A Seamless Handoff With Multiple Radios in IEEE 802.11 WLANs

Sunggeun Jin, *Member, IEEE*, and Sunghyun Choi, *Senior Member, IEEE*

***Abstract*—It is obvious that a seamless handoff should be pursued for better service. For this reason, we design a novel and feasible 802.11 handoff scheme for 802.11 wireless local area networks (WLANs). In the proposed handoff scheme, the 802.11 access points (APs) have multiple radios. One of the multiple radios is exclusively reserved for scanning purposes. It certainly helps the 802.11 mobile stations (STAs) to easily search neighboring APs. Moreover, the reserved exclusive channel is available for data frame exchanges. Consequently, STAs can be serviced with minimized data frame losses while they are performing the proposed handoff. For practical observations, we implement the proposed handoff scheme. Then, we evaluate handoff performances by comparing the packet losses between the proposed handoff scheme and the existing handoff schemes. Based on the evaluation, we have built analytical models to estimate overall packet losses while an STA moves from an AP to another AP in an indoor environment. The analytical results show that the proposed handoff significantly reduces packet losses compared with existing 802.11 handoff schemes.**

***Index Terms*—Handover, mobile radio mobility management, wireless local area network (WLAN).**

I. Introduction

DUE TO THE commercial success of 802.11 wireless local area networks (WLANs), we are witnessing explosive expansions of the regions covered by 802.11 WLANs. Accordingly, we are encouraged to walk around across the 802.11 WLANs' coverage with real-time services demanding stringent quality-of-service requirements. For this purpose, many studies have been carried out on the topic of the 802.11 handoff since it is the technology that helps the station (STA) cross cell boundaries without service disruptions. Additionally, recent studies have shown that well-designed handoff operation is helpful to reduce STAs' energy consumption in mobile environments [2]–[4].

The 802.11 standard specifies the 802.11 handoff operation consisting of three procedures: 1) scanning; 2) authentication; and 3) reassociation. The 802.11 scanning is a procedure for an 802.11 STA to search neighboring access points (APs). The scanning STA may choose the best appropriate AP among scanned APs for its handoff. The authentication and reassociation procedures are used for the validation and the connection establishment for the scanning STA, respectively. In [5] and [6], it is empirically shown that the scanning is the most time-consuming job out of three procedures composing the 802.11 handoff. For this reason, the studies on the 802.11 handoff have been focused on reducing the scanning time, as discussed later in detail [7]–[15].

Brik *et al.* [8] and Ramachandran *et al.* [9] tried to eliminate scanning latency to keep communicating between a scanning STA and a serving AP. For this purpose, they proposed 802.11 handoff schemes by utilizing multiple radios. In their schemes, STAs are designed to try scanning procedures with one radio for exclusive scanning purposes. The other radios are used for normal 802.11 operations, including the 802.11 frame exchanges. Their schemes contribute to significant reduction in potential 802.11 frame losses and frame transmission delays during the scanning procedure. However, their benefits are limited in that the proposed schemes require STAs to have at least two radios despite that typical commercial STAs have only one radio.

In contrast, we propose APs to be equipped with multiple radios, whereas an STA has a single radio. All the radios of an AP are set to share the same basic service set identity[1] (BSSID). One of them is configured to operate in an exclusively reserved channel for the scanning. That is, all the APs have one radio operating in the reserved channel. Then, an STA scans only the reserved channel without needing to scan other channels. Therefore, we do not need to worry about scanning time no matter how long the scanning time is. It is because a typical scanning STA with a single radio can continue to conduct normal 802.11 operation with the serving AP. We empirically show that the proposed handoff incurs fewer packet losses compared with the other handoff schemes. In addition, we analytically estimate the overall packet losses, which each handoff scheme may result in, while a user is assumed to move from one AP to another AP.

This paper is organized as follows. In Section II, we discuss previous work with an overview of the 802.11 scanning. In Section III, we propose a novel 802.11 handoff operation with a scanning procedure utilizing multiple radios. In Section IV, we explain how to build the proposed 802.11 handoff operation and provide the experimental results. In Section V, we numerically

Manuscript received December 23, 2011; revised November 8, 2012, March 8, 2013, and July 9, 2013; accepted August 21, 2013. Date of publication September 27, 2013; date of current version March 14, 2014. This work was supported by Daegu University Research Grant, 2013. An earlier version of this paper was published in the IEEE Communications Letters, October 2009. The review of this paper was coordinated by Dr. P. Lin.

S. Jin is with Daegu University, Gyeongsan 712-714, Korea (e-mail: sgjin@daegu.ac.kr).

S. Choi is with the Department of Electrical and Computer Engineering and the Institute of New Media and Communications, College of Engineering, Seoul National University, Seoul 151-744, Korea.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2013.2283914

[1] BSSID is identical to the AP's MAC address.

analyze the packet losses due to the handoff operations by referring to the experimental results. Section VI concludes this paper.

II. Previous Work

In the 802.11 standard, a handoff procedure consists of scanning, authentication, and reassociation. For the scanning, passive scanning and active scanning are defined. An STA adopting the passive scanning should receive APs' beacon frames, which are transmitted every beacon interval. Typically, a beacon interval is 100 ms. On the contrary, an STA with the active scanning should broadcast probe request frame(s) in a channel and then wait for probe response frames, with which nearby APs receiving the probe request(s) reply. The scanning STA may conduct the scanning procedure in all available channels. It implies that the scanning time increases in proportion to the number of the available channels. After selecting the most appropriate AP via the scanning procedure, the scanning STA proceeds with the subsequent handoff procedure including authentication and reassociation. Usually, it is known that active scanning is more beneficial than passive scanning in operational time. Therefore, we deal with only active scanning in this paper.

For active scanning, the 802.11 standard specifies two configurable parameters determining how long an STA should wait for probe responses after sending a probe request, namely, MaxChannelTime and MinChannelTime. MinChannelTime is the minimum time that a scanning STA stays in a scanned channel, whereas MaxChannelTime is the maximum. For example, if a scanning STA detects busy channel during MinChannelTime after broadcasting probe requests, the STA stays more in the channel until MaxChannelTime. However, the 802.11 standard does not specify what values are sufficient for Min/MaxChannelTimes. Typical commercial 802.11 devices apply 20 and 40 ms to MinChannelTime and MaxChannelTime, respectively [16].

Large values of Min/MaxChannelTimes improve the possibility that a scanning STA finds nearby APs successfully even in a channel with heavy contention. However, it leads to a long scanning delay. Therefore, it is important to determine appropriate Min/MaxChannelTimes. In [15], aggressive 1 and 10 ms for Min/MaxChannelTimes, respectively, in the 802.11b WLANs are recommended.

Along with the Min/MaxChannelTimes, the number of employed channels is another major factor influencing the overall scanning delay. Shin *et al.* [14] proposed a scanning scheme employing the neighbor graph containing the list of channels occupied by neighboring APs. Due to the neighbor graph, a scanning STA can scan in a reduced number of channels. The neighbor graph is also beneficial to reducing processing time overhead required for authentication and security operations as a serving AP propagates STAs' contexts to its neighboring APs in advance to cache the context related to the scanning STA [16]. Additionally, Pack *et al.* [17] improved the caching strategy considering the handoff statistics gathered by monitoring handoff patterns. The obtained weight factors from the statistics are applied to STAs' context propagation, resulting in reducing message overhead on the links between neighboring APs.

In many cases, it is assumed that scanning as a part of 802.11 handoff is initiated when the 802.11 handoff is triggered with a particular condition such as signal quality dropping below a threshold. As explained earlier, the scanning in all employed channels may incur a series of data frame losses. For this reason, Wu *et al.* [10] and Chen *et al.* [11] proposed to conduct scanning in each channel in advance, even if a handoff triggering condition is not satisfied.

The authors target at minimizing data frame losses by separating scanning from the actual handoff. Brik *et al.* [8] and Ramachandran *et al.* [9] tried to remove scanning time itself with multiple radios. In their approaches, an STA needs to have at least two radios, one of which is reserved for scanning, and the others are used for normal operation. Accordingly, the scanning STA can exchange data frames with a serving AP while it performs scanning. However, since typical commercial STAs are not equipped with multiple radios, such schemes are limited in use.

