quality with respect to the mobile host. Their goal is to reduce the total number of probed channels as well as the total time spent waiting on each channel.

Pack and Choi (2002a,b) proposed a fast inter-access point handoff scheme for public wireless LAN. They use predicative authentication scheme to minimize the handoff latency caused by authentication procedures at the new access point. Whereas, our work focuses on the implementation of the system supporting IAPP protocol and using dual packet filtering technique to reduce traffic on wireless networks and improve transmission performance.

3. System design and implementation

In this section, we present our system design and implementation, first briefly describing our system environment and architecture. Based on this architecture, we present the implementation of access points that follow the original IAPP protocol (Menri et al., 1998). On the other hands, since there have been many studies on Mobile IP technologies (Dixit and Gupta, 1996; Imielinski and Korth, 1996; Perkins, 1996), we make use of the existing Mobile IP programs (Dixit and Gupta, 1996) developed at Binghamton University to reduce implementation effort and focus on the integration of Mobile IP and IAPP protocol.

3.1. System environment and architecture

Fig. 5 shows our proposed wireless environment and the system architecture. In this environment, each subnet has one agent (home or foreign agent) to manage the whole subnet. The Mobile IP standard is used as the communication protocol among agents. Each subnet may consist of one or several access points due to the limited coverage of an access point. The original IAPP protocol is used as the transmission protocol among access points.

Because of the spirit of GNU General Public License (GPL) (Free, 1991) and open source codes, Linux (Bovet and Cesati, 2002) has gained popularity and provides the advantages of stability, reliability, high performance, and comprehensive documentation. Therefore, we used Linux as our experimental environment. Our implementation mainly includes the following works:

- Access points
  This work implements the wireless and wired interfaces of access points, including the construction of hardware and software for access points.
- IAPP management program
  This work implements an IAPP management program in the user level of an access point to perform IAPP communication procedure.
- Integration of Mobile IP and IAPP
  To reduce implementation effort, we use the Mobile IP programs developed by Dixit and Gupta (1996). Our work mainly implements a dual packet filtering technique for reducing unnecessary or redundant packet transmission, especially when Mobile IP and IAPP are integrated.

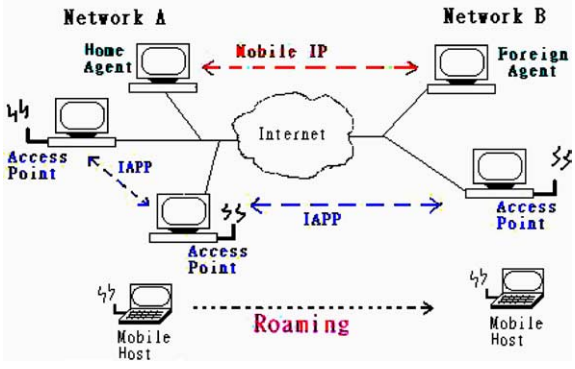

Fig. 5. System architecture.

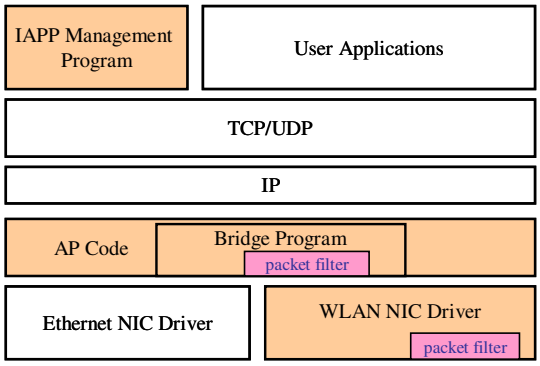

Fig. 6. Software architecture.

The software architecture of our access point is depicted in Fig. 6. The implementation is detailed in the rest of this section and in Section 4.

3.2. Implementation of access points

A wireless LAN is comprised of mobile hosts and access points. Access points act as servers, which forward MAC frames among mobile hosts and offer bridging services between wireless LANs and other IEEE 802-series LANs. Though there are access points made by many manufacturers, but they do not all follow the IAPP protocol. To conform to the IAPP specification built on the baseline capabilities of the IEEE 802.11 standard (1997), an access point must be able to handle IEEE 802.11 management frames sent by mobile hosts, such as association requests, reassociation requests, and disassociation requests, etc. Therefore, modification of wireless LAN card drivers at access points is needed to handle these requests. However, vendors' driver source codes are hard to obtain. Therefore, we implemented access points ourselves.

