ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Computer Communications 30 (2007) 1785–1793

computer communications

www.elsevier.com/locate/comcom

DualMAC: A soft handoff mechanism for real-time communications in secured WLANs

Shiao-Li Tsao *, Pang Hsiang Lo

Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan, ROC

Received 6 June 2006; received in revised form 12 February 2007; accepted 12 February 2007
Available online 17 February 2007

Abstract

WLAN has been widely deployed over public and private areas in recent years and has become one of the most popular access technologies for mobile Internet services. Handoffs between WLAN access points (APs) that introduce packet loss and delay during a network session is one of the critical issues for real-time communication services. Unfortunately, most of the previous studies in reducing handoff latency and packet loss in WLANs rely on WLAN infrastructure upgrades, and those solutions suffer from deployment problems in the well-established WLAN hotspots. In this work, a pure station (STA)-side approach which only requires the firmware or software upgrade on WLAN STAs without the enhancements of the WLAN standards and infrastructures is presented. The proposed mechanism developed from a time division duplex concept maintains both connections with the serving and target AP simultaneously using two different medium access control (MAC) addresses. Thus, an STA can perform WLAN association, authentication, security key handshake procedures with the target AP, or further acquires an IP address in a new subnet while transmitting and receiving real-time packets through the serving AP at the same time. Simulation results demonstrate that seamless handoffs for real-time communications in secured WLANs can be easily achieved by the proposed mechanism.

Keywords: Wireless LAN (WLAN); Handoff; Mobility management; Real-time communication; Voice over IP (VoIP) over WLAN (VoWLAN)

1. Introduction

The IEEE 802.11 WLAN that has been widely deployed over public and private areas in recent years is considered to be one of the most popular access technologies for mobile Internet services. WLAN handoff that involves a number of link-layer and/or network-layer procedures and introduces packet delay and loss is one of the critical issues for mobile Internet applications and services. In secured WLANs that enable the access control and link-layer encryption, handoff delays further increase since a station (STA) has to negotiate the security context and encryption keys with the target AP after a handoff. The packet delay and loss due to handoffs in secured WLANs may not be acceptable for real-time communications such as voice over IP (VoIP) over WLAN (VoWLAN).

Mishra et al. [1] investigated the latency of a WLAN handoff in a network without the access control and link-layer encryption, and indicated that channel probe contributes a significant portion of the handoff delay. They thus suggested a mobile STA to remember the visited APs and to construct a neighbor relationship graph of these APs. Hence, an STA knows the information of neighboring channels, and can avoid unnecessary scans during a handoff. The scan delay is thus minimized [3]. WLAN scan mechanisms that measure the strength of signals from APs and decide an AP to handoff can be categorized into active and passive scan. For an active scan, an STA actively sends a *Probe Request* message to a WLAN channel and waits for *Probe Response* messages from APs. On the other hand, an STA listens passively to beacon

[*] Corresponding author. Address: Room EC426, No. 1001 Ta Hsueh Road, Hsinchu, Taiwan 300, ROC. Tel.: +886 3 5712121x54717; fax: +886 3 5721490.

E-mail address: sltsao@cs.nctu.edu.tw (S.-L. Tsao).

0140-3664/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2007.02.009

messages from APs for a passive scan. Experiments indicate that an STA may spend up to several hundred milliseconds for an active scan of all channels [1]. A complete scan of all channels introduces considerable delay and service disruption for a real-time communication. Ramani et al. [8] thus proposed a new passive scan mechanism, called the SyncScan, which assumes STAs to have timing information of beacons from APs. According to the SyncScan strategy, an STA switches to a specific channel in a proper time interval to listen passively to a beacon from an AP, switches back to the original channel and then resumes packet exchanges with the serving AP. Hence, the scan procedure can be performed without introducing too much packet loss and delay for real-time communications over WLANs.

For WLANs whose access control mechanism such as the IEEE 802.1x and link-layer encryption function such as the IEEE 802.11i are enabled, the authentication and key exchange procedures between an STA and the target AP introduce further delays during a handoff [4,5]. Mishra et al. [5] applied their neighbor graph concept to implement a proactive key distribution method in secured WLANs. According to the proactive key distribution mechanism, a full IEEE 802.1x authentication with the target AP could be avoided. Moreover, the conventional four-way handshake defined in the IEEE 802.11i for establishing a security key between an AP and STA can be simplified as a two-way handshake. This idea is also adopted in the newly established 802.11 working group, the IEEE 802.11r, for fast base-station switching [10]. The neighbor graph concept can be further employed to pre-assign network resources such as IP address for a network-layer handoff. Then, an STA can acquire an IP address in a new subnet before a handoff so that the handoff delay is reduced [6,7]. Unfortunately, previous solutions either need all APs and STAs to upgrade to support new protocols, such as the IEEE 802.11k and 802.11r [10,11], which are still not yet settled or require infrastructure enhancements, and the solutions suffer from deployment problems over the well-established WLAN hotspots. In this work, a pure station (STA)-site approach that only requires the software/firmware enhancement on WLAN STAs without modifying the IEEE standards and WLAN infrastructures is presented. The proposed mechanism, called DualMAC, is developed from a time division duplex concept, and maintains connections with the serving and target AP simultaneously using two medium access control (MAC) addresses. Then, an STA can perform WLAN authentication and association, establish encryption keys with the target AP before disassociating with the serving AP. Thus, a soft handoff between WLAN APs can be achieved and the service disruption time for a real-time communication during a handoff in secured WLANs can be minimized.