III. Proposed 802.11 Handoff Procedures

Fig. 1(a) shows the case when an STA in a nonreserved channel performs a handoff via the reserved channel. All three APs are equipped with two radios. Recall that two radios of an AP share the same medium access control (MAC) address. We summarize the detailed procedure as follows. Prior to scanning, an STA transmits a null frame, i.e., a data frame without a payload, with a power-saving mode (PM) bit set to 1 to inform its serving AP that it enters the power-saving mode (PSM), and then, the serving AP begins to buffer data frames destined for the STA [see (1) in Fig. 1(a)]. The STA switches its operating channel to the reserved channel for scanning [see (2) in Fig. 1(a)]. Thereafter, it transmits a null frame with a PM bit set to 0 to make the serving AP forward buffered data frames. This enables the STA to receive data frames while scanning. The STA broadcasts probe request frames in the reserved channel. Since at least one of each AP's multiple radios operates in the reserved channel, it is not necessary to broadcast a probe request in the other channels [see (3) in Fig. 1(a)]. In the case when the STA fails to find other APs, except the serving AP, in the reserved channel, it determines that there is no AP in its neighborhood. After the STA receives the probe response frames, it selects the most appropriate AP to proceed with an authentication [see (4) in Fig. 1(a)].

In the 802.11 standard [18], probe response and beacon frames are allowed to convey the AP information. We extend this information by adding the channel information regarding AP's multiple radios. For example, the channel information includes the reserved channel number and the operating channel number. The STA with the channel information can recognize what channels are used for normal operation and scanning. After performing authentication and reassociation for a new connection establishment with the chosen AP [see (5)–(8) in Fig. 1(a)], finally, consecutive null frames with a PM bit set to 1 and 0 are transmitted in the reserved channel and a nonreserved channel, respectively, to prevent the losses of data frames during channel switching [see (9) and (10) in Fig. 1(a)]. After the

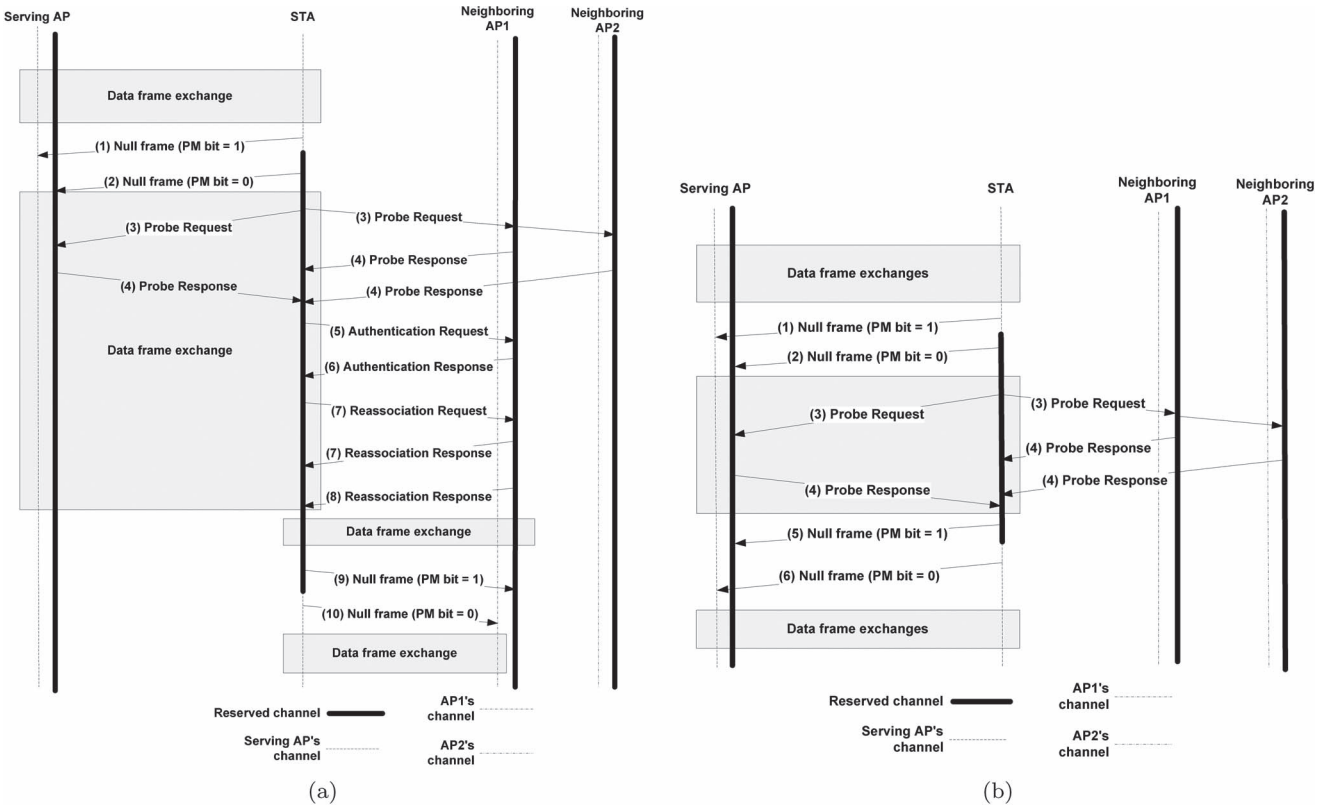

Fig. 1. Proposed handoff procedure. (a) Example for the proposed handoff procedure when an STA moves to another AP. (b) Example for the proposed handoff procedure when an STA stays at the serving AP.

channel switching, the STA can exchange data frames with the new AP.

Fig. 1(b) shows the case when an STA in a nonreserved channel determines to stay at the nonreserved channel after scanning. In this case, the STA should transmits null frames for the beginning of the PSM and channel switching [see (1) and (2) in Fig. 1(b)]. However, after scanning, the STA fails to find better APs than the serving AP; hence, it determines to stay at the serving AP [see (3) and (4) in Fig. 1(b)]. Therefore, the STA returns to the nonreserved channel where it was served by transmitting two null frames [see (5) and (6) in Fig. 1(b)].

IV. Implementation

A. Architecture

Fig. 2 shows the test bed. The test bed is a typical desktop computer equipped with two wireless adapters, i.e., CISCO's aironet 802.11a/b/g wireless adapters[2] in which Atheros AR5520 chipset is embedded. Each test bed has two PCI-to-PCMCIA interface cards converting the electrical signals of a wireless adapter supporting the PCMCIA interface into the electrical signals for the PCI interface. For an STA, we utilize Lenovo's X60T laptop computer.

We combine two wireless adapters into a single AP MAC entity having multiple radios by modifying a *madwifi* device driver. Prior to further explanation, we present an overview of *madwifi v0.9.4*, which we adopt for our implementation.

[2]Their model number is AIR-CB21AG-W-K9.

Fig. 2. Test bed equipped with two wireless adapters.

Madwifi is an open-source project that supports Atheros chipsets in Linux Operating System [19]. It provides well-organized software architecture for the logical 802.11 MAC entity working as an STA or an AP. In the architecture, the logical radio object is designed to control radio-frequency operations as well as physical-layer operations. The logical MAC entity processes most MAC layer operations defined in the 802.11 standard, including connection establishment, queue management for data frame transmissions, handoff, etc. However,

it does not directly control time-critical operations, e.g., short interframe space, point-coordination-function interframe space, distributed-coordination-function interframe space, etc. Madwifi names MAC entities and radio objects after *ath* and *wifi*, respectively. Index numbers are assigned to the names on the order of MAC entity and radio object creations. The AP MAC entity manages all associated STAs with a data structure defined by *ieee80211_node*. In addition, it includes the functionalities designed for the STA MAC entity. On the contrary, the STA MAC entity manages the operations related with an associated AP by using *ieee80211vap*. Therefore, ieee80211_node and ieee80211vap data structures are used to instantiate the objects for STAs and APs, respectively.

Madwifi provides its own scanning scheme called *background scanning*. In the background scanning, an STA splits the available channels into several groups; then, it conducts the scanning in each group of the available channels in turn periodically. For example, madwifi has 35 channels for scanning in the 802.11a WLANs; hence, it divides the 35 channels into five groups. Then, the STA scans only about seven channels for each scanning try. This scanning operation aims to reduce the number of packet losses for a single scanning try. However, it ultimately needs to perform scanning in all available channels to find a proper AP. For convenience, we refer to the handoff employing background scanning as a *legacy handoff*.