We implemented an access point on a Pentium PC, as shown in Fig. 7. In the PC with Linux environment, a wired LAN card (i.e. an Ethernet card) and a wireless LAN card (i.e. PCMCIA wireless LAN card) were installed to communicate with the wired LAN and the wireless LAN respectively. A bridge program was implemented to act as an interface between the wired and wireless LAN cards.

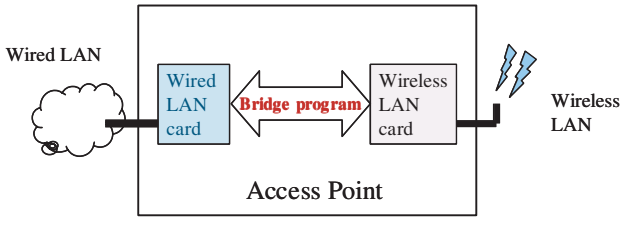

Fig. 7. Structure of an access point.

In the software implementation, we implemented wireless LAN card driver (Hwang et al., 1999) that follows the IEEE 802.11 standard to process the communication mechanism, including processing the association requests, reassociation requests, and disassociation requests of a mobile host.

To reduce unnecessary packet transmissions, we added a packet filter to the wireless LAN card driver of an access point. An access point uses this packet filter to determine whether it should forward packets received from the wired interface (i.e. its attached wired network) to the wireless interface (i.e. its covered wireless network). This packet filter examines the target address of every packet received from the wired interface; it then determines whether the target mobile host has previously registered to this access point. An existing registration means the target mobile host has roamed into the BSS covered by this access point. Then the access point will forward the received packets from the wired interface to the wireless interface. In this way, packets not destined for the mobile hosts in the BSS served by this access point will not be forwarded.

3.3. IAPP management program

To enable access points to cooperate with each other using IAPP protocol and process received IAPP packets, we implemented an IAPP management program on an access point for processing the IAPP packets according to the original IAPP protocol.

This IAPP specification mainly defines two protocols to implement the functions of the IAPP: an announce protocol and a handover protocol. The announce protocol is used to implement the coordination and management of access points. The handover protocol is used to handle handoff-related events, such as updating the access points with the current locations of mobile hosts, etc.

According to this IAPP specification, we implemented the IAPP management program that uses UDP/IP (User Datagram Protocol/Internet Protocol) protocol for data communication. It mainly includes two procedures, namely, announce and handover procedures for processing four different packet types of announce request, announce response, handover request, and handover response.

Fig. 8 shows the structure and operations of the IAPP management program. The IAPP management program is a user-level program and is initiated at startup. It executes in the background and is ready to perform operations whenever required. Since the data in the kernel level is inaccessible to the user-level program, so the IAPP management program uses implemented system calls to obtain information about the access point (e.g. physical address, Basic Station Service ID) and the mobile host (e.g. the physical address, and the physical

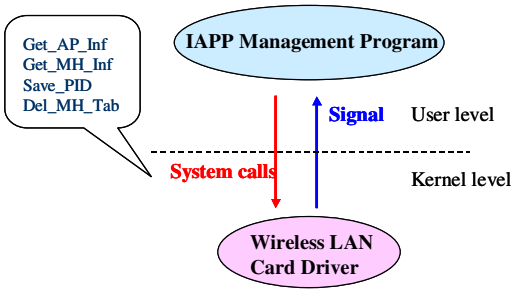

Fig. 8. The interaction of IAPP management program and wireless LAN card driver.

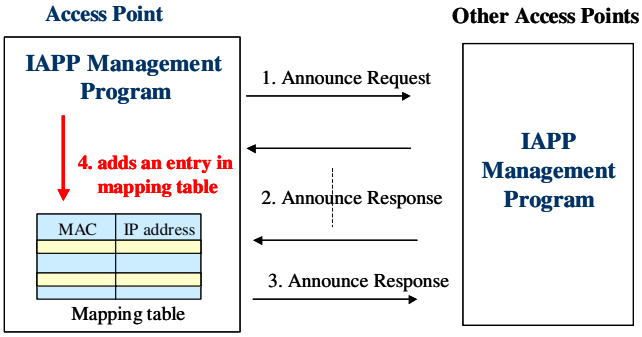

Fig. 9. The announce procedure of IAPP management program.

address of the access point previously registered by this mobile host) from the wireless LAN card driver that is located at the kernel level.