Brik et al. [9] proposed a new mechanism called MultiScan which suggests an STA to install two radio interfaces. Therefore, the STA can perform WLAN scan by using the secondary radio interface without influencing the communications with the serving AP. This approach can eliminate the scan and handoff latencies but requires the installation of an additional WLAN interface which is more expensive. To use only one radio interface and time division duplex concept to connect to two different WLAN networks is first presented in the MultiNet [2]. The MultiNet implements a middleware in-between MAC and network layer on a mobile STA to emulate multiple WLAN interfaces. The main goal of the MultiNet is to join several different networks such as an infrastructure and ad hoc network at the same time to extend network coverage. The purposes of the proposed DualMAC that considers a handoff problem and reduces the packet loss and service disruption time for a real-time communication over a secured WLAN infrastructure are different from the MultiNet. Our approach only needs to configure two MAC addresses in a WLAN driver or firmware in order to produce MAC frames with different MAC addresses to communicate with serving and target AP.

The rest of the paper is organized as follows. Section 2 describes the system architecture and delays under different handoff scenarios. Section 3 presents the proposed DualMAC approach. Section 4 provides and discusses the simulation results and finally Section 5 concludes this study.

2. System architecture and handoffs in secured WLANs

Fig. 1 illustrates a generic system architecture for real-time communications over secured WLANs. In a secured WLAN infrastructure, a mobile STA first has to associate with an AP and passes the WLAN access control such as the IEEE 802.1x. After an STA is authenticated by an AP and authentication, authorization, and accounting (AAA) server, a master key is distributed from the AAA

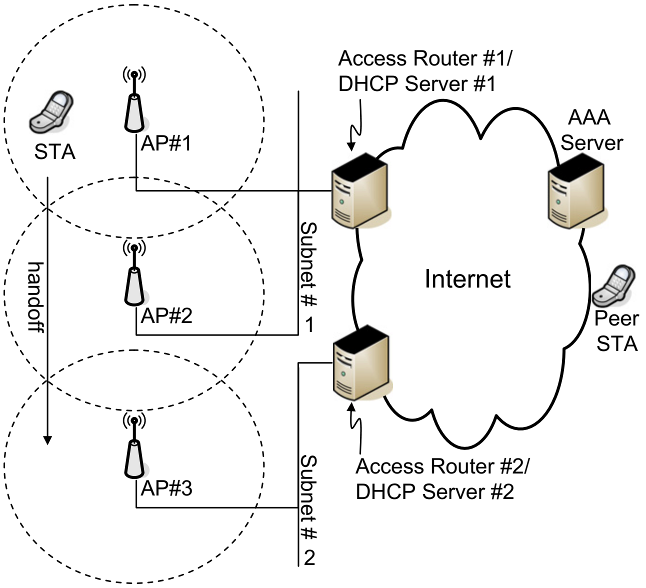


Fig. 1. A generic system architecture for real-time communications over secured WLANs.

server to the AP. The AAA server maintains the subscriber information such as master keys for all STAs and provides authentication, authorization, and accounting functions of STAs for accessing a network. A temporary key is further generated according to the master key and is employed to encrypt and decrypt WLAN link-layer frames. According to the specification defined in the IEEE 802.11i, an STA needs to perform a four-way handshake with the serving AP in order to produce a temporary key, called Pairwise Transient Key (PTK), from the master key, called Pairwise Master Key (PMK). Temporary keys, i.e., PTKs, have to be generated and changed periodically. After WLAN association, access control and encryption key exchange procedures, an STA acquires an IP address through a Dynamic Host Configuration Protocol (DHCP) server, and accesses the Internet. Finally, an STA uses a call setup protocol such as session initiation protocol (SIP) to establish a real-time communication, e.g., a VoWLAN session, with a peer node.

A mobile STA might perform a handoff from the serving to target AP during a communication session. The serving AP is the AP that an STA currently associates, and the target AP is the AP to which an STA is going to handoff. While an STA performs a handoff from the serving to target AP, the procedures comprise a WLAN channel scan to find an AP with the maximal signal strength, the open system authentication, and the association with the target AP. While an STA does not associate with the target AP before, the STA must perform a full IEEE 802.1x authentication. If the STA has previously been associated with the target AP, the IEEE 802.11i suggests three possible procedures [12]. The first possible situation is that an STA repeats the same actions as for an initial association, i.e., a full IEEE 802.1x authentication. The second situation is that the network supports the PMK cache. An STA embeds a list of PMK identifiers (PMKIDs) in the association message, and the AP and STA reuse the cached PMK so that the IEEE 802.1x authentication can be avoided. The third possible situation assumes that an STA pre-authenticates with the target AP before a handoff via the serving AP. From a handoff point of view, the above handoff scenarios can be categorized into a link-layer handoff with a full IEEE 802.1x authentication or without a full IEEE 802.1x authentication. For the pre-authentication or PMK cache that is enabled, a full IEEE 802.1x authentication can be ignored. Otherwise, a full IEEE 802.1x authentication through the target AP is needed during a handoff.

