The Design of an AP-Based Handoff Scheme for IEEE 802.11 WLANs

Yi-Cheng Chan and Dai-Jiong Lin

***Abstract*—Handoff mechanism is an important issue in wireless networks since the incurring interrupts may be unsatisfactory to support fast real-time services with stringent Quality of Service (QoS) requirements such as Voice over IP (VoIP). In this paper, we propose a novel seamless handoff scheme for IEEE 802.11 networks by equipping Access Points (APs) with multiple Wireless Network Interface Cards (WNICs), one of which is set to operate for normal transmission and the others listen or receive STAtion(STA) packets for signal measurements. We place the handoff decision in the AP and transmit management frames between APs using Inter Access Point Protocol (IAPP). The proposed scheme is compatible with the existing STAs without any hardware modifications. The NS-2 simulation results demonstrate that our proposed scheme can reduce layer-2 handoff interrupt time effectively.**

***Index Terms*—IEEE 802.11, Layer 2 handoff, seamless handoff.**

I. Introduction

Due to the continued development of wireless communication technology and the growth of wireless clients in recent years, users have increasing demand for mobile networks. Wireless networks can be simply divided into two categories that are Wireless Wide Area Network (WWAN) and Wireless Local Area Network (WLAN) by its signal coverage area. The International Telecommunication Union (ITU) has approved LTE-advanced and WiMAX2 as two IMT Advanced family. Their Base Stations (BS) are both with larger coverage area as WWAN feature. Due to the large coverage area of a single BS, there must be weak signal problems like at indoor environments. Besides, single BS may not provide enough bandwidth at some hot spots where people crowded. IEEE 802.11 Wireless Local Area Networks (WLANs) is the solution to extend wired or wireless networks due to their rapid deployment, easy configuration and low cost hardware. In order to solve the aforementioned problems, lots of public regions (for example airport, school, and hospital) have deployed IEEE 802.11 Access Points (AP). Wireless devices can connect to Internet when they are in the coverage area of APs, and can move to anywhere inside the coverage area.

When the wireless device moves out to the coverage area of an AP, it should switch to another AP and interrupt the connection. This behavior is called handoff. The BSs of LTE-advanced and WiMAX2 both have the seamless handoff mechanism. During the handoff, it keeps the communication with less interruption time and has a better performance with delay sensitive applications like Voice over IP (VOIP). However, IEEE 802.11 WLANs do not have seamless handoff mechanism.

According to IEEE 802.11 standard [1], there are three steps in the handoff procedure, namely scanning, authentication, and reassociation. Scanning is a process to find a suitable AP to switch. There are two types of scanning. In the passive scanning, a STA switches its antenna to every channel and waits for beacons from APs. In the active scanning, a STA should send Probe Request frame and wait for Probe Response frames from APs in every channels. After scanning the STA would choose a suitable AP to authenticate and associate. The authentication is a process that an AP identifies a STA, and the association is a process that a STA makes a connection to the AP. During the handoff, the STA must disconnect with the original AP and switch to other channels for scanning. As previous studies [2], the aforementioned method would take about 200 *ms* to 1000 *ms* handoff interruption time according to different hardware. Such a large interruption time does not satisfy the seamless handoff requirement in the 4G standard [3], which should be 40 *ms* to 60 *ms*.

In order to provide a more efficient handoff mechanism for IEEE 802.11 WLANs, many schemes have been proposed. To improve the scanning process is the most common strategy such as prescan [4], selective scan [5], and use RTS frame for scanning [6]. The concept of Virtual Access Points (VAPs) [7], [8] are also proposed. All these schemes can reduce the handoff latency, however, the interruption time of communication is still too long. Therefore, we propose a new handoff scheme for IEEE 802.11 WLANs namely Multi-Interface Seamless Handoff (MISH). By equipping APs with multiple Wireless Network Interface Cards (WNICs) and place the handoff decision in the AP. The new designed management frames are exchanged between APs by IAPP [9]. In our scheme, the connection interruption occurs only at the period when the STA switches between channels.