So that the user-level IAPP management program can exchange information with the kernel-level wireless LAN card driver of an access point, the following system calls are implemented:

1. *Get_AP_Info( )*: used to obtain information about the access point.
2. *Get_MH_Info( )*: used to obtain information about the mobile host, including physical address (i.e. MAC address), and the physical address of the access point previously registered by the mobile host.
3. *Save_PID( )*: used for storing the process ID of the IAPP management program in the wireless LAN card driver.
4. *Del_MH_Table( )*: executed by the IAPP management program for deleting the registration record of a mobile host when the mobile host roams to a new BSS.

Furthermore, when the wireless LAN card driver of an access point receives the reassociation request packet from a mobile host, it sends signals to the IAPP management program to perform the handover procedure.

3.3.1. Announce procedure

Fig. 9 shows the operations of the IAPP management program in processing the announce request procedure. Whenever a new access point is initially activated, the new access point broadcasts the announce request packet to the same subnet and to other subnets as well.

Since the router is usually configured to block broadcast packets, so the broadcast announce request packets will be directly broadcast to the same subnet as well as other associated subnets using UDP/IP. These associated subnets have been previously recorded in the access point or configured when the access point is initially activated. The information of these associated subnets determines which subnets should be selected to send the announce request packets. Since the IP address of each access point can be obtained from an announce response packet, so the access point can establish a *MAC-to-IP mapping table* for storing the physical address (i.e. MAC address) and its associated IP address according to each announce response packet received. Thus, this mapping table can collect and provide the information required for sending handover request packets.

The operations of the IAPP management program are described in detail as follows. First, when the IAPP management program of an access point is initially activated, it uses the Get_AP_Info system call to obtain the physical address of the wireless LAN card from the wireless LAN card driver. The physical address of the wireless LAN card acts as the Basic Service Set Identification number (BSSID) of that access point. The BSSID will be filled into the header of the announce request packet, which will then be broadcast to the current subnet of the access points and to other subnets. After that, the IAPP management program waits for announce response packets from other access points.

Afterwards, if the IAPP management program receives the announce response packets from other access points existing in the same or other subnets, then the IAPP management program will respond with an announce response packet. In addition, the IAPP management program will also obtain the physical address and the IP address of the access point from the header of the announce response packets received. Then, the physical address and the IP address of the access point are kept in the MAC-to-IP mapping table for the convenience of lookup at the time of transmitting handover request packets.

This MAC-to-IP mapping table is constructed because when the mobile host roams from one BSS to another BSS, the mobile host would register to the new access point by sending a reassociation request packet. The new access point in turn will send a handover request packet to the old access point previously registered by the roaming mobile host according to its IP address. However, the reassociation request packet contains only the physical address of the old access point rather than its IP address. Thus, the IAPP management program

will have to find the IP address of the old access point by looking up the MAC-to-IP mapping table using the physical address of the old access point as an index. After finding a match, the IP address found will be used as the destination address of the handover request packet. With this MAC-to-IP mapping table, it would be easy to find the associated IP address of an access point previously registered by a roaming mobile host, such that the IAPP manage program can successfully send out a handover request.

3.3.2. Handover procedure

The handover procedure is the most important procedure for the entire IAPP management program. When the wireless LAN card driver of an access point receives the reassociation request packet from a mobile host, the wireless LAN card driver sends a handover signal to inform the user-level IAPP management program to process the handover procedure for the roaming mobile host.

