Fast Handover Techniques for ESS-Subnet Topology Mismatch in IEEE 802.11

Chien-Chao Tseng*, Chia-Liang Lin*, Yu-Jen Chang* and Li-Hsing Yen†
*Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan, R.O.C.
E-mail: {cctseng, cllin}@cs.nctu.edu.tw, redeyes2015@gmail.com Tel: +886-3-5712121#31867
†Department of Computer Science and Information Engineering, National University of Kaohsiung, Kaohsiung, Taiwan, R.O.C.
E-mail: lhyen@nuk.edu.tw Tel: +886-7-5919452

***Abstract*—With the advances in wireless communication technology, mobile applications are gradually being introduced as part of our life. IEEE 802.11 is one of the most popular wireless communication technologies. Prior studies toward layer-2 and layer-3 handoffs assume that Extend Service Set (ESS) exactly matches a dedicated subnet. However, an inter-ESS with intra-subnet handoff and an intra-ESS with inter-subnet handoff may also be possible. Such mismatching ESS-subnet configurations result in performance degradation. This paper proposes FCS, a Further Check Scheme which detects the change of subnet after an intra-ESS handoff and eliminates unnecessary handoff latency after an inter-ESS handoff. The experimental results show that FCS outperforms the conventional implementation of NetworkManager under Linux in terms of handoff latency.**

I. INTRODUCTION

Wireless communication has emerged as the mainstream of network applications and has gained immense popularity in recent years. Wireless communication can not only avoid the expense of infrastructure deployment but also enable a variety of mobile applications. IEEE 802.11 is one of the most popular wireless communication technologies. However, mobile stations (MS) suffer from mismatching extended service subset (ESS)-subnet handoffs over IEEE 802.11 [1].

After associating with IEEE 802.11 access point (AP), a MS residing in a wireless local area network (WLAN) can then send packets through the wired infrastructure. In case of the associated AP is no longer available, the MS should discover and associate with another AP to continue its traffic. The process of changing its attached AP is called a layer-2 handoff, while a layer-3 handoff captures the case when the layer-2 handoff involves a change of network domains (i.e., renew network settings with that link).

The basic unit of an IEEE 802.11 WLAN is the basic service set (BSS). A single AP along with all associated MSs is called a BSS. The AP acts as a master to control the MSs within that BSS. A conventional BSS usually connects to a wired infrastructure. An Extended Service Set (ESS) consists of one or more interconnected BSSs that are configured with the same Service Set Identifier (SSID). Most ESSs are configured in accordance with the hierarchy of access networks to ease network management. However, SSIDs and subnets are in fact two independent configuration settings (one layer-2 and the other layer-3).

The layer-2 handoff may be inter-ESS (erESS) or intra-ESS (raESS) and each type of layer-2 handoff could further divided into intra-subnet (raSubnet) and inter-subnet (er-Subnet) layer-3 handoff, as Table I illustrates. Among four combinations of layer-2 handoff and layer-3 handoff, Intra-ESS/Inter-subnet (raESS/erSubnet) and Inter-ESS/Intra-subnet (erESS/raSubnet) are mismatching ESS-subnet handoffs. A raESS/erSubnet handoff specifies the case that the old and new APs are in the same ESS but different subnets, while an erESS/raSubnet handoff identifies the change of ESS but within the same subnet.

A typical example of mismatching ESS-subnet configuration is a campus wide or city wide wireless infrastructure [1]. This kind of infrastructure may deploy hundreds or thousands of APs and thus, it is impossible to configure all APs in the same subnet. Although these APs may reside in different subnet, they share the same SSID for an identical identification to roaming users. Therefore, a MS may reassociate with the same ESS but different subnet. The authors in [1] also identified another type of mismatch on campus network. A user may be authorized to access different ESS which belongs to different department or laboratory within the same subnet. This scenario captures the case of changing ESS without modifying its network setting.

To reduce the handoff latency caused by mismatching ESS-subnet configuration, this study first analyzes the network behavior of 802.11 in Linux and then proposes a Further Check Scheme (FCS). FCS tailors solutions for both raESS/erSubnet and erESS/raSubnet handoffs. FCS performs a further layer-3 topology check to find if MS moves into a new subnet after a layer-2 handoff. In the case of raESS/erSubnet handoff, MS can detect the change of subnet

TABLE I
HANDOFFS UNDER DIFFERENT ESS-SUBNET SETTINGS.

