國立交通大學

資訊科學與工程學系

碩士論文

DualMAC：安全無線區域網路中即時通訊之軟換手機制

DualMAC: A Soft Handoff Mechanism for Real-Time Communications in Secured WLANs

研究生：羅邦翔

指導教授：曹孝櫟 教授

中華民國九十五年七月

DualMAC：安全無線區域網路中及時通訊之軟換手機制

DualMAC: A Soft Handoff Mechanism for Real-Time Communications in Secured WLANs

研 究 生：羅邦翔　　Student：Pang-Hsiang Lo

指導教授：曹孝櫟　　Advisor：Shiao-Li Tsao

國立交通大學
資訊科學與工程學系
碩士論文

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

Computer Science

July 2006

Hsinchu, Taiwan, Republic of China

中華民國九十五年七月

DualMAC：安全無線區域網路中即時通訊之軟換手機制

學生：羅邦翔　　　　指導教授：曹孝櫟

國立交通大學資訊工程學系（研究所）碩士班

摘要

近幾年來，無線區域網路被廣泛地佈建於私人及公眾場合，已成為最重要的無線存取技術之一。然而在無線存取點之間進行切換的換手過程中，將造成通訊的中斷而對即時通訊服務的服務品質產生嚴重的影響，因此有相當多的研究已經著力於減少此換手延遲時間。然而目前現存的解決方案中，大部分的方法都未考慮在安全的無線網路下進行換手或是需要仰賴後端骨幹網路的支援，對於現階段的已佈建好的無線區域網路環境來說，作全面的更新以及升級將會有其難度。

在這篇研究中，我們提供了一個創新的設計，僅需要在使用者端做更新而不仰賴後端網路的方法。我們使用兩個媒體存取控制位址， 以分時雙工的方式同時進行即時通訊服務以及換手的連線步驟。在模擬結果中，在安全控制開啟的無線網路中，使用我們的方法可以在不影響原先即時通訊的原則下，進行無縫式的換手。

DualMAC: A Soft Handoff Mechanism for Real-Time Communications in Secured WLANs

Student: Pang-Hsiang Lo Advisor: Shiao-Li Tsao

Institute of Computer Science and Engineering
College of Computer Science
National Chiao Tung University

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.

致謝

在此我首先要感謝我的指導教授，曹孝櫟老師。在思考研究方向的過程中，老師給了我很大的幫助，讓我慢慢的釐清問題，不致於迷失方向；而在論文寫作的技巧上，老師也提供了很多架構上的建議，並且不厭其煩地為我作英文寫作方面的指導。很感謝老師總是在我遇到困難的時候，給我持續下去的勇氣，讓我可以完成這一篇論文。

接下來要感謝博士班建明學長、一正學長以及海倫學姐給我實作上的建議，並且不吝惜地在學業及研究等各方面教導我。同時也感謝實驗室同學君豪、宥霖、雅聯、凱翔、金璋以及中暉、誌謙等學弟們給我的支持與鼓勵，讓我在學習的過程中，仍然能保持著對研究的熱誠。

最後要感謝我的家人對我精神上的鼓勵，讓我能夠專心的在兩年內完成研究工作。謹以此論文，獻給我最摯愛的家人 。

目錄

圖目錄

表目錄

I. 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. 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 [1]. 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 messages from APs for a passive scan. Experiments indicate that an STA may spend up to several hundred milliseconds for an active scan, and a scan introduces considerable delay and service disruption for a real-time communication. Ramani et al. 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 [8].

For WLANs whose access control mechanism such as the IEEE 802.1x [13] and link-layer encryption function such as the IEEE 802.11i [11] 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. 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 [5]. This idea is also adopted in the newly established 802.11 working group, the IEEE 802.11r, for fast base-station switching [9]. 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 802.11r and 802.11k [9][10], 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 standard 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.

To use a 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. In Section II, the background technologies of handoffs in a secured WLAN infrastructure are introduced. Section III IV presents the proposed DualMAC approach. Section IV discusses the experimental and simulation results. and finally, conclusions are made in Section V.

II. Background

A. 802.11 Single Station Association

The IEEE 802.11 specifies that each STA may associate with a single AP at any given time. The single station association ensures that there is only one attachment point from the STA to the distribution system (DS) and prevents the path ambiguity problem. The IEEE 802.11f inter access-point protocol (IAPP) [12] has provided operations between the APs to assistant the maintenance of the association relationship on APs during handoffs. When a STA changes its association from one AP to another by performing a *re-association*, the target AP should send an IAPP MOVE-notify packet to the old AP, Reception of the packet causes the old AP to remove the association state for the specified MAC address. Moreover, it forwards any stored context to the target AP to facilitate a fast context exchange. Therefore, the target AP can resume the previous communication settings without any advanced negotiation.

When a roaming STA performs an association rather than a reassociation, the target AP enforces the single station association by sending an IAPP ADD-notify packet to the multi-cast address. Reception of the packet causes the removal of the association state and any context information stored for the specified STA. However, the context forwarding is not required for the association case. Both the operations remove the stale association information according to the STA's MAC address.

B. 802.11i: The MAC Security Enhancements

Due to the weakness of 802.11 wired equivalence private (WEP) and its authentication, the IEEE Task Group i (TGi) which has already finalized in 2004 aims to solve this problem. The goal of TGi is to construct a robust wireless environment called robust security network (RSN), where the wireless transmission is protected with stronger cryptographic algorithms and keying materials which are dynamically produced by a key management protocol. The enhanced components of the IEEE 802.11i are categorized as follows:

1. *Data confidentiality and integrity*: In data privacy, there are two cryptographic algorithms developed for encryption enhancement: Temporal Key Integrity Protocol (TKIP) and Counter Mode/ CBC-MAC Protocol (CCMP). TKIP is an optional algorithm for backward compatible to pre-RSN equipments, and is an extension version of WEP which uses RC4 stream cipher. On the other hand, CCMP is a mandatory algorithm for

robust security network association (RSNA)-capable devices. It uses AES block cipher to provide a stronger encryption. Both TKIP and CCMP support data authentication for integrity confirmation.

2. *802.1x Authentication*: The IEEE 802.11i utilizes the IEEE 802.1x as its authentication framework, which provides port-based network access control for the IEEE 802 LANs. The purpose of the IEEE 802.1x is to provide compatible mechanisms for devices those request MAC layer authentication or authorization services. Port-based access control enforces an authentication each time while the devices are attached to a network. The *port* here means a logical attachment to the LAN, for example, a 802.11 association or an ethernet port. In this architecture, three entities are introduced: *supplicant*, *authenticator*, and *authentication server*. Their definition and functionality are described as follows:

   - Authenticator: An entity that facilitates the access control and authentication of any entities on the other end of the network segment. For example, wireless APs may act as an authenticator, which provides port-based access control for mobile STAs under the same basic service set (BSS).
   - Supplicant: An entity at one end of a segment which is willing to access the resources on the other end. It should be authenticated by an authenticator, or the traffics will be blocked at the authenticator. For example, the mobile STAs.
   - Authentication Server (AS): An entity that provides authentication services for the authenticator. The centralized architecture reduces the authentication overhead at the authenticator, and provides more flexibility to add new authentication methods.