Fig. 10 shows the operations of the IAPP management program in response to a reassociation request from a roaming mobile host. When the IAPP management program receives the handover signal from the wireless LAN card driver, this indicates that a new mobile host has roamed to the BSS of the current access point. At that time, IAPP management program has to notify the old access point previously registered by the mobile host about the new location of the mobile host. The IAPP management program first uses the Get_MH_Info system call to get the physical address (i.e. MAC address) of the old access point of the mobile host. Then, the IAPP management program searches the MAC-to-IP mapping table to find the IP address of the old access point using its physical address as an index. The IP address found will serve as the destination address of the handover request packet. After that, the IAPP management program sends the handover request packet to the old access point according to the destination address and then waits for a response.

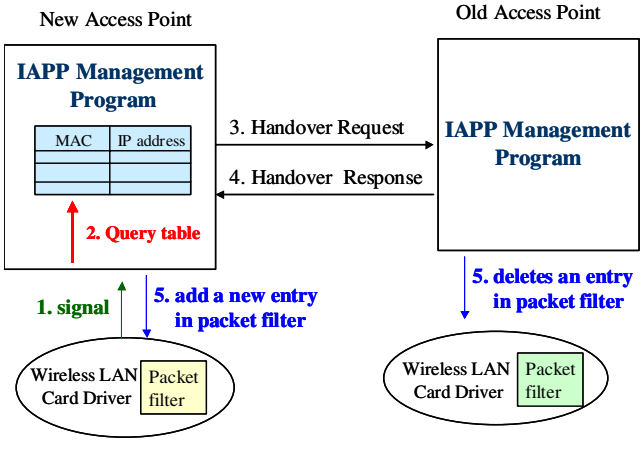

Fig. 10. The handover procedure of IAPP management program.

At this time, in addition to send out the handover request packets, the wireless LAN card driver of the current access point also inserts the information regarding the newly registered mobile host into the packet filter. Thus, every mobile host successfully registered in the current subnet will have a registration record in the packet filter. Accordingly, whenever the wireless LAN card driver receives an incoming packet, it first searches the packet filter to find if there is a correspondence between an entry of the packet filter and the destination address of the incoming packet. If there is no match, it indicates that the mobile host has roamed away from the current BSS, so the incoming packet will not be forwarded to its destination. Eventually, the traffic on the wireless LAN can be reduced.

On the other hand, upon receiving the handover request packet, the access point, which was previously registered by the mobile host, will send the handover response packet and use the Del_MH_Table system call to delete the registration record of the mobile host from the packet filter in the wireless LAN card driver. Thus, checking whether the mobile host is still within the BSS can be easily performed by searching the packet filter. If the mobile host has roamed to another BSS, the wireless LAN card driver will not forward the incoming packets destined for the mobile host to the wireless LAN. Consequently, the packet traffic can be effectively reduced.

4. Implementation of dual packet filtering

The IAPP communication mechanism is sufficient for processing the roaming of a mobile host in the same subnet. However, when a mobile host is roaming across different subnets, a Mobile IP communication mechanism is required.

According to the Mobile IP standard, each Mobile IP agent periodically broadcasts a message about itself to its own subnet. When an access point receives this broadcast packet, it also forwards it to its associated wireless LAN. Thus, it is necessary for access points to periodically forward the broadcast packets for the Mobile IP agents. On the other hand, under the infrastructure of the wireless networks, each access point also periodically broadcasts a message (i.e. beacon) about itself to the same subnet. Therefore, two kinds of broadcast message are broadcast in the wireless LANs. However, a mobile host determines its own BSS position according to the beacons of access points, rather than the packets broadcasted by the Mobile IP agents. Whereas, if an access point does not forward the broadcast packets for the Mobile IP agents, then mobile hosts will have no way to determine if they have roamed to another subnet served by another Mobile IP agent.

To further reduce unnecessary traffic on the wireless LANs, in our system, access points do not need to periodically broadcast packets for the Mobile IP agents. Instead, the access point only broadcasts the message for the agent whenever required, thus preventing waste of the wireless LANs bandwidth. In our system, an access point includes another packet filter in the bridge program for analyzing the destination of the incoming broadcast packets. Only when a mobile host is registering to the access point, will the bridge program enable the forwarding of the broadcast packets from the Mobile IP agents to the wireless LAN. Then the mobile host can determine if it has roamed to another subnet served by another Mobile IP agent and perform Mobile IP communication mechanism. After the mobile host finishes the Mobile IP procedure, it will inform the access point and the bridge program will stop forwarding the broadcast packets from the Mobile IP agents so as to further reduce the traffic to the wireless LAN. Fig. 11 shows this packet filter in the bridge program.