After the authentication procedure, an STA needs to perform a four-way handshake to exchange and install a PTK. If the serving and target AP are in the same subnet, a link-layer handoff is complete after the four-way handshake. If the serving and target AP are in different subnets, the STA further needs to perform network handoff procedures. The procedures are that an STA first acquires an IP address in the new subnet, sends an *SIP RE-INVITE* message to the peer node to update the STA's IP address and resumes the real-time communication. Fig. 2 illustrates message flows and all possible delays during a handoff for a VoWLAN session in secured WLANs. According to the description above, the delay for a link-layer handoff with a full IEEE 802.1x authentication is $T_{\text{scan}} + T_{\text{auth}} + T_{\text{asso}} + T_{\text{full-1x}} + T_{\text{4way}}$. T_{scan}, T_{auth}, T_{asso}, $T_{\text{full-1x}}$, and T_{4way} are the delays for performing scan, authentication, association, full IEEE 802.1x and four-way handshake procedures, respectively. The delay for a link-layer handoff without a full IEEE 802.1x authentication is $T_{\text{scan}} + T_{\text{auth}} + T_{\text{asso}} + T_{\text{4way}}$. The network-layer handoff delay with an IEEE 802.1x full authentication is $T_{\text{scan}} + T_{\text{auth}} + T_{\text{asso}} + T_{\text{full-1x}} + T_{\text{4way}} + T_{\text{L3}}$ and finally the network-layer handoff delay without an IEEE 802.1x full authentication becomes $T_{\text{scan}} + T_{\text{auth}} + T_{\text{asso}} + T_{\text{4way}} + T_{\text{L3}}$. In the above equations, T_{L3} denotes the network-layer delay for acquiring an IP address and performing SIP Re-INVITE procedures.

3. The DualMAC mechanism

The basic concept behind the proposed DualMAC mechanism is to configure two MAC addresses in a single WLAN interface. The mechanism can be implemented in the MAC firmware. An STA with the DualMAC mechanism uses different MAC addresses to communicate with the serving and target AP. Hence, an STA can switch between serving and target AP and maintain both link-layer and network connections with the two APs simultaneously during a handoff. The reason why two MAC addresses are used is that an STA is automatically de-associated with the serving AP once the STA uses the same MAC address to associate with the target AP. An MAC address of an STA can only appear in one AP in a subnet.

The proposed mechanism enables an STA to associate with the serving and target AP simultaneously. More specifically, an STA has a real-time communication session, and real-time packets are generated periodically, e.g., 10–30 ms for a VoIP session. An STA usually spends a short period, called a duty cycle, to transmit and receive uplink and downlink packets periodically, and stays idle before the next packet exchanges. Therefore, an STA gains a period of free time, called a sleep cycle, between two packet exchanges. Fig. 3 shows a timing diagram for uplink and downlink VoIP packet exchanges according to the PS-Poll transmission scheme presented in [13]. The PS-Poll transmission scheme adopts the power saving mode (PSM) defined in the IEEE 802.11 standard to transmit and receive voice packets in WLANs. According to the PS-Poll transmission scheme, an STA first notifies the WLAN AP to enter the PSM, and then stays in the WLAN doze state. If an STA has an uplink voice packet to transmit, it wakes up and sends the packet. After receiving the acknowledgement frame from the AP for the uplink voice packet, the STA sends a PS-Poll frame to retrieve the downlink voice packet buffered on the AP. Finally, the STA receives and acknowledges the downlink voice packet.

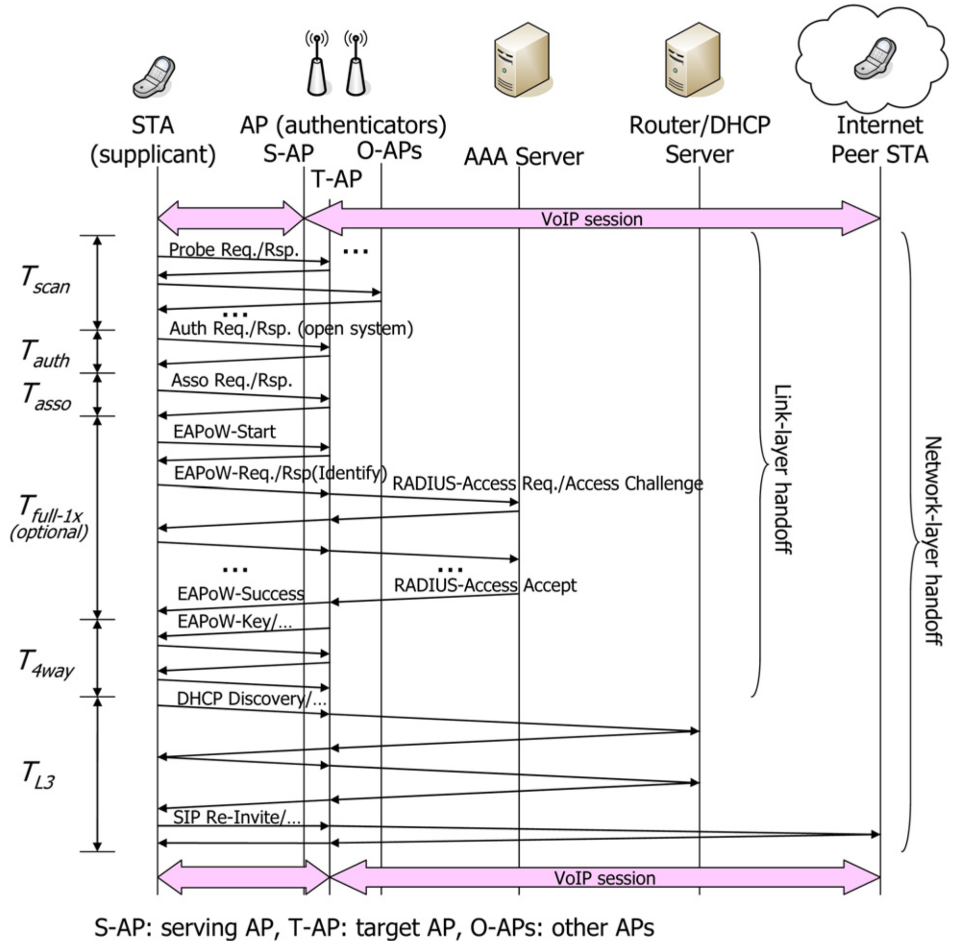


Fig. 2. A message flowchart and possible handoff delays for a VoWLAN session in secured WLANs.