II. Related Work

An IEEE 802.11 handoff consists of scanning, authentication, and reassociation. A scanning is a procedure to find the best available AP for handoff or a STA startup. There are two types defined in IEEE 802.11 standard namely active scanning and passive scanning. For passive scanning, a STA attempts to listen beacon frames which APs periodically transmit in each channel. For an active scanning, a STA broadcasts a Probe Request frame in each channel, and then waits a period time called *MinChannelTime* for Probe

Manuscript received June 17, 2013; revised August 13, 2013.

Y.-C. Chan and D.-J. Lin are with the Department of Computer Science and Information Engineering, National Changhua University of Education, Changhua 500, Taiwan (e-mail: ycchan@cc.ncue.edu.tw, achin178@gmail.com).

DOI: 10.7763/IJEEEE.2014.V4.305

Response frames from neighboring APs. If there is not any response from APs when the *MinChannelTime* exceed, the STA should broadcast a Probe Request frame in the next channel. If there are any Probe Response frame received by the STA in the *MinChannelTime* period, the STA must wait until *MaxChannelTime* in order to receive Probe Response frames from APs. Between switching channels, there is a latency which is called *ChannelSwitchingTime* required to switch. This value is an implementation-dependent factor influencing the scanning latency. The modern devices already support 200 *us* [10] and hence we consider 200 *us* for our evaluation later. An Open-System authentication is a mandatory mechanism. It only exchanges authentication request and authentication response between an AP and a STA during authentication process. We use Open-System authentication to simulate traditional handoff scheme for our evaluation. A reassociation is a procedure that a STA makes a connection with new AP. A STA transmits a Reassociation Request frame to the new AP and wait for a Reassociation Response frame form the AP. Once an AP receive Reassociation Request frame, it will do a Layer 2 update process. Finally the new AP will transmit a Reassociation Response frame to the STA and complete the handoff process.

The concept of Virtual Access Point (VAP) [7], [8] has been proposed recently. In their methods, they proposed to get rid of mobility management in mobile stations and put it entirely inside the network of interconnected access points. Every mobile station is therefore associated with its own virtual access point when it connects to the network, the latter moving along with its client. The concept of VAP achieved seamless handoff. The STA has an illusion of being almost static relatively because it always associated to a VAP with same BSSID and received corresponding beacons from the AP. Although VAP of [7] [8] brings advantage of mobility, there are still some limitations. One of the limitations is that APs have to switch channel to receive STA's packets. Once AP switches channel, the connection of STAs which are associated with this AP will be interrupted. It is not suitable for real environment.

The authors of [6] consider that the IEEE 802.11 scanning takes more than 300 *ms* to scan all channels in typical 802.11 WLANs. The reason for high scanning latency is rooted in non-optimized request-and-response operations relying on obscure waiting time in order to find neighboring APs. They proposed new scanning schemes with two phases: channel selection phase and AP search phase. The channel selection phase is used to select a best channel and then probe in the chosen channel to find a best AP to associate in the AP search phase. In channel selection phase, following IEEE 802.11 environment, the larger date rate will result in a shorter transmission distance. The authors utilize multiple RTS transmissions with incremental transmission rates. A scanning STA transmits an RTS frame at the lowest transmission rate first. If the STA senses the channel to be busy due to the corresponding CTS, it then transmits another RTS at the next higher data rate, with which the RTS transmission covers a shorter range. In this procedure, an AP receiving an RTS should reply a CTS frame at the lowest rate. If a STA can sense the channel to be busy due to CTS(s) corresponding to an RTS transmitted at a given data rate, it can expect that at least one AP exists within the transmission range of the data rate. Then it continues to increase the RTS transmission rate until it fails to sense the channel busy in order to determine the maximum achievable data rate in the channel. In order to achieve RTS/CTS handshaking in the channel selection phase, the procedure will be implemented in the virtual AP environment. Because the RTS frame is a unicast frame which needs a MAC address for destination, a single WNIC of each AP holds two different MAC addresses one of which is the shared address. Once the best channel is selected, the AP search phase is initiated. The STA sends a unicast Probe Request frame with shared address in the chosen channel. Once a virtual AP receives the Probe Request, it accesses the channel to transmit Probe Response frame, whose source address is set to its own unique MAC address, not the shared address.