For a supplicant that wants to access network resources, an extensible authentication is enforced at the authenticator just after it is attached to the LAN. Before a successful authentication is performed, any packet from the unauthorized supplicant will be discarded at the authenticator, except the authentication packets. During the authentication, the authenticator acts as a bridge between the supplicant and AS. It blocks unauthorized packet and forward authentication packets to and from a preconfigured AS. (Note: authenticator and AS may reside on the same machine, but they are always connected with network). After the AS proves the identity of the supplicant, it notifies the authenticator to open the authorized port for supplicant. Therefore, any packet from the supplicant can pass through the authenticator without port blocking.

In the IEEE 802.1x framework, there are two protocols used for transportation of authentication messages between supplicant and AS: the extensible authentication protocol (EAP) and remote authentication dial in user service (RADIUS). EAP is originally developed for authentication on point-to-point protocol (PPP) links. The LAN encapsulation of EAP packets, called EAP over LAN (EAPoL), is introduced to facilitate the transportation between supplicant and authenticator. RADIUS protocol is always used by Internet service providers (ISPs) to provide centralized authentication services. It is used by the IEEE 802.1x for the transportation between authenticator and AS. During the authentication, the authenticator is responsible for translating the encapsulation between EAPoL and RADIUS, accordingly. Both protocols provide flexibility for well-known authentication methods. Figure 1 shows the relationships and communication protocols between the supplicant, authenticator, and AS.

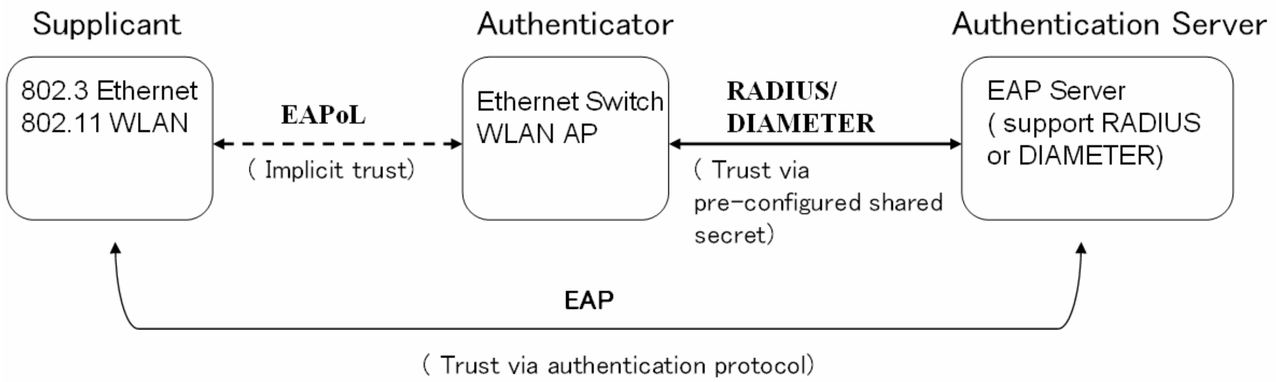

Figure 1. The relationship and trust model between the IEEE 802.1x entities. (Dotted line means implicit trust)

For each authentication, the authenticator maintains the authorization state for each supplicant for a while, which is identified by their MAC addresses After the state information expires, the supplicant is forced to perform a re-authentication again, even it resides under the same authenticator. Authorization status should be updated periodically due to a timeout of the authenticator or a RADIUS session-timeout of the AS.

3. *Key management protocol*: Due to the weakness of static keying in WEP, two protocols for dynamic key management are proposed in the IEEE 802.11i: the four-way handshake and group key handshake. Both protocols use the pairwise master key (PMK) as a basic secret, which is produced by a master key (MK) from a successful 802.1x authentication, to construct the keying materials for wireless transmission. Handshake details are described as follows.

   - Four-way handshake: Four-way handshake is a procedure to refresh the pairwise transient key (PTK) which is used for protecting unicast traffics. PTK is a set of keying materials containing the cryptographic keys for secure handshake and data transmissions, including the temporal key (TK), EAPOL-key confirmation key (KCK), and EAPoL-key encryption key (KEK). Handshaking messages are encapsulated using 802.1x EAPoL-Key format, and are protected against the Man-in-the-middle attack. Handshake massage flow is depicted below. Firstly, the authenticator starts to send a random nonce, called *ANonce*, to supplicant. After receiving the message, the supplicant produces another random nonce, called *SNonce*. The two random nonce and shared PMK are then used to produce the PTK. After that, the supplicant replies message 2 with *SNonce* to the authenticator which is protected by MIC. The authenticator produces the PTK in the same way as the supplicant., and verifies the MIC. If it proves, the authenticator sends message 3 to notify the installation of PTK, otherwise, the handshake halts. Finally, the supplicant replies message 4 to confirm the installation of PTK. As a result, new keying materials are synchronized and used by both the supplicant and authenticator.

- Group key handshake: Group key handshake is a procedure to refresh the group transient key (GTK) which is used for protecting broadcast traffics. It utilizes the PTK for secure handshaking, so it should be performed after a four-way handshake. At the beginning, the GTK is generated by the authenticator, and then sent from the authenticator to supplicant encrypted using KEK After the receiving of the message, the supplicant checks its integrity. If it is really originated from the authenticator without any alternation, the supplicant uses the same KEK to decrypt it and get the GTK. Group key handshake is an optional procedure since the broadcast messages are always less important.