We elaborate on how to build a single AP MAC entity with two radios. The adopted Aironet adapters are developed to support the PCMCIA interface. Once these adapters are installed in a test bed, the Linux kernel begins a procedure to initiate the adapters. During the initiation procedure, the alloc_netdev function is called to instantiate a radio object as a network driver object of the Linux kernel. Thereafter, ath_attach function makes queues and threads for frame transmissions and reception. Then, the initiation procedure prepares links[3] for the newly instantiated radio object referring to the queues and the threads. Consequently, the AP MAC entity is enabled to transmit and receive 802.11 frames via the radio object, providing encapsulated functions for frame transmissions and reception.

Fig. 3(a) shows an internal structure consisting of the AP MAC entity and a radio object when a single wireless adapter is installed in a test bed. A received 802.11 frame passes through the radio object, the AP MAC entity, and the IP layer in turn. In the reverse direction, the IP layer tosses data frames to the AP MAC entity. Then, the AP MAC entity prepares the 802.11 header, and the radio object appends it to the IP data frames. Finally, it triggers the hardware logic of the wireless adapter to send the data frame in the air.

When two wireless adapters are installed in a test bed, original madwifi creates two independent pairs of an AP MAC entity and a radio object to support both wireless adapters simultaneously. Fig. 3(b) shows the internal structure for the pairs. Practically, one of the pairs is chosen as a default path to convey IP frames. Accordingly, the other is used as an alternative path only when an application specifies it as an interface for its IP layer communication.

[3]The links are the connections between objects referenced by pointers in C language.

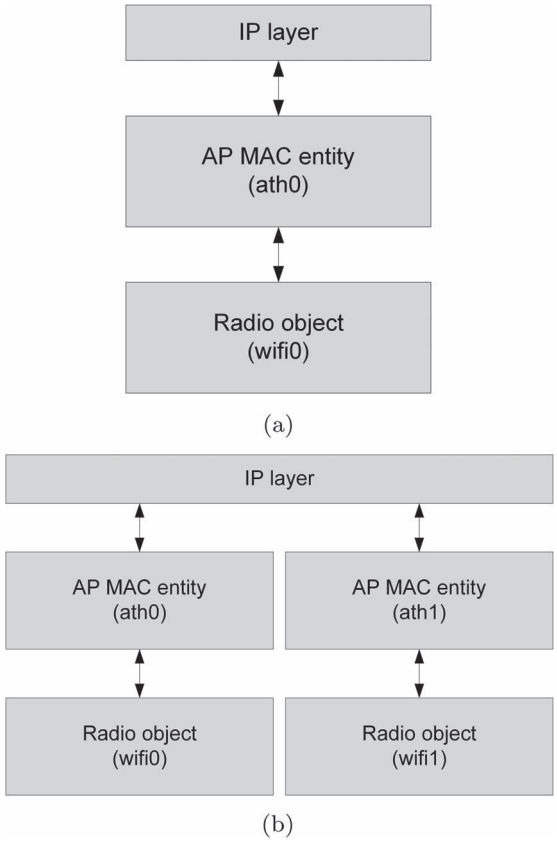

Fig. 3. Internal structures for the madwifi. (a) Internal structure indicating the relationship between the AP MAC entity and a radio object in madwifi when a single wireless adapter is installed. (b) Internal structure between AP MAC entities and radio objects in madwifi when two wireless adapters are installed in a test bed.

However, we need to make a single AP MAC entity to have multiple radios. We first set the MAC addresses of multiple adapters to a single one by using the script as follows:

1) ip link set dev wifi1 down;
2) macchanger − −mac 00 : 40 : 96 : B5 : 52 : 30 wifi1;
3) ip link set dev wifi1 up.

From this script, we change the MAC address of the wireless adapter controlled by radio object *wifi1*. We make a logical software switch connecting a single AP MAC entity and one of two radio objects for each associated STA. When a radio object receives an 802.11 frame from an associated STA, the logical software switch is switched to the radio object that has received the 802.11 frame. According to the proposed scanning procedure, prior to switching to a different channel for scanning, an STA should transmit a null frame to enter PSM. Immediately after switching, the STA should transmit another null frame to leave PSM. It implies that the null frame is used as an indication that a scanning STA switches its current operating channel to another one. Therefore, it is guaranteed that the AP successfully sends 802.11 frames to the associated STA via the connected radio object when the AP has 802.11 frames destined for the STA. Whenever the AP MAC entity makes an association with a new STA, it generates a new logical switch for the newly associated STA. Therefore, this architecture is valid in general cases when the AP MAC entity manages multiple STAs iterating over two channels for scanning. Fig. 4 shows

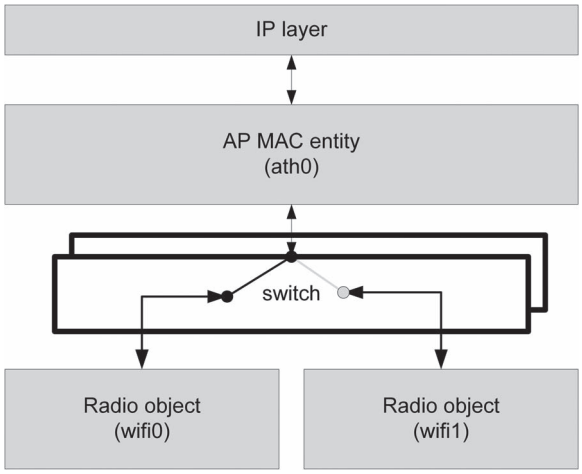

Fig. 4. Internal structure supporting the proposed handoff procedure with two radio interfaces.

an example for the structure in which two STAs are associated with an AP MAC entity. The implemented AP MAC entity can successfully support typical 802.11 handoff operations since a probe response frame is replied by the radio object having received a probe request frame. Additionally, we modify the scanning procedure of the madwifi device driver to support the proposed scanning scheme as an STA MAC entity.

B. Experimental Environments

We conduct our experiments at our office during workdays. We build two couples of test beds equipped with two wireless adapters. One of each couple supports the proposed handoff operation as an AP participating in the 802.11a WLAN. The other is used to monitor the 802.11 frames in the air. For this reason, we can observe how each AP works according to the proposed handoff operation. For experiments in the 802.11a WLAN, we modify the original device driver to perform a legacy handoff in only 5-GHz 802.11a channels. Fig. 5 shows how four test beds are situated at our office. The office is full of workstations in a 12 m $\times$ 15 m region, and two 802.11 APs are separated from each other at the straight-line distance of about 10 m. However, we have to walk by workstations following the movement path between these two APs.

During the experiments, we utilize *iperf* [20] and *wireshark* [21] for UDP packet generation and monitoring tools, respectively. We configure iperf to generate periodic User Datagram Protocol (UDP) packets. The UDP payload size is set to 1 KB. The wiresharks in the APs and the laptop computer capture UDP packets, whereas the wiresharks in monitoring test beds monitor the 802.11 frames in the air. The watches in the laptop computer and all test beds, including APs, are synchronized by using the network time protocol [22] so that we can easily compare the log files generated by the wiresharks with synchronized reference times.

First, we observe the 802.11 frame transmissions in the air until completion of the proposed handoff procedure in two cases: 1) The STA stays at a serving AP; and 2) it determines the handoff to the AP, providing better signal quality. Next, we observe UDP packet losses due to scanning in either case when the legacy handoff or the proposed handoff is employed. Note that, as explained earlier, the STA adopting a legacy handoff periodically conducts scanning in a part of the full channels so that the experimental results show the packet losses incurred by the scanning in a part of the full channels. We have two experimental scenarios for this purpose as follows. First, the iperf running in the laptop computer periodically sends UDP packets to the iperf running in the computer at the network side. These UDP packets are called uplink packets. Second, on the contrary, the iperf running in the computer at the network side transmits UDP packets to the iperf in the laptop computer. In this case, the packets are called downlink packets. Therefore, we observe uplink and downlink packets in turn. For convenience, we call the scanning for the proposed handoff *multiple wireless network interface card (MWNIC)* scanning.