The decision to implement the packet filter for filtering out broadcast packets from the Mobile IP agent in the bridge program of an access point instead of modifying Mobile IP programs is intended to preserve the flexibility and completeness of Mobile IP programs, such that even when the Mobile IP programs are changed or modified, our system is not affected at all.

5. Experimental results and analysis

This section presents the experimental results and analysis for our wireless communication system. Section 5.1 describes our experimental environment. Section 5.2 measures the time needed for a mobile host to fulfill the handover procedure. Section 5.3 measures the effect of the packet filter in the wireless LAN card driver on the transmission efficiency, which is employed to filter out packets not destined for any mobile host in the BSS. Section 5.4 measures the effect of the packet filter in the bridge program on the transmission efficiency, which is used to filter out unnecessary broadcast packets from Mobile IP agents. Section 5.5 measures the effect of the number of registered mobile hosts.

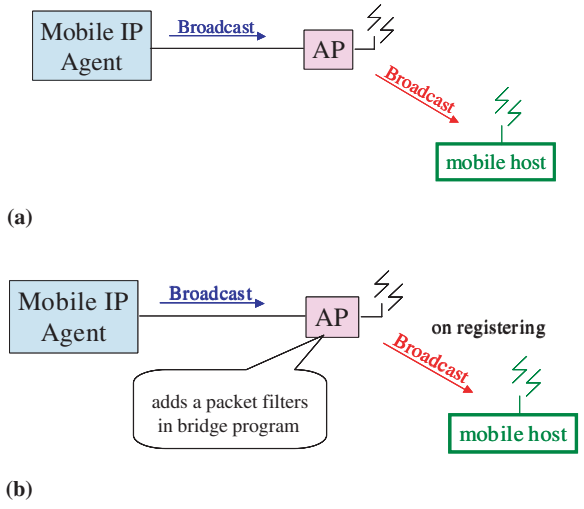

Fig. 11. Packet filtering used in the integration of Mobile IP and IAPP: (a) without packet filtering; (b) with packet filtering.

5.1. Experimental environment

We use Linux as our experimental platform. Fig. 12 and Table 1 show our experimental environment, consisting of two different IP subnets, with each subnet having a Mobile IP agent, represented as home agent and foreign agent respectively, to provide services on the network layer for mobile hosts. The Mobile IP agents communicate with each other via Mobile IP communication mechanism, and there are several access points in the different subnets to provide services over the entire network. Each access point communicates with another via an IAPP communication mechanism. The mobile hosts make use of access points to communicate with wired networks.

5.2. Handoff performance

Since the time needed to fulfill the registration represents the time needed to fulfill the handover procedure, this section measures the time for a mobile host to register for a new access point when it roams into a BSS serviced by the new access point. The longer the handover time, the higher the data loss rate while the handover procedure is underway.

When a mobile host roams to another BSS, it receives a beacon (i.e. broadcast packet) from the new access point. The measured time begins from the time that a mobile host sends out the reassociation request packet to the new access point to the time when it receives the reassociation response packet from the new access point, indicating the completion of registration. The measurement was repeated ten times for a mobile host that roamed from the BSS of access point 1 to the

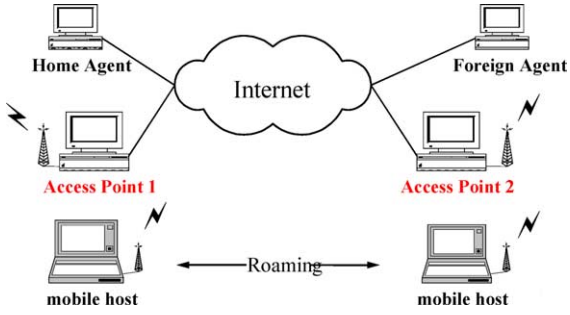

Fig. 12. Experimental environment.