	Layer-2 Handoff	
Layer-3 Handoff	Intra-ESS (raESS)	Inter-ESS (erESS)
Intra-subnet (raSunet)	Intra-ESS/Intra-subnet (raESS/raSubnet)	Inter-ESS/Intra-subnet (erESS/raSubnet)
Inter-subnet (erSubnet)	Intra-ESS/Inter-subnet (raESS/erSubnet)	Inter-ESS/Inter-subnet (erESS/erSubnet)

and renew its network settings accordingly. FCS utilizes Address Resolution Protocol (ARP) to identify raSubnet and erSubnet handoffs. After sending an ARP request to the IP address associated with previous gateway, the recipient of ARP reply represents a raSubnet handoff while a timeout indicates an erSubnet handoff. When MS moves to a different ESS, in addition to Dynamic Host Configuration Protocol (DHCP), it also conducts gateway probing and cancels DHCP if the APR reply from previous gateway has received.

The remainder of this paper is organized as follows. We first describe background of handoff behaviors in 802.11 and then introduce the mismatching ESS-subnet handoffs in IEEE 802.11. In the following sections, we will describe the design of FCS, present the setup of experiments and analyze the experimental results. We summarize our findings in the final section.

II. BACKGROUND

MSs equipped with IEEE 802.11 network interfaces can send IP packets through APs to the Internet. When a MS detects poor link performance (e.g., low received signal strength or high frame error rate), the MS may decide to change its attached AP to another in order to retain its sessions (Fig. 1). The link-switch process is called a layer-2 handoff and involves AP probe, authentication, and association phases in 802.11 networks. A MS discovers available APs through either an active or a passive scan in the probe phase. Active scan allows a MS broadcasting probe request message with a particular service set identifier (SSID) in dedicated channels. If the SSID matches an AP's configuration, the AP responds with a probe response to the MS and makes the MS aware of its presence. In addition to active scan, a passive scan is also possible for the MS. The MS does not issue any message but listens to beacon messages broadcasted periodically by APs. After retrieving AP information from the probe response or beacon message, the MS selects a new AP as the target for handoff. In the following phase, the MS performs 802.11 authentication and exchanges 802.11 authentication messages with the AP. Then MS sends a reassociation request to the selected AP and receives a reassociation response replied by the AP to conclude the 802.11 handoff process.

Handoff may also be triggered at higher layers. If the handoff involves changing network domains (i.e., an erSubnet handoff), the MS must acquire a new IP address via schemes such as the Dynamic Host Configuration Protocol (DHCP) in the new subnet, possibly Duplicate Address Detection (DAD), and then configure its IP address.

DHCP operation involves four basic phases: IP discovery, IP lease offer, IP request, and IP lease acknowledgment. The MS broadcasts messages on the subnet to discover available DHCP servers in the DHCP discovery phase. In the following DHCP offer phase, when a DHCP server receives an IP lease request from a MS, it reserves an IP address and extends an IP lease offer by sending a DHCPOFFER message to the client. DHCP request phase allows the MS replying with a DHCP request for requesting the offered address in response to the

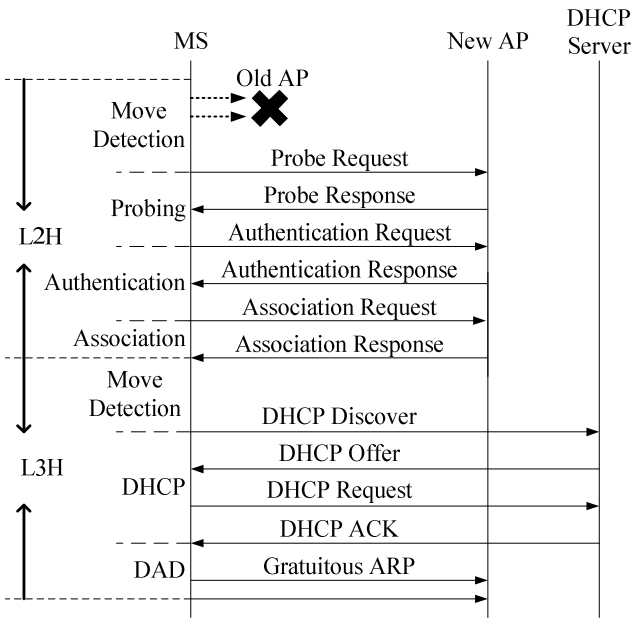

Fig. 1 General layer-2 handoff and layer-3 handoff in IEEE 802.11.

DHCP offer. When the DHCP server receives the DHCPREQUEST message from the MS, the server sends a DHCPACK packet to the MS to complete the configuration process.

DAD is responsible for preventing different MSs from acquiring the same IP address and therefore interfere communication among them. The current DAD utilizes Internet Control Message Protocol (ICMP) echo request and reply to conduct testing and incurs in a delay on the order of one second.