C. Observations on the Proposed Handoff

For the experiments, UDP packets are generated regularly in uplink and downlink directions, respectively. Fig. 6(a) shows the monitored frames when the STA determines to stay at serving AP after scanning. First, the UDP packets are successfully forwarded until 24.525 ms in channel 157. However, the STA makes a decision to scan neighboring APs since the current signal is not satisfactory. The STA then first transmits a null frame with a PM bit set to 1 to the serving AP [see (1) in Fig. 6(a)]. The serving AP is not allowed to forward 802.11 frames to the STA until receiving a frame with PM bit set to 0. It takes about 6 ms for the STA to change the channel [see (2) in Fig. 6(a)]. After that, the STA sends a null frame with PM bit set to 1 by changing its channel number to 165. Thereafter, the serving AP can forward 802.11 frames to the STA. For 167.5 ms, the STA performs scanning by transmitting probe request messages and waiting for probe response messages. However, it fails to find a better AP so that it determines to stay at the serving AP. The STA transmits a null frame with PM bit set to 1 to go back to the serving 157 [see (3) in Fig. 6(a)]. In channel 157, the STA continues to communicate with the current AP [see (4) in Fig. 6(a)].

Fig. 6(b) shows the captured 802.11 frames when the STA successfully hands off to its neighboring AP. The operations at the points of (1) and (2) are similar to the points in Fig. 6(a). However, the STA succeeds in finding a better AP, i.e., AP2, so that it tries to handoff to the newly found AP2. The STA already obtained the channel number occupied by AP2, i.e., channel 153 through AP2's probe response messages. It sends two null frames to AP2 having a PM bit to change its channel. After that, UDP packets are forwarded in channel 153.

D. Observations on Packet Losses

Iperf is configured to generate UDP packets every 10 ms in an uplink or downlink direction, respectively. We observe uplink and downlink packets separately. In all the figures here, the y-axis represents the time intervals between two consecutive packets. The x-axis indicates the packet sequence number that we insert in the payload of UDP packets.

Fig. 7 shows downlink UDP packets when the MWNIC scanning is employed. The host continuously sends UDP packets

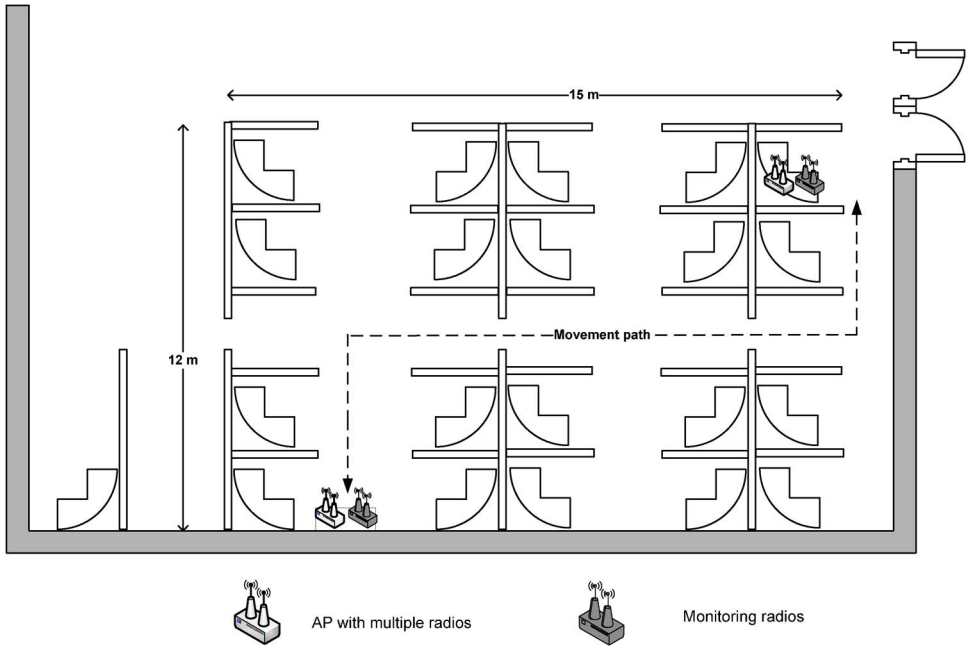

Fig. 5. Experiment venue.

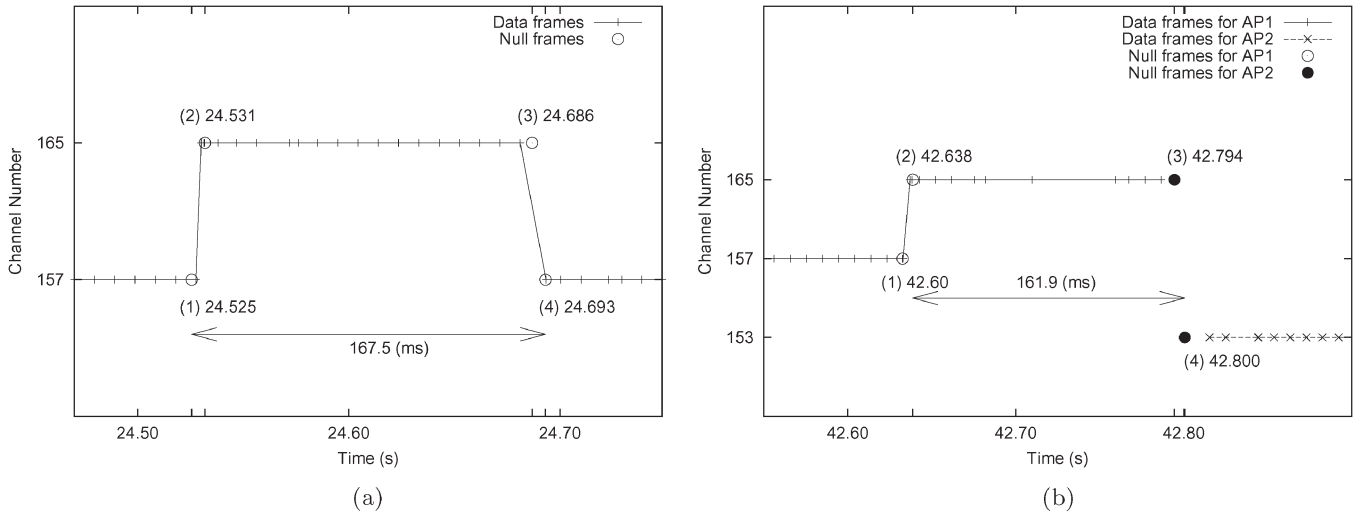

Fig. 6. Captured 802.11 frames depending on the handoff operation. (a) Captured 802.11 frames in the case when the STA stays at the serving AP after scanning. (b). Captured 802.11 frames in the case when a handoff is conducted after scanning. The STA hands off to its neighboring AP.

to the laptop computer. We can observe the latency marked with (1). There are two reasons for this. First, a single packet is lost during channel switching operation. Second, the new AP accepting the scanning STA defers packet transmission until successful STA's channel switching. Immediately after the packet transmission with the delay marked with (1), the packets buffered at the new AP rush toward the laptop computer with very short intervals. We can find another latency mark with (2). However, it has nothing to do with the handoff itself since the delay is caused by retransmission trials due to channel error. Consequently, we find only a single packet loss during MWNIC scanning. Fig. 8 shows downlink UDP packets when background scanning is performed. In contrast to the results shown in Fig. 7, we can observe a big hole due to consecutive 16 UDP packet losses. The packet losses begin from the 100th UDP packet. The delay marked with (1) is incurred by a channel error.

Figs. 9 and 10 shows the results with uplink UDP packets. In Fig. 9, the delays marked with (1) and (2) is caused by UDP packet losses at the laptop computer and an AP, respectively, during the MWNIC scanning. Consequently, UDP packets are forwarded to the host with two packet losses while the scanning STA performs the proposed handoff operation. In contrast, Fig. 10 shows that 22 UDP packets are lost during a background scanning. From the figures so far, we can find out that the MWNIC scanning significantly reduces packet losses compared with the background scanning.