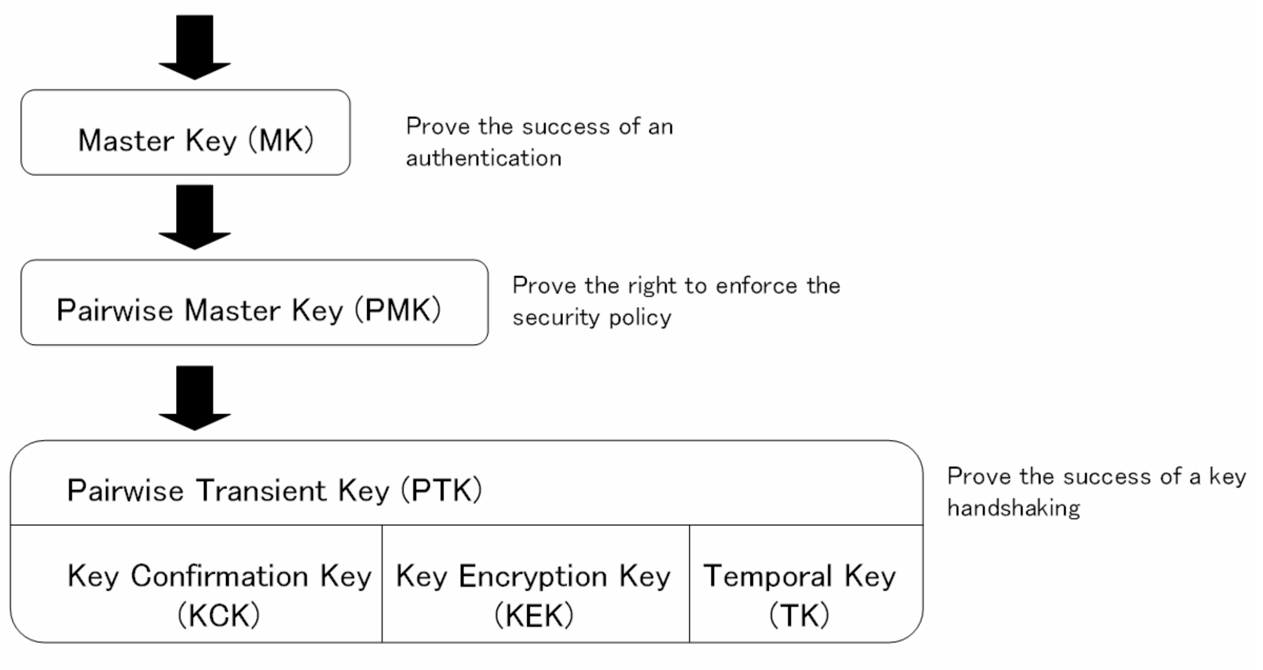
Master Key (MK)
Prove the success of an authentication
Pairwise Master Key (PMK)
Prove the right to enforce the security policy
Pairwise Transient Key (PTK)
Prove the success of a key handshaking
Key Confirmation Key (KCK)
Key Encryption Key (KEK)
Temporal Key (TK)

Figure 2. Key hierarchy of MK, PMK, and PTK

Dynamic key management protocols are performed based on a shared PMK between the supplicant and authenticator. However, not all of the authentication methods provide key derivation function to produce a shared secret. Therefore, the IEEE 802.11i has recommended that supplicants those are willing to create a robust security network association (RSNA) should perform an authentication method that support key devirition. (e.g. EAP-TLS, EAP-SIM, …). Figure 2 shows the PTK key hierarchy and its root secret.

C. Handoffs in IEEE 802.11i Networks

As soon as the handoff condition holds, STA initiates a decision to select the target AP and starts the handoff. The following steps are required for creating an association in a secured WLAN. The latencies of each step are showed in Table 1.

1 802.11 scan: The discovery of available APs from different channels.

2 802.11 authentication: The basic authentication method provided by IEEE 802.11 APs, including the open system authentication and shared-key authentication. However, both are proved to be insecure.

3 802.11 (re-)association: Establish a radio link with the target AP..From now on, AP provides the bridging services between the associated STA and DS.

After the STA attaches to the DS, a basic security should be produced between STA and AP for the dynamic key protocols. There are two ways to exchange such a fresh context, and are depicted as 4(a) and 4(b) respectively. 4(a) shows the first way which produces the context based on a master secret which generated from an extensible authentication method. A successful authentication always produces a master secret between the STA and AS. The master secret can be used to generate a root PMK on both the supplicant and AS. The root PMK is then sent from the AS to an authenticator to enforce the policy decisions. Therefore, AP that possesses the shared PMK can perform a key handshake with the STA. Since a full authentication is always time-consuming, 4(b) takes another approach. Shared context between STA and new AP are produced from a previous PMK instead of a new master secret. The old AP is responsible to distribute the security context to the target AP. Therefore, STA and the target AP can share the PMK without an authentication. In this case, inter-access point protocol (IAPP) services should be provided by the infrastructure to transport PMK between APs.

4(a) 802.1x authentication: An extensible authentication method is performed based on the IEEE 802.1x framework which provides port-based access control. Mutual authentication is enforced if the STA is willing to create a secure association. Figure 3 represents the handoff procedures of a full authentication.

4(b) IAPP key distribution: Security context is exchanged while STA request an association to the target AP. New keying material between the STA and target AP is produced from a previous PMK and transferred using IAPP. Figure 4 represents the handoff procedures of such a case.

5 802.11i key handshake: The dynamic key management protocol for producing a fresh key for wireless transmissions.

Handoff step	Latency
T_{Scan}	< 500ms
T_{Auth}	< 10ms
T_{Asso} / T_{Reasso}	< 10ms
$T_{802.1x}$	< 1500ms
$T_{4\text{-}way}$	< 100ms

Table 1. Latency for each handoff step based on the IEEE 802.11b

Since the 802.1x authentication dominates the handoff latency, the IEEE 802.11i provides *preauthentication* to perform it in a proactive manner. Preauthentication utilizes the serving AP to relay the authentication messages between the STA, target AP, and AS. As a result of a successful preauthentication, authorized port of the target AP is opened. Therefore, STA just need to perform the four-way handshake while it associates to the target AP without any port blocking. However, preauthentication may require the topology information of the infrastructure to acquire the MAC address of the target AP. It makes difficulty to apply in recent WLAN networks.