The authors of [11] proposed an IEEE 802.11 handoff scheme by AP equipped with Multiple Wireless Network Interface Cards (Multi-WNICs). In a single AP, Multi-WNICs use the same BSSID, and thus STAs can roam across the Multi-WNICs without reassociation. In their protocol, a STA in a non-reserved channel performs a handoff by moving to the reserved channel. All three APs are equipped with two WNICs. Prior to a scanning, a STA transmits a null frame which is a data frame without a payload, with 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 to the STA. The STA switches its operating channel to the reserved channel for scanning. Thereafter, it transmits a null frame with PM bit set to 0 in order to make the serving AP forward buffered data frames. This procedure is feasible since the serving AP should have a WNIC operating in the reserved channel permanently. It enables the STA to receive data frames during scanning. The last steps are normal handoff procedure but scan only one channel which is reserved. After performing a reassociation for a new connection establishment with the chosen AP, consecutive null frames with PM bit set to 1 and 0 are transmitted in the reserved channel and a non-reserved channel, respectively, to prevent the loss of data frames during a channel switching. After a channel switching, the STA can exchange data frames with the new AP. The limitation of this scheme is the reserved channel which occupied a frequency channel and may result in interferences if there are multiple STAs.

III. The Proposed Scheme

Traditionally, the scanning step would take the most time of all handoff duration. A STA should wait a *MinChannelTime* when it sends a probe request frame, and then if there are any probe responses from any AP in the channel, the STA should wait a *MaxChannelTime* to receive all probe response frames of all APs in the channel. IEEE 802.11 standard did not define the *MinChannelTtime* and the *MaxChannelTime* explicitly but the traditional scheme usually takes it as 20 *ms* and 40 *ms*, respectively. This will generate a long interruption time.

In our scheme, APs are equipped with multiple WNICs [11] and the handoff decision is placed in the APs. The APs equipped with multiple WNICs keep data transmission without disconnect when handoff procedure occurs, and if the suitable AP is chosen, the old AP assigns the STA to the chosen AP. In order to realize the proposed scheme, we describe the proposed handoff procedure in details as Fig. 1.

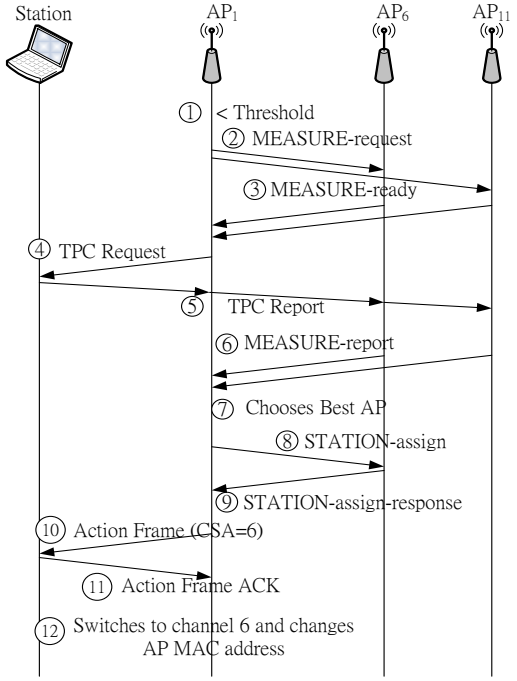

Fig. 1. The new handoff procedure.

In the Fig. 1, we suppose that every AP has multiple WNICs, and each WNIC operates on one of the nonoverlapped channels. Each AP sets one WNIC to do normal data transmission and the others are set to measure the signal of STAs in different channels. To realize the proposed protocol easily, we suppose the handoff is happened in IEEE 802.11b/g environment which have three nonoverlapped channels (1, 6, and 11), and the AP sets normal data transmission in channel 1 called AP_1 and in channel 6 or 11 are called AP_6 and AP_{11}, respectively. For example, AP_1 transmits normal data packets in channel 1 and the other WNICs are set to operate in channel 6 and 11. All APs are connected with each other by wired LAN, and all inter AP messages are transmitted by Inter Access Point Protocol (IAPP) [9].