In summary, from the observations in Section IV-C and D, we find out that the proposed handoff scheme has a long scanning time similar to the legacy handoff scheme. Even in this case, the proposed handoff scheme significantly reduces the packet losses since the STA can be serviced with data frames during the scanning. Herein, we have more

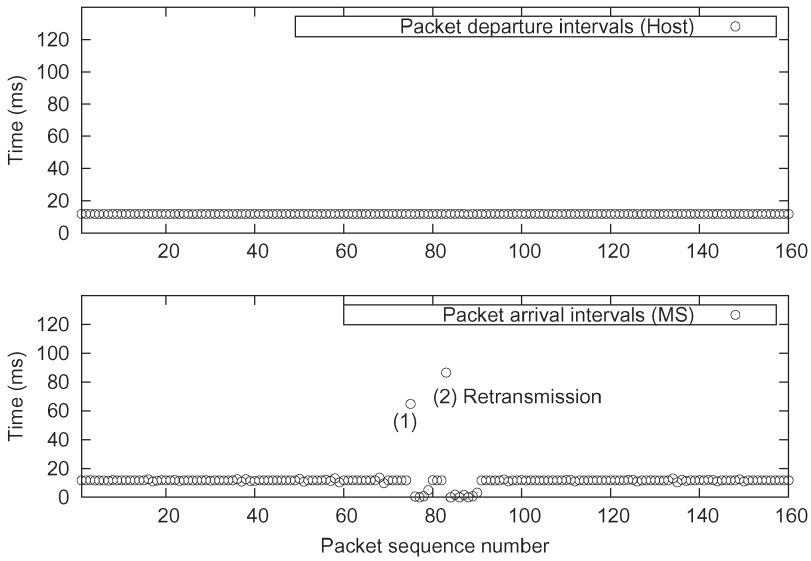

Fig. 7. Captured downlink UDP packets when MWNIC scanning is conducted.

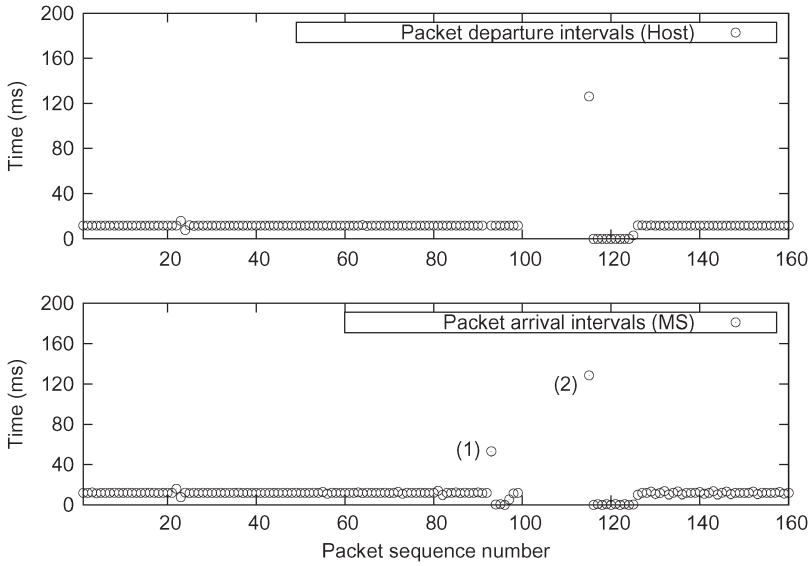

Fig. 8. Captured downlink UDP packets when background scanning is conducted.

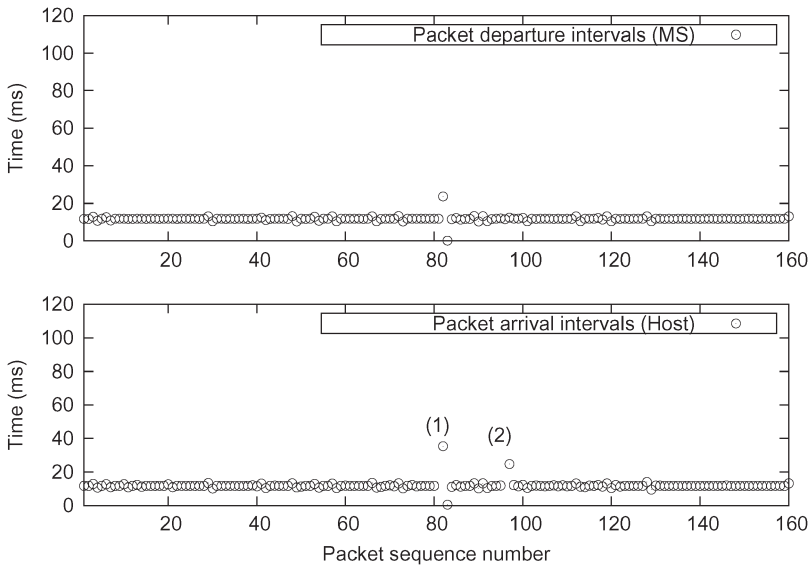

Fig. 9. Captured uplink UDP packets when the MWNIC scanning is conducted.

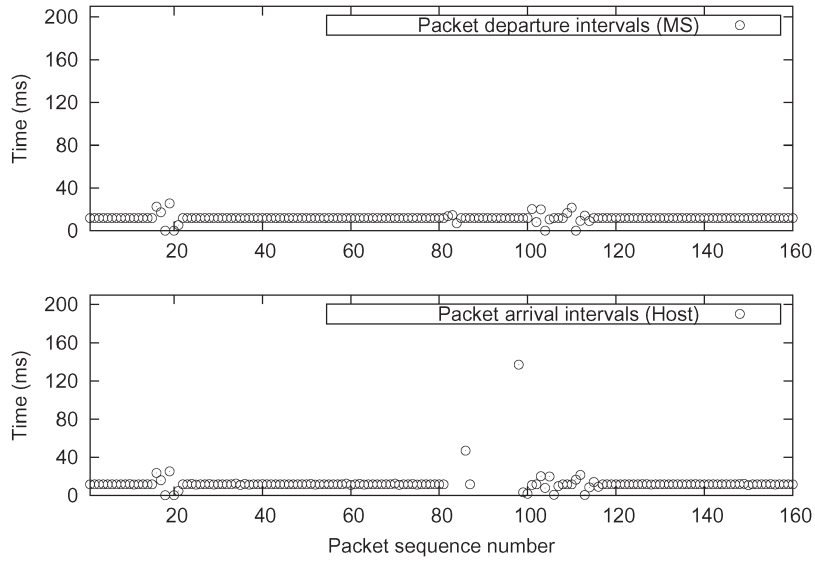

Fig. 10. Captured uplink UDP packets when the background scanning is conducted.

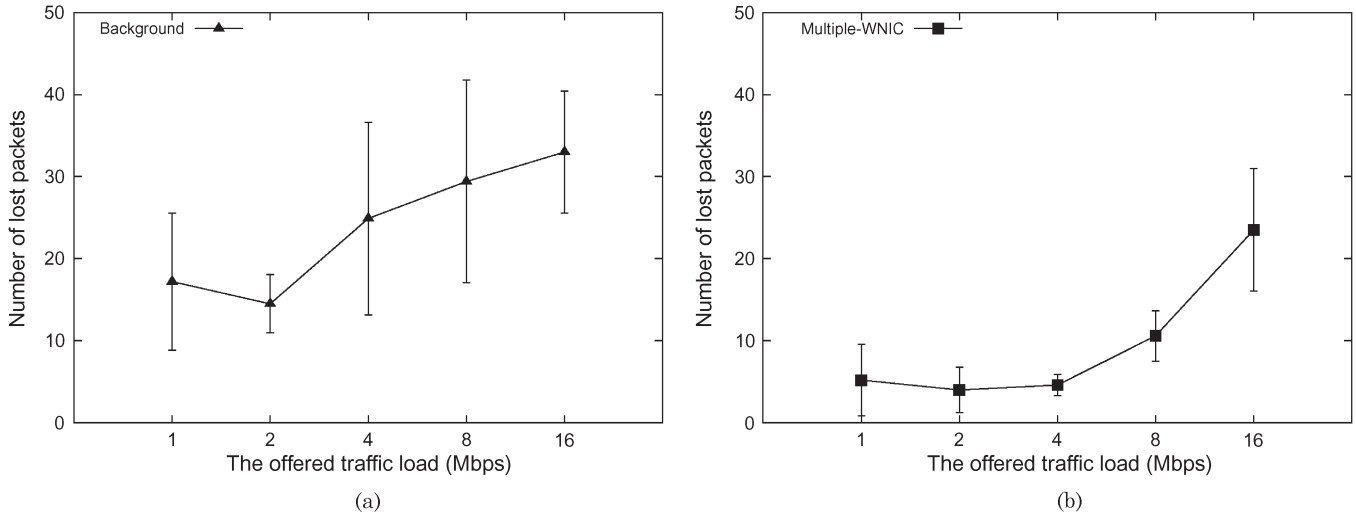

Fig. 11. Comparisons of packet losses while legacy and proposed handoff schemes are applied. (a) Background scanning. (b) MWNIC scanning.

observations on the packet losses depending on the offered traffic load.