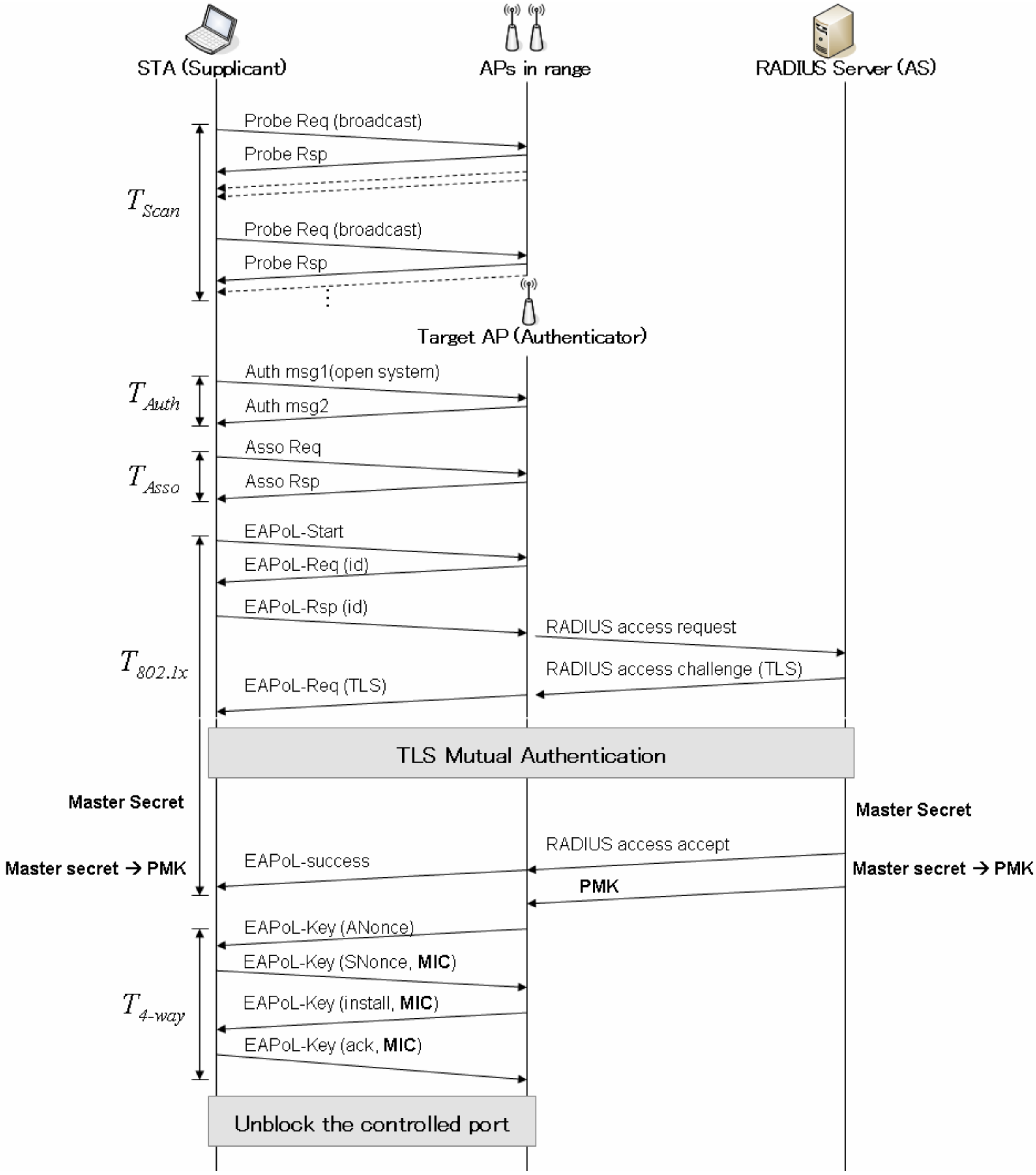

Figure 3. The handoff procedures that perform a full 802.1x authentication

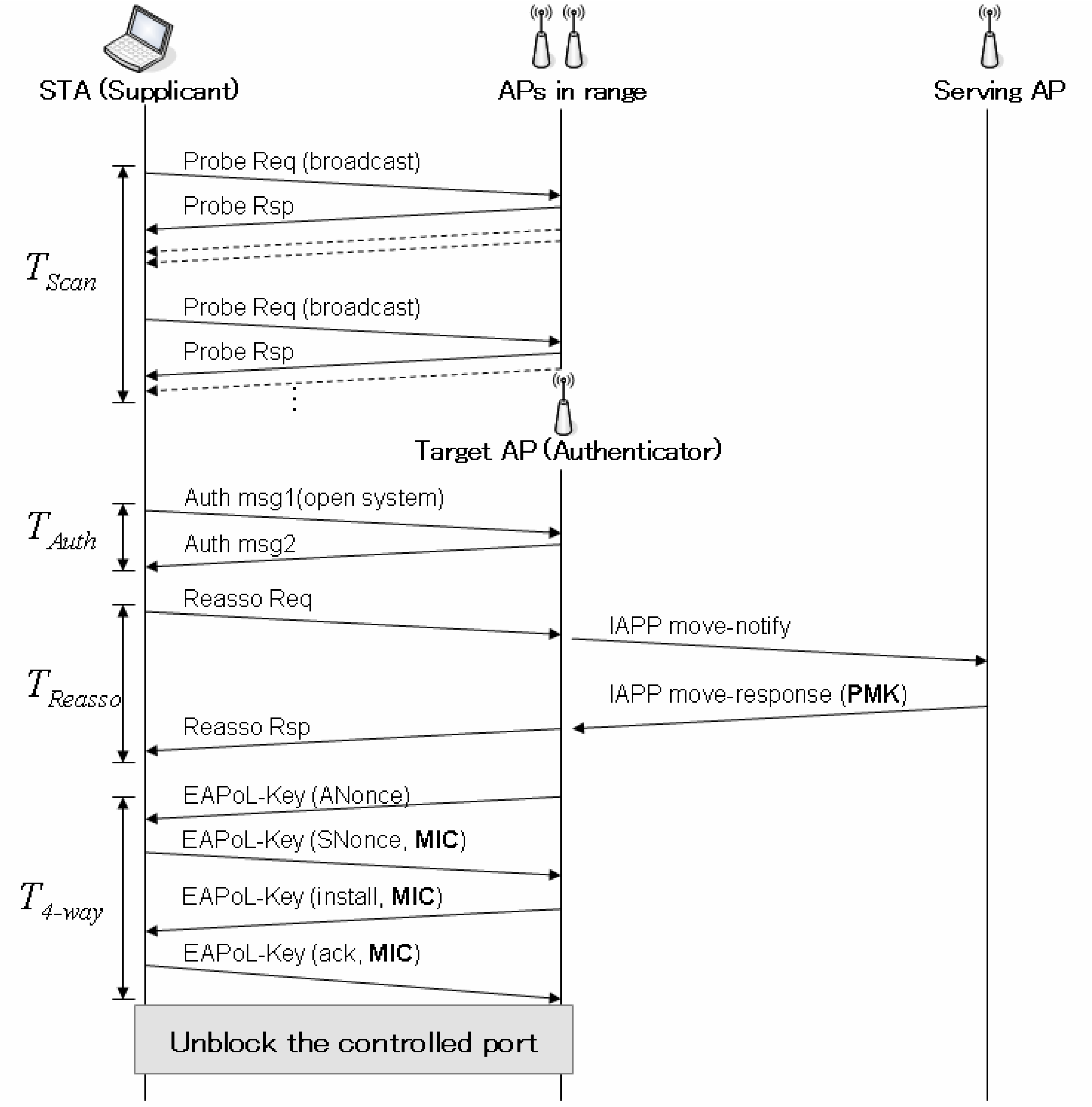

Figure 4. The handoff procedures that perform the IAPP key distribution

d. WLAN Multiplexing Scheme

To use a time division multiplex concept to connect to different WLAN networks is first presented in the MultiNet [2]. The proposed MultiNet facilitates the multiple accesses between the ad hoc networks and infrastructure networks by providing a virtualization architecture over a single WLAN card. In this architecture, each network is handled by a virtual adapter which is abstracted from the physical hardware. The virtual adapters act as general WLAN interfaces, but are controlled by a MultiNet protocol driver that performs the multiplexing over different networks in a time division manner. In order to prevent the packet loss during the multiple accesses, MultiNet provides a buffering protocol by utilizing the WLAN power saving mode. Any packet arrives during the power saving period should be buffered by the previous hop in an ad hoc network or by the associated AP in an infrastructure network. STA may retrieve the packet while it switches back to the network. MultiNet also provides switching algorithms for different access strategies between each network.