When AP_1 that the STA associated detects one of the certain conditions of the STA is less than the predefined threshold, the AP_1 sends MEASURE-request frames which include the MAC address of the associated STA to its neighbor APs. The MEASURE-request frame is used to tell neighbor APs to ready for receiving the packet of the STA and measuring the signal strength of this packet. All APs that received the MEASURE-request frame should send back a MEASURE-ready frame for confirming and ready to receive a packet form the assigned STA. When AP_1 receives all MEASURE-ready frames, then AP_1 sends a Transmit Power Control (TPC) request [1] to trigger the STA sends out a TPC response. The TPC protocol is defined in IEEE 802.11h that all IEEE 802.11 devices should support it. Neighbor APs will receive this TPC report because they all have a WNIC works on this channel, and then measure the signal strength of this TPC report frame. The MEASURE-report frames are sent back to the AP_1. The MEASURE-report includes the received signal strength and the channel number of the WNIC of the AP which is set for normal data transmission. When AP_1 received all MEASURE-report frames, it should choose a suitable AP and then send a STATION-assign frame to the chosen AP. The STATION-assign frame includes the MAC address of the STA and the messages which is the STA's first authentication and association context to the AP_1. The STATION-assign frame is like a reassociation frame of traditional scheme of IEEE 802.11 handoff. Once received this frame, the AP needs to tell all layer 2 devices to update its forwarding table just like received a reassociation request frame. Here we suppose that the chosen AP is AP_6. As AP_6 received STATION-assign frame, it would send a STATION-assign-response to AP_1 in order to confirm whether the STATION-assign frame is received or not and assign an association ID for the STA in this frame. The AP_1 would send an action frame to the STA after it received the STATION-assign-response frame. The action frame includes a channel switch announcement element which declares the channel number that the STA should switch to according to the measure report frame. Besides, we design new element of the action frame which is used to notify the STA that it should change destination MAC address, receive the beacons from the new AP, and change its association ID. Once the STA received the action frame and switched to the assigned channel, the handoff procedure is completed. The STA will receive the beacons from the new AP and transmit data frames with new destination MAC address. If the STA does not send anything to the new AP for a while, the new AP can send a TPC request to make sure the association.

IV. Performance Evaluation

We develop a simulation model using ns2 to evaluate the proposed scheme. We consider the PHY characteristics of IEEE 802.11b and design a simple topology which is only three APs and one STA to simulate as Fig. 2. Furthermore, in order to correspond with realistic environments, we also design a grid topology with 16 APs and 3 random moved STAs as Fig. 3, and the channel switch time of all STAs is 200 *us* [10]. We compare our scheme with RTS scanning scheme [6] and the traditional scheme. The handoff interruption time is a period that a STA cannot exchange date packets with any AP during the handoff process.

The proposed scheme of [11] which is also using multiple WNICs has some limitation like degrading performance in multiple STAs environment, and a specified channel for handoff will occupy a nonoverlapped channel which is rare in IEEE 802.11 b/g 2.4GHz band. So we do not compare with the proposed method of [11]. The RTS scanning scheme uses RTS/CTS handshaking in the virtual AP environment with different data rates to scan and choose the best channel. The higher date rate will reduce transmission distance. If a STA sends a RTS fame with a high data rate and then receives a CTS frame from an AP, it means this channel has a higher

transmission quality AP. In the RTS scanning scheme, an STA probes only one channel at a time.

Fig. 4 shows the result in the simple topology with three handoff schemes. MISH represent our proposed scheme, and RTS_Scanning and Legacy is the RTS scanning scheme and traditional scheme, respectively. As mentioned before, the total interruption time in our proposed scheme is the channel switch time. The RTS_Scanning consumes about 35 *ms* and that of the Legacy is more than 300 *ms*.