Fig. 11 shows the number of packet losses depending on the traffic load. Although the STA enters PSM by buffering arriving packets, packets may be lost for the following reasons: 1) The Atheros chipset and the madwifi may lose a few packets when switching channels; and 2) the buffer is not infinite, and therefore, madwifi may discard overflowing packets. We obtain the average number of lost packets after conducting experiments ten times for each point. For these experiments, we need to eliminate the effect of the packet losses by channel errors as much as possible. Therefore, we do not walk with the STA between two APs separated by a long distance. Instead, we set the scanning threshold to a value high enough to incur more scanning between two adjacent APs. The x- and y-axes represent the offered traffic load and the number of lost packets, respectively. *Multiple-WNIC* and *Background* indicate the packet losses when MWNIC scanning and background scanning are used for the proposed handoff and the legacy handoff, respectively. The error bars are used to represent the standard deviation. Fig. 11 shows that the number of packet losses basically increases as the offered load increases. However, MWNIC scanning outperforms background scanning with a small number of packet losses all the time.

V. Numerical Analysis

We analytically estimate the packet losses, in which a handoff scheme may result, while a user moves from one AP to another AP. From the analytical estimation, we can compare the handoff performances in terms of packet losses. The comparison is valid for the following two reasons: 1) In our measurement, not the channel model but the handoff schemes are major factors for the packet losses; and 2) the employed channel model is used to estimate how many handoffs are triggered during the user's movement. Typically, an STA conducts a handoff when the received signal strength of the currently associated AP drops below a threshold compared with the measured

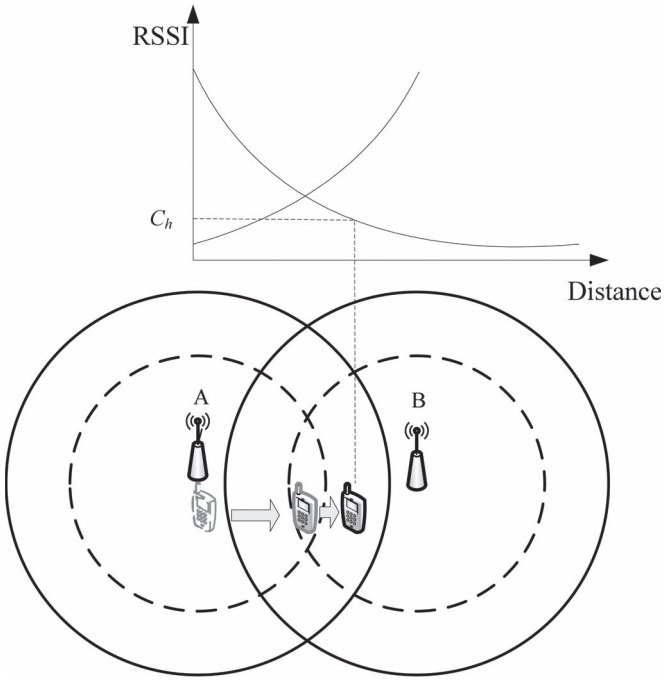

Fig. 12. Handoff decision depending on a threshold.

signal strength of a neighboring AP. We denote the handoff threshold by C_h. We consider a simple scenario shown in Fig. 12 for our analysis. Two APs are situated at positions A and B, respectively and they are separated by distance D. An STA travels from AP A to AP B at a velocity of C_V. When the STA is located at the distance of d from AP A, the received signal strengths from both APs, namely, $r_a(d)$ and $r_b(d)$, are given by [23]

$$r_a(d) = K_1 - K_2 \log(d) + u \tag{1}$$

$$r_b(d) = K_1 - K_2 \log(D-d) + v \tag{2}$$

where $0 \le d \le D$. Constants K_1 and K_2 are the parameters for path loss in an 802.11a WLAN environment. We consider that the STA measures the signal strength periodically with a given time interval $(= C_T)$. It is practical since typical APs broadcast their beacon frames in a period of 100 ms. The measured signal strengths are expressed by $r_a(iC_TC_V)$ and $r_b(iC_TC_V)$ at the ith measurement instant, where $i \ge 0$. For simplicity, we adopt new notations, namely, $r_a^{(i)}$ and $r_b^{(i)}$, corresponding to both the measured signal strengths. u and v are independent and identically distributed zero-mean stationary Gaussian random processes [24]. In other words, (1) and (2) imply that the received signal strength $r_a(d)$ (or $r_b(d)$) may be different at even the same location since u (or v) varies with time. Considering that u has a distribution identical to that of v, we can obtain the random variables for the received signaling strength from (1) and (2) by

$$r_a^{(i)} = \bar{r}_a^{(i)} + u \tag{3}$$

$$r_b^{(i)} = \bar{r}_b^{(i)} + u \tag{4}$$

where $\bar{r}_a^{(i)} = K_1 - K_2 \log(iC_TC_V)$, and $\bar{r}_b^{(i)} = K_1 - K_2 \log(D - iC_TC_V)$. From (3) and (4), we can obtain the probability density functions for random variables $r_a^{(i)}$ and $r_b^{(i)}$ by

$$P_{r_a}^{(i)}(r_a) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{\left(r_a - \bar{r}_a^{(i)}\right)^2}{2\sigma^2}\right) \tag{5}$$

$$P_{r_b}^{(i)}(r_b) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{\left(r_b - \bar{r}_b^{(i)}\right)^2}{2\sigma^2}\right). \tag{6}$$

In our analysis, the 802.11 scanning begins when the received signal strength drops below threshold C_h. Then, the STA conducts a handoff when the received signal strength of a neighboring AP is higher than that of the currently associated AP. Let $P_A^{(i)}$ (or $P_B^{(i)}$) represent the probability that the STA is associated with the AP A (or AP B) immediately after the ith measurement. Therefore, we can derive the scanning probability $P_s^{(i)}$ for the ith interval by

$$\begin{aligned} P_s^{(i)} &= P_{s|A}^{(i)} + P_{s|B}^{(i)} \\ &= P\left(C_h > r_a^{(i)}\right) P_A^{(i-1)} + P\left(C_h > r_b^{(i)}\right) P_B^{(i-1)} \end{aligned} \tag{7}$$

where $P_A^{(0)} = 1$, and $P_B^{(0)} = 0$. We continue to derive $P(C_h > r_a^{(i)})$ by

$$\begin{aligned} P\left(C_h > r_a^{(i)}\right) &= \int_{-\infty}^{C_h} P_{r_a}^{(i)}(r_a)\, dr_a \\ &= \int_{-\infty}^{C_h} \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{\left(r_a - \bar{r}_a^{(i)}\right)^2}{2\sigma^2}\right) dr_a \\ &= \frac{1}{2}\left(1 + \operatorname{erf}\left(\frac{C_h - \bar{r}_a^{(i)}}{\sqrt{2}\sigma}\right)\right) \end{aligned} \tag{8}$$

where the error function $\operatorname{erf}(r) = (2/\sqrt{\pi}) \int_0^r \exp(-x^2) dx$. Similarly, we have $P(C_h > r_b^{(i)})$ by

$$P\left(C_h > r_b^{(i)}\right) = \frac{1}{2}\left(1 + \operatorname{erf}\left(\frac{C_h - \bar{r}_b^{(i)}}{\sqrt{2}\sigma}\right)\right). \tag{9}$$

There are two cases for the STA associated to an AP after the ith measurement instant: 1) The STA hands off to the AP when it recognizes that the AP provides better signal quality by scanning, or 2) it stays with the AP since the received signal is stronger than C_h. For this reason, we can derive $P_A^{(i)}$ and $P_B^{(i)}$ from (7)–(9) by

$$\begin{aligned} P_A^{(i)} &= P_s^{(i)} P\left(r_a^{(i)} > r_b^{(i)}\right) \\ &\quad + \left(1 - P\left(C_h > r_a^{(i)}\right)\right) P_A^{(i-1)}, \qquad i > 0 \end{aligned} \tag{10}$$

$$\begin{aligned} P_B^{(i)} &= P_s^{(i)} P\left(r_b^{(i)} > r_a^{(i)}\right) \\ &\quad + \left(1 - P\left(C_h > r_b^{(i)}\right)\right) P_B^{(i-1)}, \qquad i > 0. \end{aligned} \tag{11}$$