The purpose of the MultiNet is to extend the network connectivity for a STA. STA may stay on an infrastructure network to access the public resources while acts as a relay node for an ad hoc network. However, the purpose of the DualMAC is to facilitate a seamless connectivity during the handoff. The network duplex is performed between two infrastructure networks rather than an ad hoc network and an infrastructure network. Furthermore, DualMAC enforces the switching mechanism according to the real-time communications while MultiNet focuses on the load balance between each network.

III. DualMAC Handoff

In this section, we describe the proposed DualMAC mechanism for the WLAN handoff, and show how it works. During a WLAN handoff, the old link is forced to disconnect while STA associates to a new AP. The latency introduced by the context exchange and the key handshaking totally reflects the service disruption time of a real-time communication, which may reach thousands of milliseconds. In our approach, DualMAC-capable STA uses an additional MAC address to create a new radio link with the target AP without breaking the existing association. Therefore, STA can access both the channels by multiplexing both the infrastructure BSSs in a time-division manner. We also provide a switching algorithm to ensure the service quality of the real-time communications and a buffering protocol to prevent the packet loss problem.

A. DualMAC vs. single station association

In section II, we have introduced the WLAN single station association and the correspondent IAPP operations those ensure such a requirement. During the change of the association from the old AP to the target AP, the IAPP MOVE-notify and ADD-notify sent by the target AP remove the old association states according to the MAC address specified in the packet. Since DualMAC STA has two different MAC addresses, using another MAC address to create a new association can avoid the IAPP operations for single station association. The STA that possesses two MAC addresses are considered as two different identities for the WLAN DS. Therefore, DualMAC-capable STA can keep the serving traffics while performs handoff procedures.

B. Multiple access between networks

By using the different MAC addresses to connect to the different APs, multiple access between the infrastructure BSSs is possible for a STA. However, there should be other mechanisms provided to prevent the packet loss during the network switching. Furthermore, we should model the real-time communication behaviors to determine the switch timing. The following depicts the buffering protocol and the switching algorithm for a DualMAC-capable STA that performs real-time communications:

1. *Buffering protocol*: Since adjacent WLAN APs are always on the independent channels, STA should perform channel switching periodically to listen to arrival packets from both the serving AP and the target AP. A good switching method always relies on the accurate prediction for the arrival time of the incoming packets. However, it is hard to achieve due to the fluctuation of network traffics or the channel condition. Instead of providing such a prediction method, we take a buffering approach. The IEEE 802.11 provides

packet buffering for incoming traffics while a STA enters the *power saving mod*e (PSM).

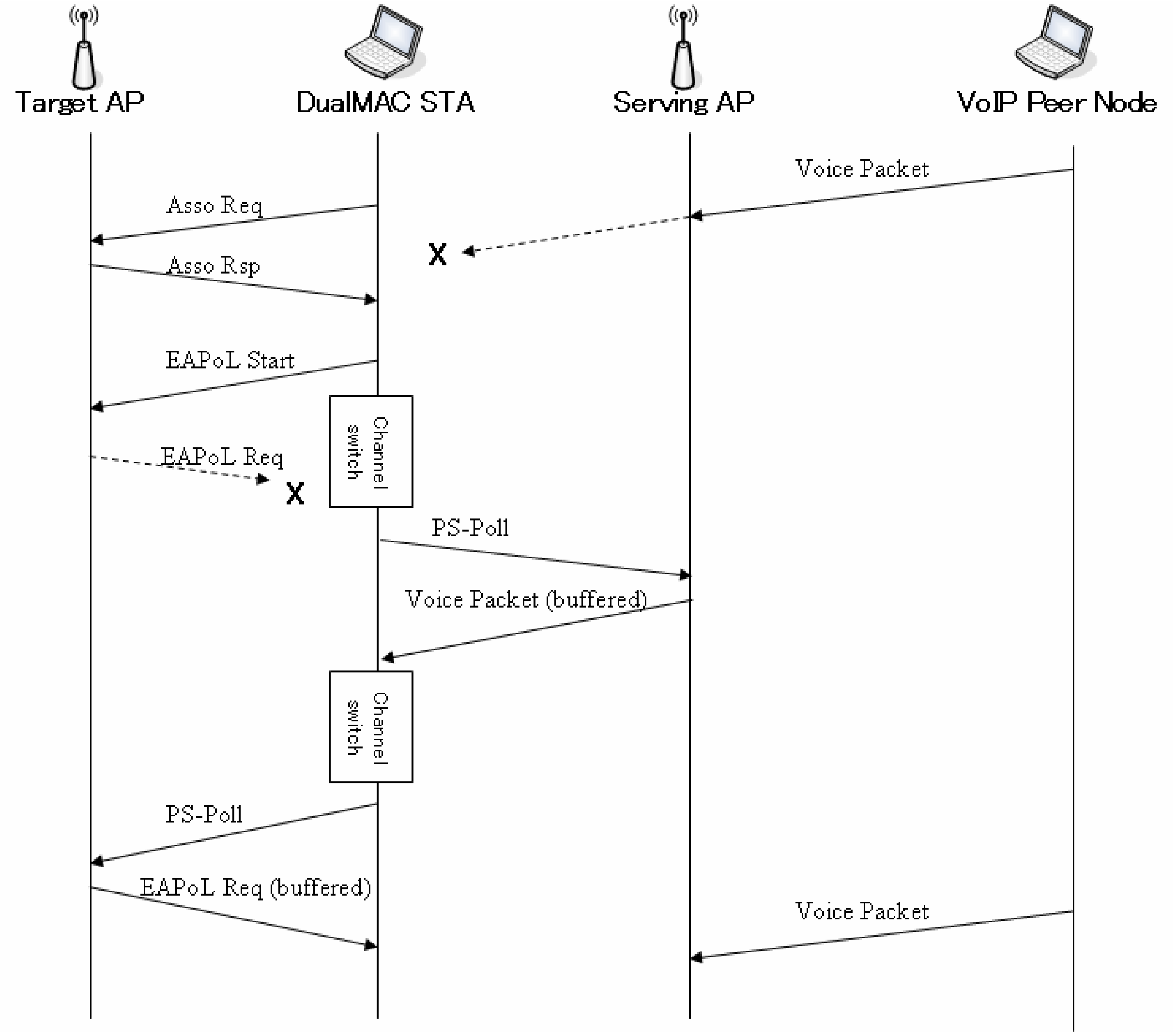

Figure 5. The scenario of the buffering protocol for both the infrastructure BSSs

During the power saving interval, the serving AP buffers any packet destined for the STA. STA can retrieve the buffered packets later by sending a *PS-Poll* to the AP. The buffering protocol is used in the following two cases:

- The real-time communications: STA enters the PSM of the serving AP to prevent the packet loss of the incoming real-time packets.
- The handoff procedures after the association: STA enters the PSM of the target AP to prevent the packet loss of the handoff traffics that includes the security context exchange and the four-way handshake.

Figure 5 shows the scenario of the PSM buffering.