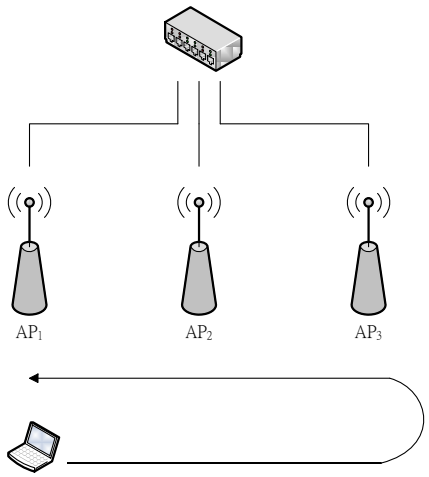

Fig. 2. The simple topology.

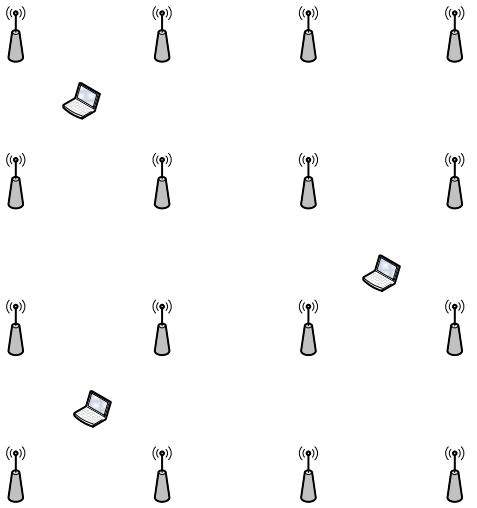

Fig. 3. The grid topology.

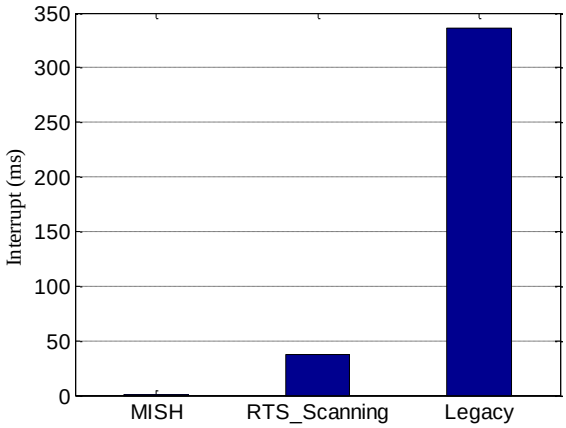

Fig. 4. The handoff interruption time in the simple topology.

Fig. 5 is the result in the grid topology. The interruption time of our proposed scheme still only take 200 *us* because the AP manage most handoff procedures and STAs only needs to switch channel. The RTS_Scanning consumes more 10 *ms* than that in the simple topology because the multiple STAs interfere with each other. The Legacy scheme still takes too much time to handoff.

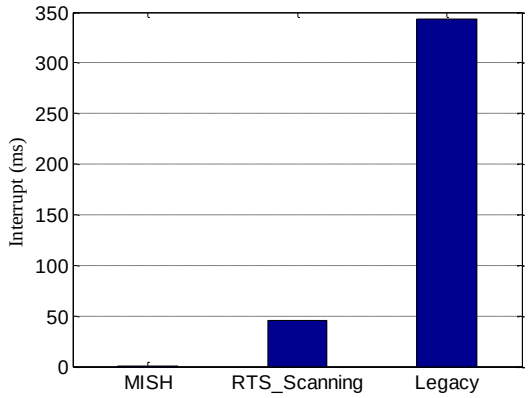

Fig. 5. The handoff interruption time in the grid topology.

We compare handoff duration using the proposed scheme in different topologies and show the results in the Fig. 6. The handoff duration is the period of the first management frame to the handoff completed.

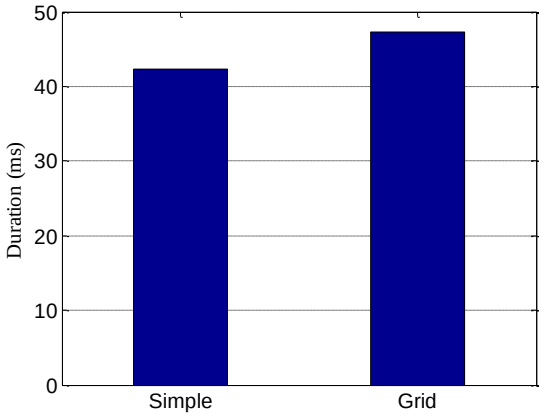

Fig. 6. The handoff duration time in the different topologies.