The judgment of the need for a layer-3 handoff after a layer-2 handoff is layer-3 handoff detection. However, the rule of performing a layer-3 handoff detection is not standardized. Most of the implementations utilize some layer-2 event to trigger layer-3 handoffs and thus, such event is identified as the layer-2 trigger [2]. The selection of an ideal layer-2 event as the trigger is that such event always followed by the need for a layer-3 handoff. A link-down event indicates a loss of link connectivity with the currently attached AP. If the loss of connectivity comes from a change of access network across different network domains, the link-down event will be a promising choice for the trigger. However, link-down events may also arise from other causes. ESS transition is one of such causes. Furthermore, a layer-3 handoff should be performed without link-down event is also possible. The raESS/erSubnet handoff shown in Table I is one such example. Therefore, the link-down event is not an ideal L2 trigger. On the other hand, a link-up event simply indicates an attachment to a new AP. It should signal a layer-3 handoff only in case of erSubnet handoffs, while an erESS/raSubnet handoff is not applicable. Therefore, link-up event alone is not an ideal trigger for layer-3 handoffs. Unfortunately, link-down or similar event (e.g., Link-To-Be-Down [3],

Link_Going_Down [4]) has been misinterpreted as an appropriate (and sometimes the only) layer-2 trigger.

III. FURTHER CHECK SCHEME (FCS)

As we are interested in actual performance of real systems, it is crucial to understand how the raESS/erSubnet and erESS/raSubnet handoffs are dealt with by the FCS in practice. Since Linux is an open source operating system, this study utilizes Linux as the underlying system to implement FCS. NetworkManager [5] is a software utility designed to simplify the use of computer networks on Linux-based and other Unix-like operating systems. NetworkManager is a dynamic network control and configuration tool that provides automatic network detection and configuration for the system. It also attempts to keep network device up and connections active when they are available. After enabling the daemon of NetworkManager, it also monitors the network interfaces and automatically switches to the best connection at any given time. Applications that support NetworkManager may also automatically switch between on and off modes when the system gets or loses network connectivity. Such facilities are most useful for mobile devices with multi network interface, where the user may move between wireless networks and plug into a variety of wired networks. Besides, NetworkManager also provides features that are relevant to workstations. Current versions of NetworkManager support not only modem connections but also certain types of VPN.

NetworkManager stores the information of connections to the internet. A wireless connection in IEEE 802.11 may contain an ESSID and a key for authentication. As long as NetworkManager initiate a wireless connection successfully, it will record such connection information. NetworkManager could use the connection information to establish a wireless link with an AP automatically when booting up. Fig. 2 shows the operation of NetworkManager with WLAN interface. After initiating the WALN interface, NetworkManager stays at Device Disconnected state and tries each AP on the list to establish a wireless link. When NetworkManager has

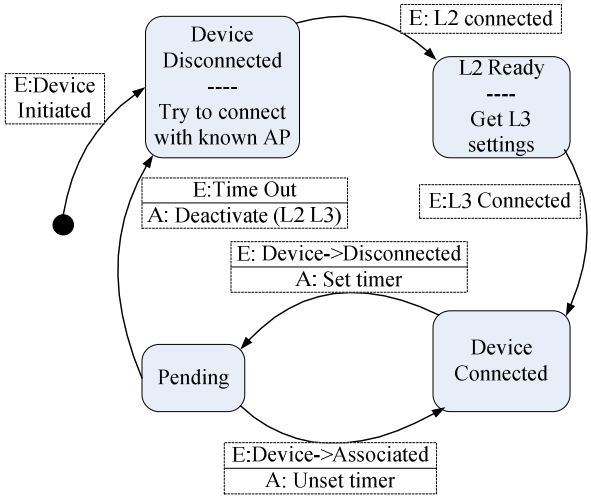

Fig. 2 The operation of NetworkManager with WLAN interface.