Since the power saving mode can be activated only after a successful association, there should be packet loss problem for the handoff procedures before the association. Here we describe the method to prevent such the condition. The first step of the handoff is to probe all available APs. STA uses active scan in this case. STA that sends the probe request should wait for *minChannelTime* period if there is no available AP on this channel or *maxChannelTime* period for all probe responses. During the wait interval, the STA should stay on the target channel to listen for any response, or the responses may be lost. After probing a channel, STA switches back to the serving channel to retrieve the buffered packets, and then probes the next channel. Until the scan procedure is finished, the authentication and association is then performed. The authentication and association should be performed atomically without switching to prevent the packet loss of the response packets.

2. *Switching protocol*: In order to ensure the service quality of real-time communications, the delay of the arrival packet should be bounded to an acceptable range. Therefore, we should design a scheduling algorithm to access both the channels under the QoS constraint. Real-time communications are always modeled as a periodic traffic with a small inter-arrival time. Because the real-time packets arrive periodically in the ideal case, there must be free time between the arrival intervals. We define this interval as the *idle interval*. During the idle interval, the DualMAC-capable STA can switch to another infrastructure BSS to perform the handoff procedures. After the end of each idle interval, the STA switches back to the serving AP, transmits uplink packet, and then polls for the buffered packet. However, the STA cannot stay on the target channel too long, or the reception of the real-time packets may be delayed. The time quota to enforce the handoff procedures for each idle interval is depicted as the following equation.

T = (packet inter arrival time) – 2*(channel switching time)

Since the STA should switch to the target channel and then switch back to the serving channel, the channel switching time is multiplied by two. Notice the real-time packets may not arrives periodically in the real environment, we should analysis the introduced delay by the above switching algorithm in the best case and the worst case.

- The packet arrives just before the predicated arrival time: In this case, the packet can be directly retrieved while the STA switches back to the serving channel. The introduced packet delay is close to zero.
- The packet arrives just after the predicated arrival time: In this case, the packet can not be retrieved since it has not arrived at the serving AP. The retrieval of the packet is postponed until the end of the next idle interval. As a result, the worst case delay is close to the ideal inter-arrival time.

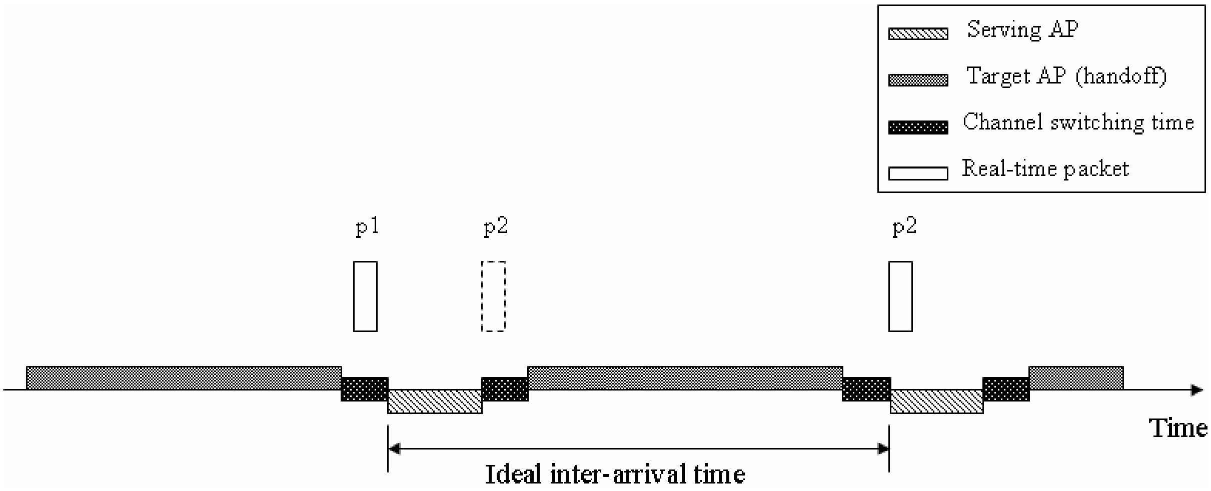

Figure 6. Packet *p1* arrives just before the predicated arrival time, so it can be retrieved directly without any delay. However, packet *p2* arrives just after the predicated arrival time. The retrieval of the packet is delayed for a period

According to the analysis above, the additional delay introduced by the network multiplexing is bounded to a small range. Therefore, real-time packets that arrive at any time may be acceptable for most of the real-time applications by the proposed switching algorithm. Figure 6 shows both the cases.

DualMAC provides an opportunity to access multiple infrastructure BSSs with a single WLAN card. Based on the multiplexing scheme over different networks, the handoff can be performed in the background while STA keeps real-time communication. Therefore, we can facilitate a make-before-break handoff approach which minimizes the link creation latency.

IV. Simulations and Results

In this section, we present the simulation model and results of the DualMAC handoff. Furthermore, we will consider the same case under an inter-subnet handoff. We focus on the service quality of the real-time communications while creating a new association in a secured WLAN, and compare its connectivity under different approaches. The WLAN environment is based on 802.11b PHY, where only 11 channels are available. The real-time traffics are simulated using *IxChariot* [18], a well-known network tester which supports most types of network flow, including the voice call. We use G.711 as the voice sampling codec which generates voice packets every 20 milliseconds.

In order to simulate our approach in a real environment and, we have setup the IEEE 802.1x framework and activate the dynamic key management. We experiment the handoff in such a secured WLAN for several times in order to log the traffics and its relative arrival time, which will be taken as our simulation input. The experiment environment is constructed by a supplicant that runs wi-fi protected access (WPA) client provided by Windows XP service pack 1, an *Planex GW-AP54SGX* AP that acts as an authenticator, and an authentication server that runs *freeRADIUS* [16]. We use EAP-TLS as the default authentication method which is based on public key certificates. Wireless packets are captured using *Airopeek* developed by *WildPackets* [17]. Our simulation takes the log files of both voice traffic and handoff traffic as the input. We also implement the functions of the buffering protocol and the switching algorithm in our simulation. The objective of the simulation is to observe:

1. Packet delay of the real-time communications caused by the buffering protocol and the switching protocol.
2. The service disruption time of the real-time communication..
3. The duration of each handoff procedure (the IEEE 802.11 scan, authentication, and association, the IEEE 802.1x EAP authentication, the IEEE 802.11i four-way handshake, the DHCP handshaking) and the overall cost.

A. Simulation assumptions

1. There are only voice traffics during the handoff.
2. Packet delay that equal to or longer than *150ms* are regarded as packet loss for voice call [15].
3. Link creation traffics are sent without retransmission.
4. Channel switching time is 5ms while using prism2-based NIC [8].
5. Available APs are only on independent channels: channel 1, 6, and 11.
6. The probing phase uses active scan, and the *minChannelTime* and *maxChannelTime* are 7ms and 11ms, respectively. It is the recommended value according to [1].
7. The signal quality of both the serving link and target link remains acceptable during the handoff.