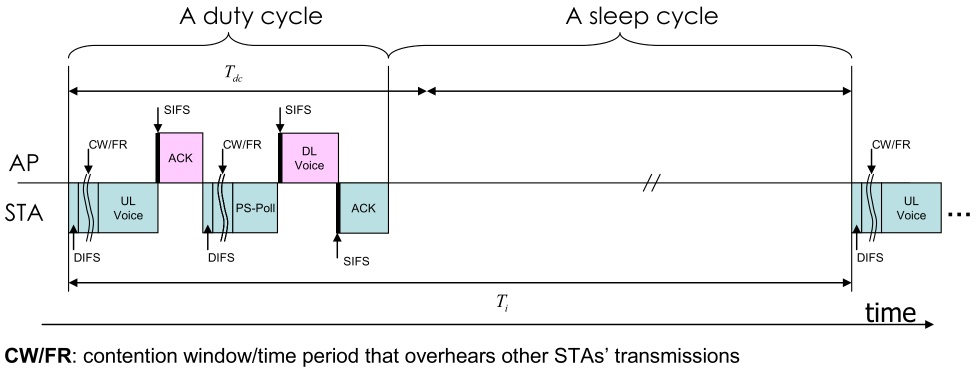


Fig. 3. The PS-Poll transmission scheme for voice packets over WLAN.

There is another similar transmission scheme for real-time communications in WLAN, called automatic power saving delivery (APSD) which is defined in the IEEE 802.11e.

In this work, we assume that either the PS-Poll transmission or ASPD transmission is implemented so that there are sleep cycles between every packet exchange. Assume that uplink and downlink real-time packets are generated periodically, say T_{i}. An STA spends the length of a duty cycle, defined as T_{dc}, in transmitting uplink and downlink packets in each period. Then, an STA has $T_{\mathrm{i}} - T_{\mathrm{dc}}$ spare time, i.e., a sleep cycle, in every packet exchange period, and an STA can use sleep cycles to switch to other channels and perform WLAN scan, association, the IEEE 802.1x authentication and four-way handshake with APs. Thus, a soft handoff that minimizes packet loss and service disruption time for a real-time communication can be achieved. Detailed procedures are described in the next subsections.

3.1. Link-layer handoff procedures before associating with the target AP

When the signal strength of the serving AP is lower than a pre-defined threshold, handoff is activated. The first step of the handoff procedure is to measure the signal strength from other APs. Unlike SyncScan which utilizes passive scan and requires the infrastructure support, our proposed method suggests an STA-centric active scan approach. Conventional active scan approaches usually pause packet transmission with the serving AP, scan all channels completely, and then resume the transmission with the serving AP. Our proposed active scan method suggests the STA to perform a channel hopping and scan only one channel during a sleep cycle. In order words, the proposed method separates active scans of neighboring channels and multiplexes the packet transmission with serving AP and active scans. Fig. 4 shows an active scan example during a VoWLAN session. While a VoIP STA completes its uplink and downlink transmissions with the serving AP, say at the WLAN channel 1 (CH1), the STA switches and scans the other channel, say the WLAN channel 6 (CH6), during a sleep cycle. The STA switches from the CH1 to the CH6, sends a probe request and waits for probe responses from APs in the CH6. After a waiting period, the STA switches back to the CH1 to receive real-time packets again. The period that an STA can stay in the other channel is $T_i - T_{dc} - 2 \times T_s$, where T_s denotes the channel switching time for a WLAN interface. For an active scan, two parameters are configured, i.e., the maximal channel time, $T_{max\_ ch}$, and the minimal channel time, T_{min_ch}. The minimal channel time is the minimal waiting time for a probe request without getting any probe response. If an STA receives at least one probe response from APs before the minimal channel time, an STA must wait for the maximal channel time in order to collect all APs' responses in the same channel. Since an STA must stay in the scanned channel for at least T_{min_ch} or T_{max_ch} if it receives a response, packet delays are introduced if the length of a sleep cycle is less than the minimal or maximal channel time. The delay for real-time packets during a scan period is $(T_{dc} + 2 \times T_s + T_{max\_ch}) - T_i$ or $(T_{dc} + 2 \times T_s + T_{min\_ch}) - T_i$. In other words, an STA has to stay in the scanned channel, completes a single channel scan procedure, and can switch back to the serving AP to receive and transmit packets. Fortunately, the length of a sleep cycle is long enough to scan at least one channel without introducing packet delays if the inter-packet arrival, i.e., T_i, is more than 20 ms according to the measurement and investigation in [1,8]. For the case that an STA completes a scan in one channel and still has time in the sleep cycle, an STA may use one sleep cycle to scan multiple channels. By applying this scan strategy, WLAN scan procedures can be performed in the background without blocking a real-time communication session.