Table 1
Experimental platform

	CPU	Wired network card	Wireless network card
Hardware:			
Access point 1	Pentium 75 (RAM 64M)	D-Link DE220	DBtel PCMCIA (2 Mbps)
Access point 2	Pentium 75 (RAM 32M)	D-Link DE220	DBtel PCMCIA (2 Mbps)
Home agent	Pentium 120 (RAM 40M)	D-Link DE528	None
Foreign agent	Pentium 90 (RAM 32M)	D-Link DE220	None
Mobile host (notebook)	Pentium 200 (RAM 64M)	None	DBtel PCMCIA (2 Mbps)
Software:			
Operating system: Linux (RedHat 5.2), Kernel version 2.0.30			
PCMCIA device driver: version 3.0.5			
Mobile IP program (Dixit and Gupta, 1996), version 1.00			

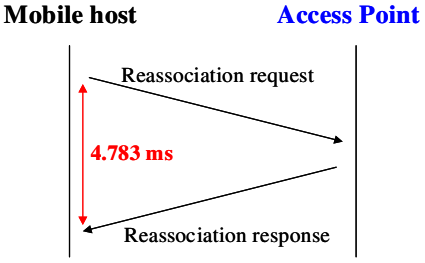

Fig. 13. The measured time of handover.

BSS of access point 2 and then back to the BSS of access point 1. The mobility of the mobile host was not concerned in this evaluation since we measured the time needed to fulfill the registration including handover time.

Fig. 13 shows that an average of 4.783 ms was required for a mobile host to fulfill the handover procedure. This also means when a mobile host roams to a new BSS, it has to wait for average 4.783 ms to continue data transmission.

5.3. The performance of the packet filter in the device driver

This section measures the effect of the packet filter in the wireless LAN card driver on the transmission efficiency, which we used to filter out packets not destined for any mobile hosts in the BSS. Without this packet filtering, the access point will forward whatever it receives from wired networks to its BSS.

Our test program was modified from *NetPerf* program (Hewlett, 1995), which originally repeatedly transmitted 64-byte packets between two PCs. The time period for this measurement lasted 10 s and we measured how many packets were successfully transferred. Then the packet round trip time can be obtained. In this test environment, only one mobile host registered to the access point. This test program was performed 20 times on one pair of mobile host and fixed host. Since this test focused on the measurement of the effect of the packet filter in the wireless LAN card driver, so the fixed and mobile hosts were located in the same subnet and the Mobile IP programs were not executed. Ten fixed hosts (PCs) and the access point reside in the same subnet. Except from the PCs in experiment, other PCs are idle during the experiments.

To explore the effect of the packet filter, our measurements were performed under three different network transmission environments, as follows:

Case 1. Baseline network environment

Only run our test programs on one pair of mobile host and fixed host. Other machines are all idle.

Case 2. Network environment with additional traffic

In addition to running the test programs, one PC repeatedly runs Ping program for creating additional traffic on the network.

Case 3. Network environment with extra workload

The test programs were running on two pairs of PCs to add the workload of transmission.

The results shown in Fig. 14 demonstrate that under various network environments, when a packet filter is

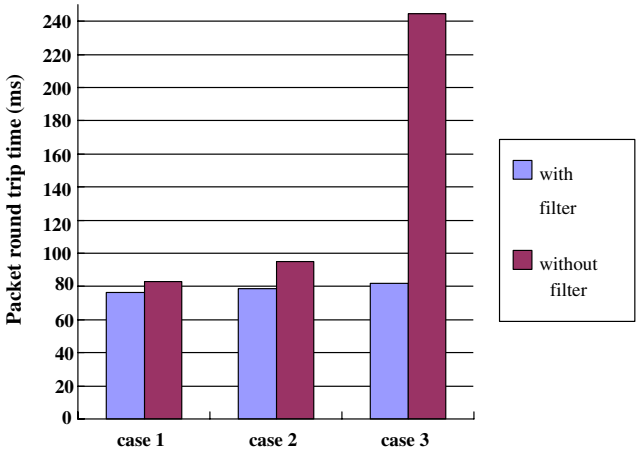

Fig. 14. Effect of packet filtering in device driver under various network environments.

used, the transmission efficiency can be largely improved. The improvement of transmission efficiencies are 8.17% for Case 1, 17.23% for Case 2, and 66.55% for Case 3.

We believe that for real practical network environments, the network traffic is much heavier and also many more mobile hosts will reside in the wireless networks. By filtering out unnecessary packets, the transmission efficiency can be dramatically improved.