B. Simulation cases

We design some handoff approaches to observe the effect caused by the multiplexing scheme. There are two cases:

1. General handoff: STA provides a single MAC address and performs the general handoff.
2. DualMAC handoff: STA provides two MAC addresses and performs the network multiplexing during the handoff.

C. Simulation results

1. *The effect of DualMAC*: Compare Figure 7 and Figure 8. In Figure 7, we can see that the STA maintains good connectivity before the handoff starts. However, as the STA change its association to the target AP, the old connection is forced to broken due to the single station association. The voice call is recovered until the STA finishes the security key exchange and acquires a new IP address. On the other hand, Figure 8 shows that DualMAC approach works well during the overall handoff without any disruption. DualMAC provides the ability to perform the handoff but keeps the serving communication in the same time.
2. *The effect of network multiplexing*: As mentioned in section IV, the buffering protocol provides an opportunity to access multiple networks without packet loss. Therefore, the handoff and the real-time communication can be preformed according to the switching algorithm without considering the packet arrival time. Figure 8 shows the voice connectivity of the DualMAC handoff, which switches back to the serving channel every 20ms. We can see that the packet inter-arrival time (IAT) is fluctuant from 3ms to 37ms during the handoffs. Due to the network routing or the CSMA/CA contention of the WLAN, the real-time packet does not arrive at serving AP every 20ms. Therefore, packets those arrive while the STA stays on the target channel are retrieved until the next time. It causes the IAT close to 40ms. If more than two real-time packets arrive at the serving AP during an idle interval, they will then retrieved by a continuous *PS-Poll*.

Hence the IAT of these packets are the polling delay which is close to 0.

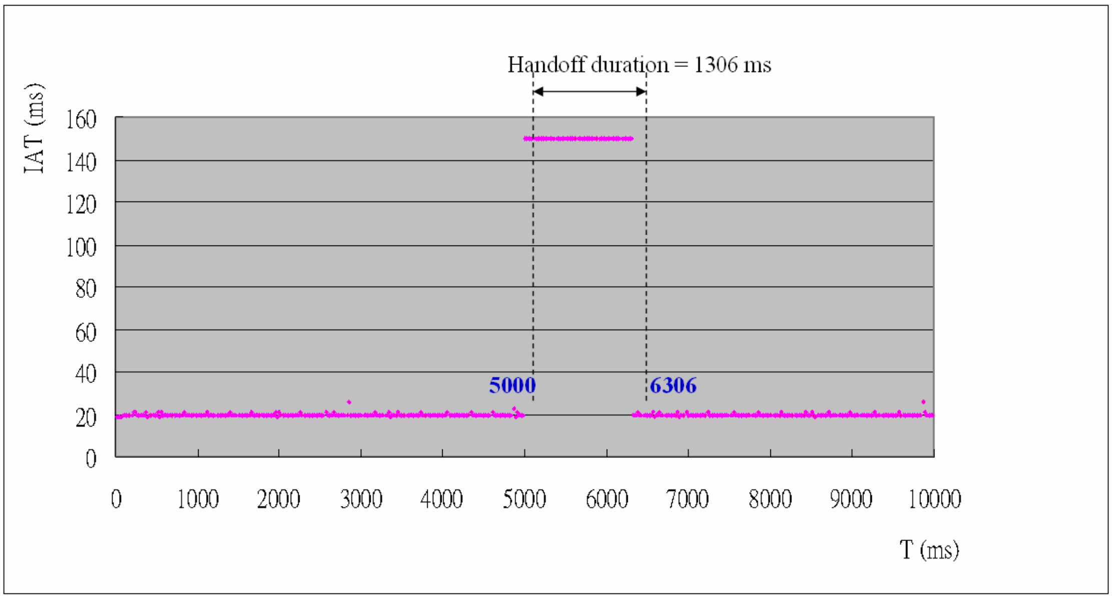

Figure 7. The connectivity of the real-time traffics during a general handoff

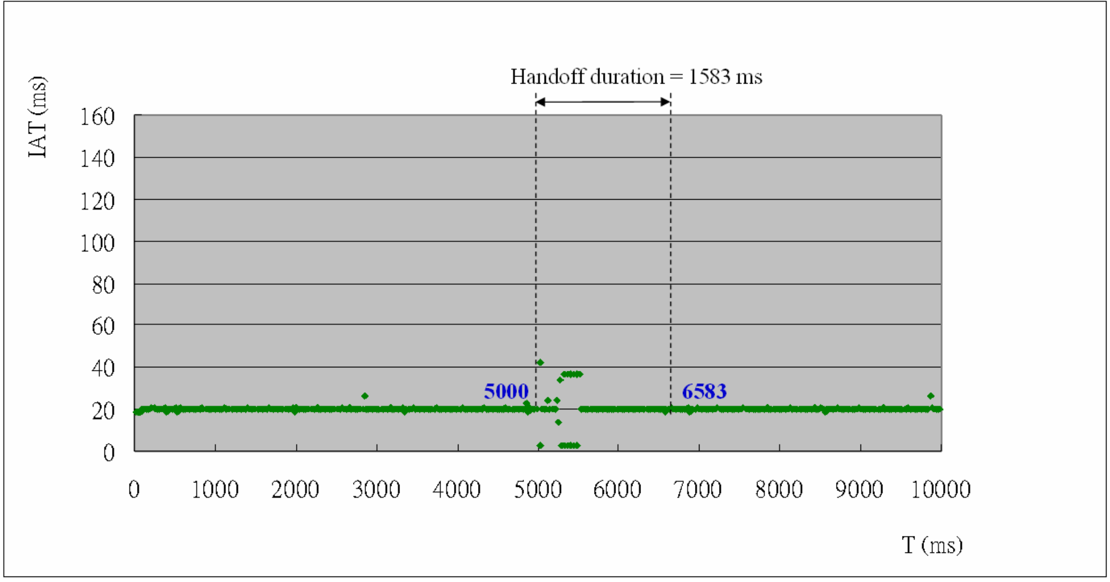

Figure 8. The connectivity of the real-time traffics during a DualMAC handoff

We make a statistical analysis about the IAT during the different handoff approaches. Figure 9 shows the cumulative distribution function (CDF) of the IAT during the general handoff and the DualMAC handoff. The ideal IAT is 20ms based on G.711 codec, but it may exceed 150ms if the STA loss the connectivity with serving AP. For the general handoff, all packets during the handoff are lost due to the channel switching and the single station association, thus the inter-arrival time is all exceed 150ms. On the other side, the IATs introduced by the DualMAC are ranged from 3ms to the 37ms according the best case and the worst case delay. We can observe that 80% of the IATs during the handoff are still close to 20ms. Only a small part of packets are delayed until the next retrieval interval. We compute the average IAT for the DualMAC handoff and find that the average IAT is close to the ideal 20ms.