Since an STA does not associate with any WLAN AP during a scan phase, an STA can use the same MAC address used in the serving AP to send *Probe Request* messages. After an STA decides on an AP for handoff, the STA performs open authentication and association with the target AP also during sleep cycles. Different from the scan phase, an STA should use a different MAC address to associate with the target AP. To use two different MAC addresses to communicate with the serving and target AP maintains both connections with the two APs simultaneously. During the association, an STA also informs the target AP that the STA is in PSM. Then, the target AP starts to buffer the messages and packets to the STA after the association. Our experiments indicate that after APs accept the PSM associations from STAs, they start to buffer the messages sent to the STAs whether the STAs pass the IEEE 802.1x authentication or not. It is important to note that before the association, the target AP does not buffer messages sent to an STA. An STA must send the request message and wait for the response in the same sleep cycle. Packet delay may be introduced if an STA cannot switch back from the other channel to the serving channel on time. After the association, the target AP buffers the messages sent to an STA in PSM, and then an STA can then send request messages in one sleep cycle and retrieve the response messages in the subsequent sleep cycles. This property enables request and response messages between APs and STAs to be performed in separated sleep cycles.

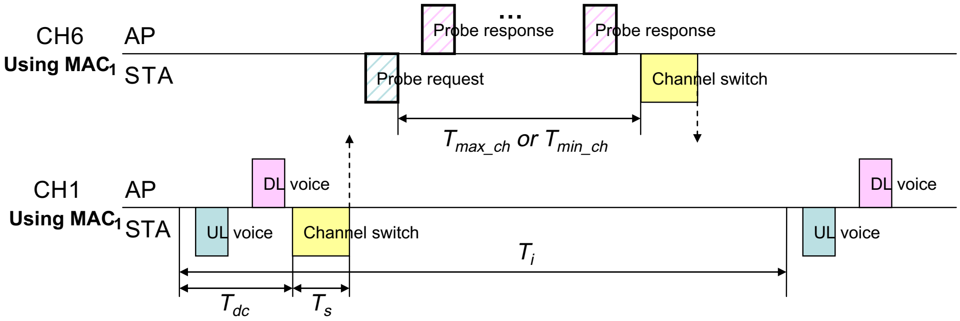


Fig. 4. Handoff procedures and message exchanges before associating with the target AP (a WLAN scan example).

3.2. Link-layer handoff procedures after associating with the target AP

After an STA associates with the target AP using a different MAC address, the IEEE 802.1x authentication is activated if necessary. Different from the situation before an STA associates with the target AP, the target AP starts to buffer messages sent to the STA. Then, request and response messages can be exchanged in separated sleep cycles. That is, an STA can send a request message to the target AP in one sleep cycle and retrieve the response message from the target AP in the next sleep cycle. Notably, an STA must actively retrieve the response messages from the target AP using the PS-Poll mechanism since the target AP presumes that the STA is staying in the PSM. The maximal duration that an STA can stay in the channel of the target AP without introducing packet delays is $T_i - T_{dc} - 2 \times T_s$. Fig. 5 shows an example where an STA actively retrieves the messages from the target AP, and performs a four-way handshake with the target AP using a different MAC address. An STA thus uses sleep cycles to complete a full IEEE 802.1x authentication and the IEEE 802.11i four-way handshake. Since an STA uses a different MAC address to associate with the target AP, the AP sees the STA as a different STA. Fortunately, this design does not introduce problems in the IEEE 802.1x and IEEE 802.11i procedures. In the IEEE 802.1x, STAs are normally authenticated by their accounts not their MAC addresses. If the MAC address information is required during the authentication phase, the AAA server must configure the two MAC addresses associated with the same STA into the database. According to the specification defined in the IEEE 802.11i, the PMK, AP's MAC address, and STA's MAC address are used to generate PTKs. Therefore, STAs can produce PTKs by using the new MAC address without any problem. Depending on network deployment and configuration, people may turn on AP's MAC filter function which does not allow the association from unauthorized MAC addresses. In this case, the two MAC addresses which belong to an STA need to be configured into the MAC filtering database.

After authentication and encryption key establishment procedures are complete, an STA either sends an ARP request message to update the MAC address to IP address mapping tables in the STAs in the subnet, or any outgoing packets from the STA automatically updates the mapping tables in the STAs in the subnet. After the ARP update, packets are sent to the STA via the target AP. The STA interchanges its two MAC addresses during handoffs in different APs. The idea can be also extended to multiple MAC addresses to associate with multiple APs. The proposed DualMAC mechanism utilizes two MAC addresses to implement a soft handoff mechanism without introducing packet loss and service disruption for real-time communications in a secured WLAN environment.

3.3. Network handoff procedures

If the serving and target AP are in the same subnet, an STA resumes the real-time communication with the peer node after a link-layer handoff. If an STA moves to the target AP in a new subnet, the STA further needs to perform network handoff procedures. In this study, SIP mobility is adopted for the mobility management for real-time communications. In this situation, an STA acquires a new IP address from a DHCP server in the new subnet and sends a *SIP RE-INVITE* message to update the IP address in the peer node so that the real-time communication resumes. Since the two APs are simultaneously connected by applying the DualMAC mechanism, an STA can complete all network handoff procedures through the target AP using sleep cycles while exchanging real-time packets through the serving AP at the same time. Therefore, the services disruption time and packet loss during a network-layer handoff is also minimized.