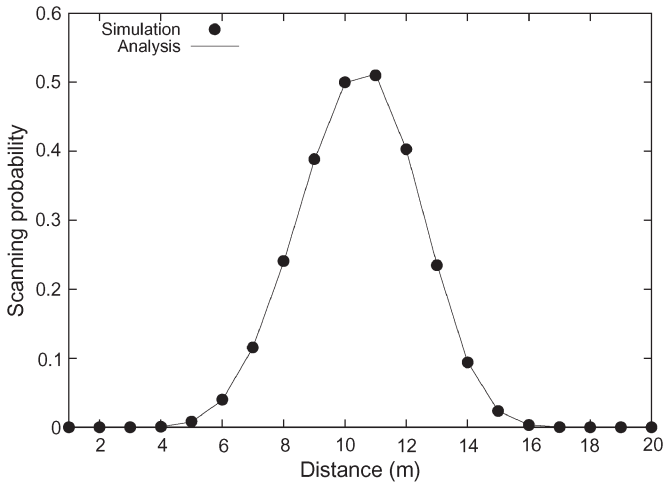

Fig. 13. Scanning probability when an STA travels from AP A to AP B.

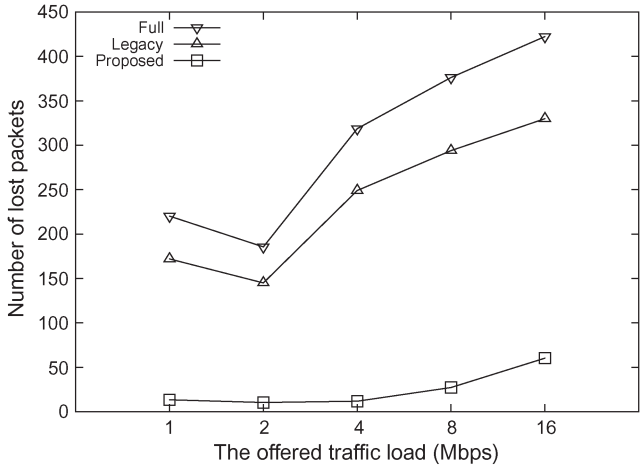

Fig. 14. Expected number of packet losses while an STA moves from AP A to AP B.

Since $r_a^{(i)}$ and $r_b^{(i)}$ follow Gaussian distributions, we can derive $P(r_a^{(i)} > r_b^{(i)})$ by

$$\begin{aligned} P\left(r_a^{(i)} > r_b^{(i)}\right) &= \int_{-\infty}^{\infty}\int_{r_b}^{\infty} P_{r_a}^{(i)}(r_a)P_{r_b}^{(i)}(r_b)\,dr_a\,dr_b \\ &= \int_{-\infty}^{\infty}\int_{r_b}^{\infty} \frac{1}{\sigma\sqrt{2\pi}}\exp\left(-\frac{\left(r_a-\bar{r}_a^{(i)}\right)^2}{2\sigma^2}\right) dr_a P_{r_b}^{(i)}(r_b)\,dr_b \\ &= \int_{-\infty}^{\infty} \frac{1}{2}\mathrm{erfc}\left(\frac{r_b-\bar{r}_a^{(i)}}{\sqrt{2}\sigma}\right) P_{r_b}^{(i)}(r_b)\,dr_b \end{aligned} \quad (12)$$

where the complementary error function $\mathrm{erfc}(r) = 1 - \mathrm{erf}(r)$. In the same way to the derivations for this equation, we have $P(r_b^{(i)} > r_a^{(i)})$ by

$$\begin{aligned} P\left(r_b^{(i)} > r_a^{(i)}\right) &= \int_{-\infty}^{\infty}\int_{r_a}^{\infty} P_{r_b}^{(i)}(r_b)P_{r_a}^{(i)}(r_a)\,dr_b\,dr_a \\ &= \int_{-\infty}^{\infty} \frac{1}{2}\mathrm{erfc}\left(\frac{r_a-\bar{r}_b^{(i)}}{\sqrt{2}\sigma}\right) P_{r_a}^{(i)}(r_a)\,dr_a. \end{aligned} \quad (13)$$

Now, we validate the analytical modeling by comparing it with the simulation results. For this purpose, we build a simulator in the *Matlab* environment. For this validation, we use $K_1 = -23.42$, $K_2 = 47.5$, and $\sigma = 5.97$, as indicated in [24]. We run the simulation more than a million times with the maximum transmission power ($= 23$ dBm) allowed for the 802.11a WLANs. The handoff threshold C_h is set to -70.92 dBm. Fig. 13 shows the scanning probabilities while an STA travels from AP A to AP B. As shown in Fig. 13, the analytical results match well with simulation results. It implies that the scanning probability equation (7) is correctly derived. With this equation and the experimental results, we continue the equation derivations to estimate the packet losses during each handoff operation.

Let N_p denote the number of packet losses when an STA conducts the MWNIC scanning once. Then, we can have the expected number of packet losses for the proposed handoff from (7) by

$$\sum_{i=0}^{\lfloor D/(C_T C_V)\rfloor} N_p P_s^{(i)}. \quad (14)$$

Note that we need to consider the full scanning scheme since it is a typical scanning scheme for the 802.11 WLANs. As explained in Section IV-A, an STA with a legacy handoff conducts a background scanning in each group of available 802.11a channels in turn. Let N_f be the number of lost packets for a full scanning at a time. Since there are five groups for the 802.11a channels in the madwifi, we estimate $N_f = N_b \times 5$, where N_b is the number of packet losses for background scanning. We can derive the expected number of lost packets for the handoff with full scanning by

$$\sum_{i=0}^{\lfloor D/(C_T C_V)\rfloor} N_f P_s^{(i)}. \quad (15)$$

However, an STA employing the legacy handoff should perform scanning in a predefined period; hence, the number of packet losses is derived by

$$\sum_{i=0}^{\lfloor D/(C_P C_V)\rfloor} N_b \quad (16)$$

where C_P is the predefined period for the background scanning. For our evaluations, we set D, C_V, C_T, and C_P to 20 m, 1 m/s, 1 s, and 2 s. Additionally, N_p and N_b are configured with the obtained results, depending on the offered traffic load in Fig. 11.

Fig. 14 shows the estimated number of packet losses while an STA travels from AP A to AP B. In this figure, *proposed*, *legacy*, and *full* represent the proposed handoff, the legacy handoff, and the handoff with full scanning. We can find the proposed handoff requires fewer packet losses than any other handoff schemes. Fig. 14 also shows that the handoff with full scanning incurs more packet losses compared with the legacy handoff.

VI. Conclusion

We have proposed a novel scanning scheme for the 802.11 handoff and then implemented the proposed scanning scheme

with madwifi. The experimental results show that the proposed scanning scheme greatly reduces data frame losses, whereas the scanning time remains unchanged. We have estimated the number of packet losses depending on the handoff schemes by numerically analyzing the performance of the handoff schemes. In summary, the proposed scanning scheme is useful for the application such as voice over IP and multimedia streaming services since those applications are quite sensitive to data frame losses. In addition, we demonstrate that the proposed scanning scheme is feasible to be used in practical life with implementation.

REFERENCES

[1] S. Jin, M. Choi, and S. Choi, "Multiple WNIC-based Handoff in IEEE 802.11 WLANs," *IEEE Commun. Lett.*, vol. 13, no. 10, pp. 752–754, Oct. 2009.

[2] S. Jin, K. Han, and S. Choi, "A novel Idle mode operation in IEEE 802.11 WLANs: Prototype implementation and empirical evaluation," in *Proc. ACM WMASH*, Sep. 2006, pp. 71–80.

[3] S. Jin, K. Han, and S. Choi, "A Novel Idle Mode Operation in IEEE 802.11 WLANs," in *Proc. IEEE ICC*, Jun. 2006, pp. 4824–4829.