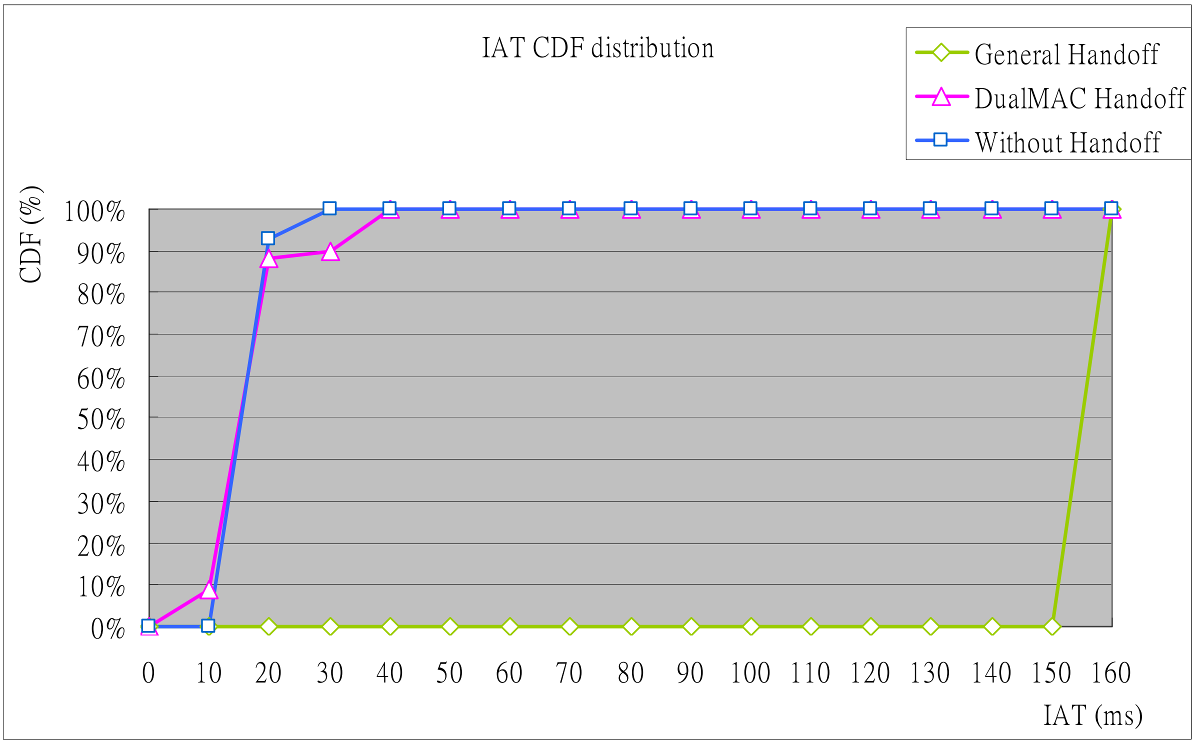

Figure 9. The CDF of the IAT under different handoff approaches

Table 2 shows the latency of each handoff step. We can observe that the handoff latency for DualMAC is always longer then the general case. The reason for this effect is trivial. Approach that implements multiplexing protocols suffers from the overhead of channel switching time. It also requires additional traffics to retrieve the buffered frames from APs. Therefore, the duration is longer than the general handoff that only suffers from the link creation latency.

Handoff delay items	General Handoff (ms)		DualMAC Handoff (ms)	
	AVG	STD	AVG	STD
SCAN	144.00	0.00	227	0.00
AUTH	1.46	0.04	14.52	0.04
ASSOC	2.09	0.08	15.00	0.08
Full 802.1x AUTH	542	3.63	598.68	4.43
802.11i 4-way	22.18	0.16	32.14	0.07
DHCP	636.92	4.48	699.92	1.56

Table 2. The latency of each handoff procedure for both the general handoff and DualMAC approaches.

Finally, we compare the handoff duration based on whether the STA performs the handoff with a full 802.1x authentication or not. Besides, we also compare the overall handoff duration and the service disruption time, to show that the DualMAC requires more time for handoff but maintains better connectivity. Table 3 shows the comparisons.

Handoff types	**Handoff duration(ms)**		**Service disruption(ms)**		**Service disruption /**
(DHCP is included)	**AVG**	**STD**	**AVG**	**STD**	**handoff duration**
General handoff (with full 802.1x authentication)	1294.51	4.23	1294.51	4.23	100%
General handoff (without full 802.1x authentication)	747.46	4.05	747.46	4.05	100%
DualMAC handoff (with full 802.1x authentication)	1586.92	1.80	0	0	0%
DualMAC handoff (without full 802.1x authentication)	1000.42	1.59	0	0	0%

Table 3. The relationship of handoff duration and service disruption time compared among different handoff procedures and approaches

V. 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% to 70% and 17% to 25% respectively by applying the proposed mechanism, the packet loss and the service disruption for real-time communications during handoffs are both avoided.

References

[1] A. Mishra, M. H. Shin, and W. A. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," ACM Computer Communications Review, Vol. 33, No. 2, pp. 93 - 102, 2003.

[2] R. Chandra, P. Bahl, and P. Bahl, "MultiNet: Connecting to Multiple IEEE 802.11 Networks Using a Single Wireless Card," Proceedings of IEEE Infocom 2004, Hong Kong, March 7-11, 2004.

[3] M. H. Shin, A. Mishra, and W. A. Arbaugh, "Improving the Latnecy 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, and 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, and W. A. Arbaugh, "Proactive Key Distribution Using Neighbor Graphs," IEEE Wireless Communications, Vol. 11, Feb. 2004.

[6] C.-C. Tseng, L.-H. Yen, H.-H. Chang, and K.-C. Hsu. "Topology-Aided Cross-Layer Fast

Handoff Designs for IEEE 802.11/Mobile IP Environments," IEEE Communications, pp. 156-163, Dec. 2005.

[7] J. Chan, B. Landfeldt, A. Seneviratne, and P. Sookavatana, "Integrating Mobility Prediction and Resource Pre-allocation into a Home-Proxy Based Wireless Internet Framework," in 2000 IEEE Conf. on Networks, ICON2000, Singapore, pp. 18-23.

[8] I. Ramani and S. Savage, "SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks," Proceedings of the IEEE Infocom Conference, Miami, March 2005.

[9] IEEE 802.11r, "Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment 2: Fast BSS Transition," Draft 1.

[10] IEEE 802.11k, "Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications Amendment 9: Radio Resource Measurement," Draft 3.

[11] 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.

[12] IEEE 802.11f, "IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation," 2003.

[13] IEEE 802.1x, "Port-Based Network Access Control," 2001.

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

[15] Mahbub Hassan, Alfandika Nayandoro, and Mohammed Atiquzzaman, “Internet Telephony: Services, Technical Challenges, and Products,” in IEEE Communications Magazine.

[16] freeRADIUS, http://www.freeradius.org/.

[17] AiroPeek, http://www.wildpackets.com/products/airopeek/overview.

[18] IxChariot, http://www.ixiacom.com/.