4. Simulation results

To evaluate the performance of the proposed DualMAC mechanism, an experimental environment for real-time communications over secured WLANs was first established in our campus network. A WLAN interface card using Intersil PRISM GT chip is installed on a notebook which serves as a mobile STA, and APs that support the IEEE 802.1x and IEEE 802.11i are used. An AAA server using freeRADUIS [14] and DHCP server are also configured in the experimental environment. Ethereal and Airopeek are employed to monitor and record the packet exchanges over LAN and WLANs, respectively [15,16]. IxChariot, a network traffic generator, is running on the mobile STA and an Internet node to generate voice packets for a VoWLAN session [17]. The voice traffic that IxChariot generates

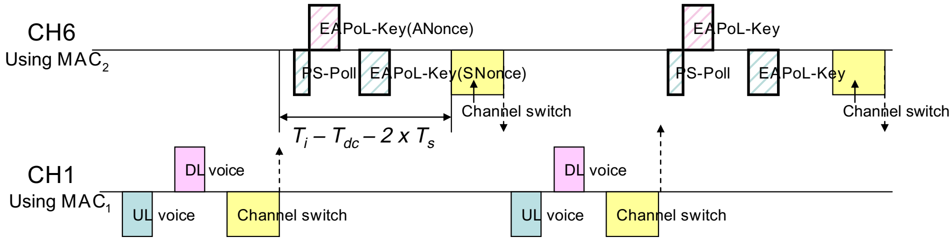


Fig. 5. Handoff procedures and message exchanges after associating with the target AP (a four-way handshake example).

is constant bit rate (CBR) G.711 voice packets in 64Kbps without silence suppression. An automatic testing program running on the mobile STA was then written to generate the WLAN association, the IEEE 802.1x authentication based on Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) and the IEEE 802.11i encryption key exchanges. Complete handoff transactions are logged and all packets during handoffs including the content of the packet and the timing information of the packets over LAN and WLAN are all recorded. A total of 100 tests for a network-layer handoff with a full IEEE 802.1x authentication and another 100 tests for a network-layer handoff without a full IEEE 802.1x authentication are logged. Duplicated address detection (DAD) procedures after a new IP address is configured on the STA are turned off in all tests. These measurement and experiment logs are fed to our simulation program which is written in C language to evaluate the delays, packet loss, and service disruption time for a real-time communication during handoffs. Table 1 summarizes the measurement results and the parameters used for the simulations.

Fig. 6 shows an example of packet delays and service disruption for a network-layer handoff with a full IEEE 802.1x authentication when the DualMAC is not employed. As can be seen, a service disruption of about 1.3 s occurs. The 1.3 s service disruption is due to the link-layer and network-layer handoff procedures. By applying the proposed DualMAC mechanism, the service disruption for the VoWLAN session is significantly reduced. Simulation results show that there is no voice packet loss during handoff, but packet delays may be introduced. An example is shown in Fig. 7. As can be seen, although some packet delay occurs, all voice packets during a handoff period can still be received and transmitted within 50 ms. The figure also indicates that during the initial stage of a handoff, the packets suffer from delays. This is because before the WLAN association, an STA that sends a request message must stay in the other channel to wait for the response according to the DualMAC mechanism, and delays for receiving and transmitting packets may be introduced. The packet delays occur during WLAN scan, open system authentication, and WLAN association procedures. After the association procedure, the target AP starts to buffer the response messages to an STA. An STA can defer the process of the response messages in the target AP, and process the packet transmission on the serving AP first without introducing packet delays. Fig. 8 further illustrates the packet delay distribution during a handoff period for the proposed DualMAC mechanism. All packets delays during the handoff periods for the 100 handoff experiments are counted. Fig. 8 demonstrates that less than 35 ms delay is introduced for about 25% voice packets and about 35 ms to 40 ms delay is introduced for 75% voice packets during the handoff periods. Although packet delays are introduced during a handoff, packet delays are within 50 ms and can be acceptable for real-time applications such as VoIP services.

Finally, Tables 2 and 3 summarize the average and standard deviation for handoff duration and service disruption time of a real-time communication for a G.711 VoWLAN session under different handoff scenarios. Table 2 lists the individual duration for each handoff procedure. As can be

Table 1
Measurement results and simulation parameters

Parameters	Values
Maximal channel time ($T_{\text{max\_ch}}$) (ms)	11
Minimal channel time ($T_{\text{min\_ch}}$) (ms)	7
Number of channels to scan	11
Number of channels with APs (Channels 1, 6, and 11)	3
Channel switch time (T_s) (ms)	5
Average VoIP inter packet arrival time (T_i) based on G.711 (ms)	20
Average duty cycle (T_{dc}) (ms)	2
Average open system authentication delay (T_{auth}) (ms)	0.9
Average association delay (T_{asso}) (ms)	1.1
Average full IEEE 802.1x authentication delay ($T_{\text{full-1x}}$) (ms)	539.5
Average IEEE 802.11i four-way handshake delay (T_{4way}) (ms)	16.30
Average DHCP and SIP Re-INVITE delay (T_{L3}) (ms)	630

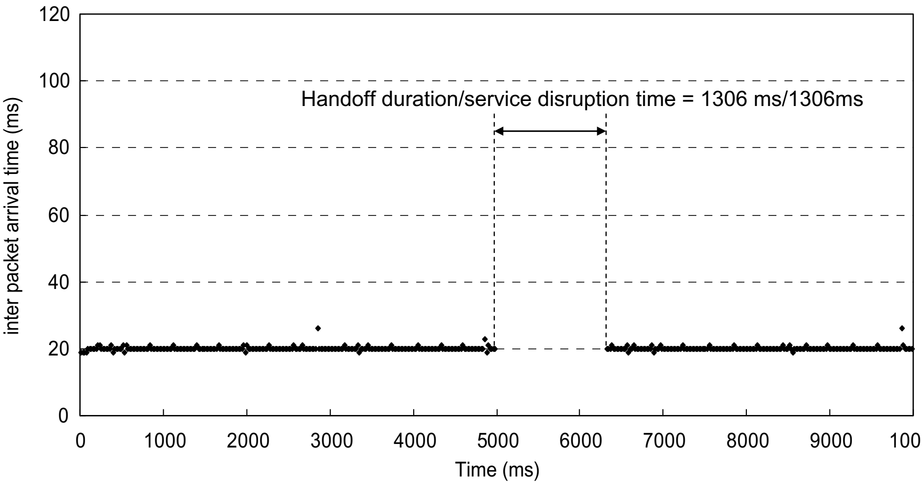


Fig. 6. An example of a network-layer handoff with a full IEEE 802.1x authentication for a VoWLAN session when the DualMAC is not employed.