[4] S. Jin, K. Han, and S. Choi, "Idle mode for deep power save in IEEE 802.11 WLANs," *J. Commun. Netw.*, vol. 12, no. 5, pp. 480–491, Oct. 2010.

[5] S. Kim, S. Choi, S.-k. Park, J. Lee, and S. Kim, "An empirical measurements-based analysis of public WLAN handoff operations," in *Proc. WILLOPAN*, Jan. 2006, pp. 1–6.

[6] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 33, no. 2, pp. 93–102, Apr. 2003.

[7] S. Jin, M. Choi, L. Wang, and S. Choi, "Fast scanning schemes for IEEE 802.11 WLANs in virtual AP environments," *Elsevier Comput. Netw.*, vol. 55, no. 10, pp. 2520–2533, Jul. 2011.

[8] V. Brik, A. Mishra, and S. Banerjee, "Eliminating handoff latencies in 802.11 wlans using multiple radios: Applications, experience, and evaluation," in *Proc. ACM SIGCOMM*, Aug. 2005, pp. 27–27.

[9] K. Ramachandran, S. Rangarajan, and C. J. Lin, "Make-before-break mac layer handoff in 802.11 wireless networks," in *Proc. IEEE ICC*, Jun. 2006, pp. 4818–4823.

[10] H. Wu, K. Tan, Y. Zhang, and Q. Zhang, "Proactive scan: Fast handoff with smart triggers for 802.11 wireless LAN," in *Proc. IEEE INFOCOM*, May 2007, pp. 749–757.

[11] Y.-S. Chen, M.-C. Chuang, and C.-K. Chen, "Deucescan: Deuce-based fast handoff scheme in IEEE 802.11 wireless networks," *IEEE Trans. Veh. Technol.*, vol. 57, no. 2, pp. 1126–1141, Mar. 2008.

[12] S.-H. Park, H.-S. Kim, C.-S. Park, J.-W. Kim, and S.-J. Ko, "Selective channel scanning for fast handoff in wireless LAN using neighbor graph," in *Proc. Pers. Wireless Commun.*, Jul. 2004, pp. 194–203.

[13] I. Ramani and S. Stephan, "SyncScan: Practical fast handoff for 802.11 infrastructure networks," in *Proc. IEEE INFOCOM*, Mar. 2005, pp. 675–684.

[14] M. Shin, A. Mishra, and W. Arbaugh, "Improving the latency of 802.11 hand-offs using neighbor graphs," in *Proc. ACM MobiSys*, Jun. 2004, pp. 70–83.

[15] H. Velayos and G. Karlsson, "Techniques to reduce the IEEE 802.11b handoff time," in *Proc. IEEE ICC*, Jun. 2004, pp. 3844–3848.

[16] A. Mishra, M. Shin, and W. Arbaugh, "Context caching using neighbor graphs for fast handoffs in a wireless network," in *Proc. IEEE INFOCOM*, Mar. 2004, pp. 351–361.

[17] S. Pack, H. Jung, T. Kwon, and Y. Choi, "SNC: A selective neighbor caching scheme for fast handoff in IEEE 802.11 wireless networks," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 9, no. 4, pp. 39–49, Oct. 2005.

[18] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, (Revision of IEEE Std 802.11-1999)*, IEEE 802.11-2007, Jun. 2006.

[19] [Online]. Available: http://madwifi-project.org

[20] [Online]. Available: http://sourceforge.net/projects/iperf

[21] [Online]. Available: http://www.wireshark.org

[22] [Online]. Available: http://www.ntp.org

[23] R. Vijayan and J. M. Holtzman, "A model for analyzing handoff algorithms," *IEEE Trans. Veh. Technol.*, vol. 42, no. 3, pp. 351–356, Aug. 1993.

[24] D. Cheung and C. Prettie, "A path loss comparison between the 5 GHz UNII band (802.11 a) and the 2.4 GHz ISM band (802.11 b)," Intel Labs, Santa Clara, CA, USA, 2002.

Sunggeun Jin (M'08) received the B.S. and M.S. degrees from Kyungpook National University, Daegu, Korea, in 1996 and 1998, respectively, and the Ph.D. degree from Seoul National University, Seoul, Korea, in 2008.

In 1998, he joined the Electronics and Telecommunications Research Institute, Daejeon, Korea. He is currently an Assistant Professor with Daegu University, Gyeongsan, Korea. He has participated in standard developments, including IEEE 802.11v, IEEE 802.16j, IEEE 802.16m, IEEE 802.11ad, and IEEE 802.15.8. His research interests include implementation of wireless networks, including mobile Worldwide Interoperability for Microwave Access, Third-Generation Partnership Project Universal Mobile Telecommunications Systems, and Wi-Fi networks.

Sunghyun Choi (SM'05) received the B.S. (*summa cum laude*) and M.S. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, Korea, in 1992 and 1994, respectively, and the Ph.D. degree from the University of Michigan, Ann Arbor, MI, USA, in 1999.

For three years, he was a Senior Member Research Staff and a Project Leader with Phillips Research USA, Briarcliff Manor, NY, USA. Since 2002, he has been with Seoul National University, Seoul, Korea, where he is currently a Full Professor with the School of Electrical Engineering. From June 2009 to June 2010, he was also a Visiting Associate Professor with the Department of Electrical Engineering, Stanford University, Stanford, CA, USA. He is the author or coauthor of over 150 technical papers and book chapters in the areas of wireless/mobile networks and communications. He is the coauthor of *Broadband Wireless Access and Local Networks: Mobile WiMAX and WiFi* (Norwood, MA: Artech House, 2008). He is the holder of about 70 patents and has several patents pending. His current research interests include wireless/mobile networks with emphasis on wireless local area networks (WLAN), metropolitan area networks, and personal area networks; next-generation mobile networks; mesh networks; cognitive radios; and cross-layer approaches.

Dr. Choi was an active voting member of the IEEE 802.11 WLAN Working Group from 2000 to 2007. He is currently a member of the Association for Computer Machinery (ACM), the Korea Information and Computer Society, The Institute of Electronics Engineers of Korea (IEEK), and the Korean Institute of Information Scientists and Engineers. He served as a Technical Program Cochair for the Second ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (ACM WMASH) in 2004; the General Chair for the Third ACM WMASH in 2005; the Workshop Cochair for the First International Workshop on Wireless Personal and Local Area Networks in 2006; the Cochair for the Cross-Layer Designs and Protocols Symposium at the International Wireless Communications and Mobile Computing Conference in 2006, 2007, and 2008; the Technical Program Committee Cochair for the ACM International Conference on Multimedia, the IEEE International Symposium on a World of Wireless, Mobile, and Multimedia Networks, and the International Conference on Communication System Software and Middleware (COMSWARE) in 2007; the General Cochair for COMSWARE in 2008; and the Cochair for the IEEE Global Communications Conference Wireless Networking Symposium in 2011. He has also served on program and organization committees for numerous leading wireless and networking conferences, including the Annual International Conference on Mobile Computing and Networking (ACM MobiCom), the IEEE International Conference on Computer Communications, the IEEE Sensor and Ad Hoc Communications and Networks, the IEEE International Conference on Mobile Ad hoc and Sensor Systems, and the IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM). He is also currently a member of the editorial boards for the IEEE TRANSACTIONS ON MOBILE COMPUTING and IEEE WIRELESS COMMUNICATIONS and has served as an Editor for *ACM SIGMOBILE Mobile Computing and Communications Review*, the *Journal of Communications and Networks, Computer Networks*, and *Computer Communications*. He has served as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS; the IEEE WIRELESS COMMUNICATIONS, PERVASIVE, AND MOBILE COMPUTING; *ACM Wireless Networks; Wireless Personal Communications*; and *Wireless Communications and Mobile Computing*. He gave a tutorial on IEEE 802.11 at the ACM MobiCom in 2004 and at the IEEE International Conference on Communications in 2005. He has received numerous awards, including the Young Scientist Award from the President of Korea in 2008; the IEEK/IEEE Joint Award for Young Information Technology Engineers in 2007; the Outstanding Research Award in 2008 and the Best Teaching Award in 2006, both from the College of Engineering, Seoul National University; the Best Paper Award from IEEE WoWMoM in 2008; and the Recognition of Service Award in 2005 and 2007 from ACM. He received the Korea Foundation for Advanced Studies Scholarship and the Korean Government Overseas Scholarship for 1997–1999 and 1994–1997, respectively.