5.4. The effect of the packet filter in the bridge program

The packet filter in the bridge program is used to filter out broadcast packets from the Mobile IP agent. Only in certain periods will the bridge program forward broadcast packets from Mobile IP agent to its associated wireless LAN.

In this measurement, the benchmark was the same as those of previous measurements. Mobile IP programs were executed and the device drivers of access points also have packet filters. To find out the minimum improvement, the test programs were run under the baseline network environment (i.e. Case 1) and only one mobile host has registered to the access point. In this test, the Mobile IP agent sent out broadcast packets about once per second.

Fig. 15 shows the results. Though under this very light workload, the bridge program with packet filtering performed better than the program without packet filtering. This performance improvement is because of the reduction of transmission of broadcast packets from the Mobile IP agent and the reduction of the processing overhead for mobile hosts to handle the received broadcast packets, such as determining whether mobile hosts have roamed to a new subnet, etc. The performance improvement would be expected to be more significant in a practical network environment with heavier workload or with Mobile IP agents broadcasting packets more often.

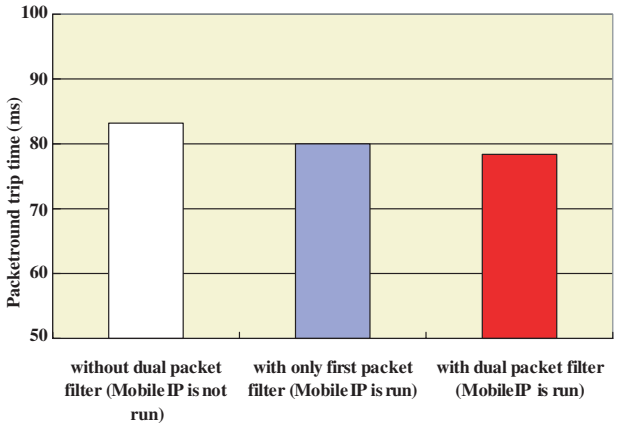

Fig. 15. Effect of packet filtering in bridge program.

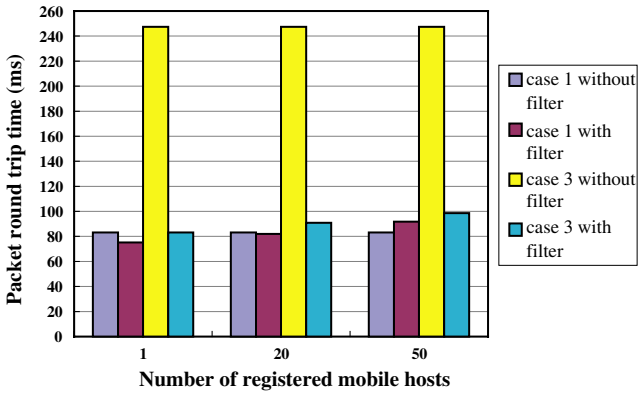

Fig. 16. Effects of the number of registered mobile hosts.

5.5. The effect of the number of mobile hosts

Previous experimental results show that our dual packet filtering can greatly improve transmission efficiency. Those measurements were done under the environment in which only one mobile host resided in the wireless LAN. This section measures the effect of the number of mobile hosts registered to an access point on the transmission efficiency. The time to look up the filter table in the packet filter also affects the efficiency. The larger the filter table is, the longer the time required for filtering processing.

In the test, the system used sequential search to look up the filter table in the packet filter of wireless LAN driver, and assumed the worst case that the queried mobile host entry resided in the final entry of the filter table. The network environment was the same as those of previous measurements.

Fig. 16 shows that when packet filtering is used in the wireless LAN driver, the improvement of transmission efficiency ranged from 8.17% to 66.54%. However, when the number of registered mobile hosts was larger, the transmission efficiency decreased. This is because more time is needed to look up an entry in the filter table for filtering processing. Therefore, an efficient method such as hashing instead of using sequential search would be required for table lookup when the number of registered mobile hosts is large.