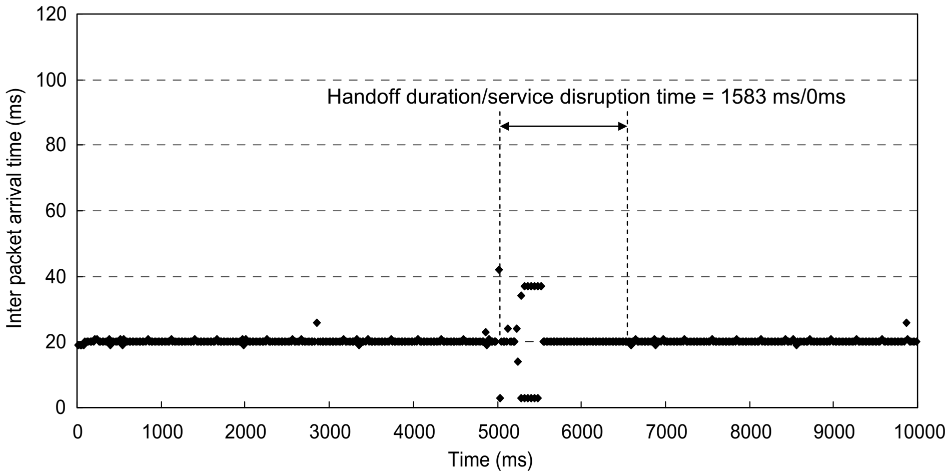


Fig. 7. An example of a network-layer handoff with a full IEEE 802.1x authentication for a VoWLAN session when the DualMAC is employed.

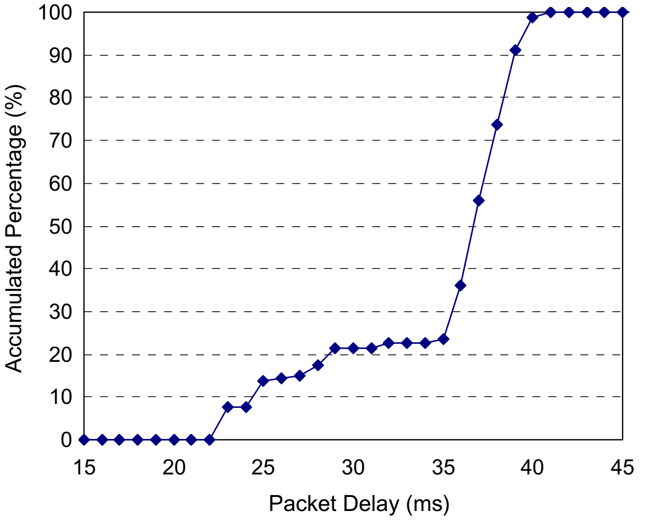


Fig. 8. Distribution of voice packet delays during handoffs when the DualMAC is employed.

Table 2
Average duration and standard deviation for each handoff procedure

Duration of each handoff procedure	Conventional single MAC approach		The proposed DualMAC approach	
	Average (ms)	Standard deviation	Average (ms)	Standard deviation
Active scan	144.00	0.00	227	0.00
Open system authentication	1.46	0.04	14.52	0.04
(Re)-association	2.09	0.08	15.00	0.08
Full IEEE 802.1x authentication	542	3.63	598.68	4.43
IEEE 802.11i four-way handshake	22.18	0.16	32.14	0.07
DHCP and SIP Re-Invite (without DAD)	636.92	4.48	699.92	1.56

Table 3
Handoff duration and service disruption time for different handoff scenarios and configurations

Handoff categories	Handoff duration		Service disruption time	
	AVG (ms)	STD	AVG (ms)	STD
Link-layer handoff with a full IEEE 802.1x authentication				
Without DualMAC	711.36	0.23	711.36	0.23
With DualMAC	887.34	0.19	0	0
Link-layer handoff without a full IEEE 802.1x authentication				
Without DualMAC	170.52	0.25	170.52	0.25
With DualMAC	288.66	0.12	0	0
Network-layer handoff with a full IEEE 802.1x authentication				
Without DualMAC	1349.51	4.23	1349.51	4.23
With DualMAC	1586.92	1.80	0	0
Network-layer handoff without a full IEEE 802.1x authentication				
Without DualMAC	802.46	4.05	802.46	4.05
With DualMAC	1000.42	1.59	0	0

seen, the proposed DualMAC approach always introduces longer duration than the previous single MAC approach. That is because the proposed DualMAC approach has to perform the message exchanges with the target AP during sleep cycles without blocking the real-time connections with serving AP. Therefore, an STA has to switch between serving and target AP in order to transmit and receive the real-time packets and exchange messages in parallel. Therefore, the handoff duration increases. It is important to note that a longer duration of each handoff procedure does not imply a longer service disruption time. For the proposed DualMAC approach, although the duration of each handoff procedure increases, the VoIP session through the serving AP is still maintained, and voice packets are not lost. In Table 3, the handoff duration and service disruption time for different handoff categories are further listed. As seen from the table, the previous single MAC approach introduces less handoff duration, but the packets sent to the serving AP are lost during the handoff. On the other hand, the proposed DualMAC spends 25–70% and 17–25% more handoff time for a link-layer and network-layer handoff, respectively; without disrupting the real-time service. The proposed DualMAC realizes a soft handoff mechanism for real-time communication over secured WLANs.