The proposed scheme spent 42.7 *ms* in the simple topology and 47.3 *ms* in the grid topology. There is about 5 *ms* differences between the results in two topologies. When an AP sends a MEASURE-request frame, it should wait all MEASURE-ready frames from neighbor APs in the topology, thus more APs will result in more duration time. Even though the duration time will be longer in more AP environment, but the interruption time is still a channel switch time.

V. Conclusions

Mobility management is an important problem of the IEEE 802.11 wireless networks. The IEEE 802.11 standard did not define a satisfying seamless handoff scheme to support fast real-time services. The current proposed mechanisms also do not provide a high performance result because of the long interruption time.

Our proposed scheme uses multiple WNICs and places the handoff decision in the APs without modifying the hardware of existing STAs. We design a new handoff protocol and

management frames. The most management frames which are transmitted between APs by IAPP resulted in a short delay time consuming. The connection interruption only occurred when the STA switched between channels. The handoff interruption time will depend on channel switch time which is a device-dependent factor.

Through the simulations we can find that the proposed scheme outperforms the others schemes in terms of handoff interruption time. The interruption time of our proposed scheme is about 200 *us* which conforms the requirements defined in 4G standard. This feature may fulfill the real-time applications with stringent delay requirements.

REFERENCES

[1] IEEE 802.11 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.

[2] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 2, pp. 93-102, Jan. 2003.

[3] D. Singhal, M. Kunapareddy, V. Chetlapalli, V. B. James, and N. Akhtar, "LTE-Advanced: Handover interruption time analysis for IMT-A evaluation," in *Proc. International Conference on Signal Processing, Communication, Computing and Networking Technologies*, July 2011, pp. 81-85.

[4] M. Yoon *et al.*, "AdaptiveScan: The fast Layer-2 handoff for WLAN," in *Proc. Eighth International Conference on Information Technology: New Generations*, April 2011, pp. 106-111.

[5] Y. Yen, R. Chang, and T. Wu, "A seamless handoff scheme for IEEE 802.11 wireless networks," in *Proc. 5th International ICST Conference on Communications and Networking in Chin*a, Aug. 2010, pp. 1-5.

[6] S. Jin, M. Choi, L. Wang, and S. Choi, "Fast scanning schemes for IEEE 802.11 WLANs in virtual AP environments," *Computer Networks*, vol. 55, pp. 2520–2533, July 2011.

[7] M. E. Berezin, F. Rousseau, and A. Duda, "Multichannel virtual access points for seamless handoffs in IEEE 802.11 wireless networks," in *Proc. IEEE 73rd Vehicular Technology Conference (VTC Spring)*, May 2011, pp. 1-5.

[8] Y. Grunenberger and F. Rousseau, "Virtual access points for transparent mobility in wireless LANs," in *Proc. IEEE Wireless Communications and Networking Conference*, April 2010, pp. 1-6.

[9] 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.

[10] A. Mishra, V. Shrivastava, D. Agrawal, and S. Ganguly, "Distributed channel management in uncoordinated wireless environments," *ACM MobiCom'06*, September 2006, pp. 170-181.

[11] S. Jin, M. Choi, and S. Choi, "Multiple WNIC-based handoff in IEEE 802.11 WLANs," *IEEE Communication Letters*, vol. 13, no. 10, pp. 751-754, October 2009.

Yi-Cheng Chan received his Ph.D. degree in computer science and information engineering from National Chiao Tung University, Taiwan in 2004. He is now an associate professor in the department of computer science and information engineering, National Changhua University of Education, Taiwan. His research interests include the design and analysis of network protocols, wireless networks, and active queue management.

Dai-Jiong Lin is currently prusuing the M.S. degree in computer science and information engineering at National Changhua University of Education, Taiwan. His research interest focuses on the protocol enhancement of WLANs.