6. Conclusions

We have successfully implemented a seamless wireless communication environment that supports IAPP protocol and Mobile IP standard, such that a mobile host can roam among various wireless cells and across different subnets. In addition, a dual packet filtering mechanism is employed to filter out unnecessary or redundant traffic of packet transmission. One packet filter in the wireless LAN card driver of an access point determines if an

incoming packet will be forwarded to its associated wireless LAN and the other packet filter in the bridge program of an access point controls the traffic flow towards the wireless LAN. Preliminary performance evaluation shows that transmission efficiency is greatly improved when this dual packet filtering mechanism is used.

Our implementation supporting the original IAPP protocol can be thought of the system implementing the IAPP recommended practice with level 1 security that has no RADIUS usage. For a trusted or small-scale wireless environment, this is acceptable. Besides, since it does not rely on the RADIUS server for operations, better reliability can be achieved. However, if a secure environment is needed, a RADIUS server such as Free RADIUS (2003) should be added.

Based on this system, several issues can be explored or enhanced, and several services can be added, such as authentication of mobile hosts on registration or handover, provision of user profiles, different quality of services (QoS) for registered mobile hosts, etc. In addition, providing the forwarding of buffered frames would be helpful for reducing the data loss rate during handoff.

References

Aironet Wireless Communications, http://www.aironet.com/>.

Bovet, D.P., Cesati, M., 2002. Understanding the Linux Kernel, second ed. O'Reilly Associates, Inc.

Digital Ocean, http://www.digitalocean.com/>.

Dixit, A., Gupta, V., 1996. The User Guide of Mobile IP for Liunx, Binghamton University.

Fikouras, N.A., Könsgen, A.J., Görg, C., 2001. Accelerating Mobile IP hand-offs through link-layer information, an experimental investigation with 802.11b and Internet audio. In Proceedings of the International Multiconference on Measurement, Modeling, and Evaluation of Computer-Communication Systems (MMB), Aachen, Germany.

Free Software Foundation, Inc., 1991. GNU General Public License (GPL), http://www.linux.org/info/gnu.html>.

Free RADIUS Server Project, http://www.freeradius.org>.

Helal, S., Lee, C., Zhang, Y., Richard III, G.G., 2000. An Architecture for Wireless LAN/WAN Integration, Wireless Communications and Networking Conference.

Hewlett-Packard Company, 1995. Netperf: A Network Performance Benchmark.

Hwang, L.Y., Hwang, W.S., Lin, Y.T., Chiang, M.L., Chang, R.C., 1999. IEEE 802.11 PCMCIA wireless LAN drivers design and implementation. Technical Report, Department of Computer and Information Science, National Chiao Tung University, Taiwan, ROC.

IEEE 802.11, 1997. Draft Standard for Wireless LAN, Medium Access Control (MAC) And Physical Layer Specification.

IEEE Std 802.11F, 2003. Recommended practice for multi-vendor access point interoperability via an inter-access point protocol across distribution systems Supporting IEEE 802.11 operation.

Imielinski, T., Korth, H.F., 1996. Mobile Computing.

Lucent Technologies, http://www.lucent.com>.

Menri, Moelard, Lucent Technologies, 1998. Inter-Access Point Protocol Draft.

Mishra, A., Shin, M., Arbaugh, W., 2004. Context caching using neighbor graphs for fast handoffs in a wireless network. In: Proceedings of the 23rd IEEE Conference on Computer Communications (INFOCOM).

Pack, S., Choi, Y., 2002a. Fast inter-AP handoff using predictive-authentication scheme in a public wireless LAN. In: Proc. IEEE Networks 2002 (Joint ICN 2002 and ICWLHN 2002), Atlanta, USA.

Pack, S., Choi, Y., 2002b. Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1x Model. In: Proc. IFIP PWC 2002, Singapore.

Perkins, C., 1996. IP Mobility Support, RFC 2002.

Postel, J., 1980. User Datagram Protocol, RFC 768.

Postel, J., 1981. Internet Protocol, RFC 791.

Rigney, C., Willens, S., Rubens, A., Simpson, W., 2000. Remote Authentication Dial In User Service (RADIUS), RFC 2865.

Shin, M., Mishra, A., Arbaugh, W., 2004. Improving the latency of 802.11 hand-offs using neighbor graphs. In: 2nd International Conference on Mobile Systems, Applications, and Services (MobiSys).