5. Conclusions

In this study, a pure STA-side approach which only requires the firmware upgrade on mobile STAs without modifying WLAN infrastructures and the IEEE 802.11 standard was proposed. The proposed DualMAC utilizes a time division duplex concept to maintain connections with the serving and target AP simultaneously using two MAC addresses. Thus, a soft handoff between WLAN APs can be achieved. Simulation results demonstrate that although the durations of a link-layer and network-layer handoff increase 25–70% and 17–25% respectively by applying the proposed mechanism, the packet loss and the service disruption for real-time communications during handoffs are both avoided.

Acknowledgements

The authors would like to thank the MediaTek-NCTU (National Chiao Tung University) research center for financially supporting this research.

References

[1] A. Mishra, M.H. Shin, W.A. Arbaugh, An empirical analysis of the IEEE 802.11 MAC layer handoff process, ACM Computer Communications Review 33 (2) (2003) 93–102.

[2] R. Chandra, P. Bahl, P. Bahl, MultiNet: connecting to multiple IEEE 802.11 networks using a single wireless card, in: Proceedings of IEEE Infocom 2004, Hong Kong, March 7–11, 2004.

[3] M.H. Shin, A. Mishra, W.A. Arbaugh, Improving the latency of 802.11 handoffs using neighbor graphs, in: Proceedings of the Second International Conference on Mobile Systems, Applications and Services, 2004.

[4] A. Mishra, M.H. Shin, W.A. Arbaugh, Context caching using neighbor graphs for fast handoffs in a wireless network, in: Proceedings of the 23rd Conference on Computer Communications (Infocom), March, 2004.

[5] A. Mishra, M.H. Shin, N.L. Petroni Jr., T.C. Clancy, W.A. Arbaugh, Proactive key distribution using neighbor graphs, IEEE Wireless Communications 11 (2004).

[6] C.-C. Tseng, L.-H. Yen, H.-H. Chang, K.-C. Hsu, Topology-aided cross-layer fast handoff designs for IEEE 802.11/mobile IP environments, IEEE Communications (2005) 156–163.

[7] J. Chan, B. Landfeldt, A. Seneviratne, P. Sookavatana, Integrating mobility prediction and resource pre-allocation into a home-proxy based wireless internet framework, in: 2000 IEEE Conference on Nettworks, ICON2000, Singapore, pp. 18–23.

[8] I. Ramani, S. Savage, SyncScan: practical fast handoff for 802.11 infrastructure networks, in: Proceedings of the IEEE Infocom Conference, Miami, March, 2005.

[9] V. Brik, A. Mishra, S. Banerjee, Eliminating handoff latencies in 802.11 WLANs using multiple radios: applications, experience, and evaluation, in: Internet Measurement Conference 2005, October, 2005.

[10] IEEE 802.11r, Part 11: Wireless medium access control (MAC) and physical layer (PHY) specifications: Amendment 2: Fast BSS Transition, Draft 1.

[11] IEEE 802.11k, Part 11: Wireless medium access control (MAC) and physical layer (PHY) specifications: Amendment 9: Radio Resource Measurement, Draft 3.

[12] IEEE 802.11i, Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

[13] Y. Chen, N. Smavatkul, S. Emeott, Power management for VoIP over IEEE 802.11 WLAN, IEEE Wireless Communications and Networking (WCNC) (2004).

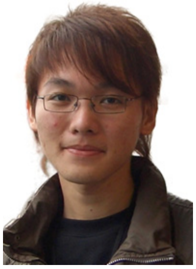
[14] freeRADIUS. Available from: <http://www.freeradius.org/>.

[15] Ethereal. Available from: <http://www.ethereal.com/>.

[16] AiroPeek. Available from: <http://www.wildpackets.com/products/airopeek/overview>.

[17] IxChariot. Available from: <http://www.ixiacom.com/>.

Shiao-Li Tsao received B.S., M.S., and Ph.D. degrees in engineering science from National Cheng Kung University, Taiwan, in 1995, 1996 and 1999 respectively. His research interests include mobile communication and wireless network, embedded software and system, and multimedia system. From 1996 to 1997, he was a research assistant of Institute of Information Science, Academia Sinica. He visited Bell Labs, Lucent technologies, NJ, USA, in the summer of 1998. From 1999 to 2003, Dr. Tsao joined Computers and Communications Research Labs (CCL) of Industrial Technology Research Institute (ITRI) as a researcher and a section manager. Dr. Tsao is currently an assistant professor of computer science of National Chiao Tung University. Prof. Tsao has published more than 50 international journal and conference papers, and has held or applied 14 US, 3 Germany, 16 R.O.C. patents. Prof. Tsao received the Research Achievement Awards of ITRI in 2000 and 2004, the Outstanding Project Award of Ministry of Economic Affairs (MOEA) of R.O.C. in 2003, the Advanced Technologies Award of MOEA of R.O.C. in 2003, and the Research Paper Award of ITRI in 2002. He is a member of IEEE and IEEE ComSoc.



Pang Hsiang Lo received M.S. degrees in computer science and information engineering from National Chiao Tung University, Taiwan, in 2006. His research interests include mobile networks and communications, and embedded software.