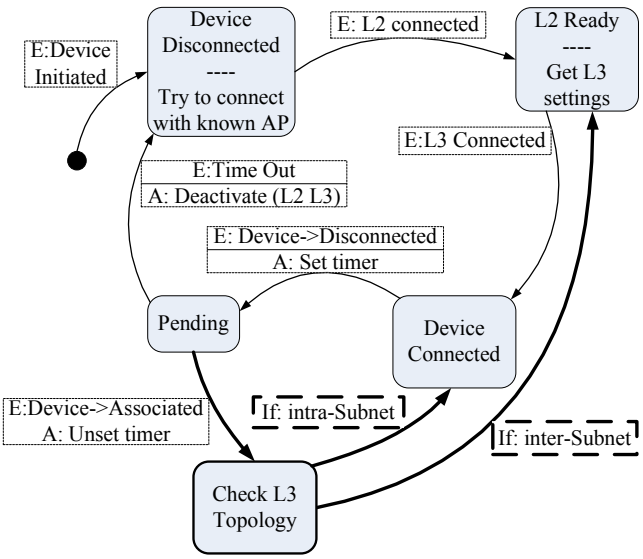

Fig. 3. The Operation of NetworkManager with FCS.

established a link with an AP, it enters L2 Ready state. Meanwhile, NetworkManager will retrieve layer-3 setting from connection information. Following state Device Connected indicates that NetworkManager has connected to the internet successfully. When the wireless link breaks, NetworkManager will set a timer and enter Pending state. If NetworkManager resumes the connectivity, it will return to Device Connected state again. On the other hand, a timeout indicates the loss of connectivity and NetworkManager will enter Device Disconnected state and try connecting to a new AP.

A. FCS for Intra-ESS/Inter-subnet Handoff

Although a raESS/erSubnet handoff results in the same ESSID, the wireless link with old AP breaks and resumes with a new AP. Refer to Fig. 2, the disconnection of wireless link makes NetworkManager enter pending state, and the establishment of connection allows NetworkManager moving back to Device Connected state. Hence, a layer-2 trigger erSubnet handoff will not be initiated by NetworkManager. If the subnets of the old AP and the new AP are different, NetworkManager will continue using the old layer-3 setting which results in mismatching ESS-subnet handoff.

As Fig. 3 illustrates, when NetworkManager resumes its wireless link, it enters the Check L3 Topology state. Then NetworkManager sends an ARP request to the IP address

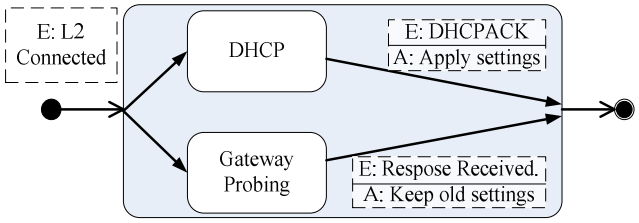

Fig. 4 The FCS Operation for erESS/raSubnet handoff.

TABLE II
DEVICES USED IN THE EXPERIMENTS.

	Model	Operating System
Mobile Station (MS)	ASUS W5000	Ubuntu 10.04
Access Point (AP) *2	ASUS RT-N1	N/A
Corresponding Node (CN)	Desktop PC	Ubuntu 10.04

associated with the previous gateway. The recipient of ARP reply represents a raSubnet handoff and NetworkManager enters Device Connected state again, while a timeout indicates an erSubnet handoff and NetworkManager moves to L2 Ready state for subsequent operation.

B. *FCS for Inter-ESS/Intra-subnet Handoff*

After performing an erESS handoff, NetworkManager will receive a new ESSID. As Fig. 2 illustrates, a new ESSID means that NetworkManager moves from Pending state to Device Disconnected state and thus, the layer-3 setting will be flushed. However, the information of layer-3 setting should still be valid after erESS/raSubnet handoff since the subnet remains the same. As a result, NetworkManager performs DHCP again and induces unnecessary handoff latency.

As Fig. 4 shows, FCS allows NetworkManager performing DHCP and sending an APR request to probe the previous gateway at the same time. If NetworkManager receives the ARP request from the previous gateway, it will cancel performing DHCP because of raSubnet handoff. Otherwise, the layer-3 setting from DHCP server is chosen for NetworkManager.

IV. EXPERIMENTAL RESULTS

To study the performance of the proposed approach and compare it with the other alternative, we construct an experimental environment with off-the-shelf APs. Table II lists the equipments required for the following experiments. In this section, we first describe the setup of experimental environment. Then we present the experimental results of raESS/erSubnet handoff with FCS and the latency when MS probes the gateway.

A. *Experimnetal Environment Setup*

As Fig. 5 illustrates, the setup of experimental environment contains two APs. Both AP1 and AP2 can

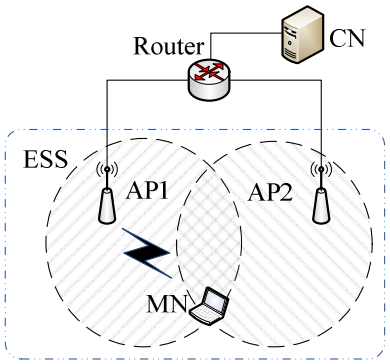

Fig. 5 Experimental Environment.

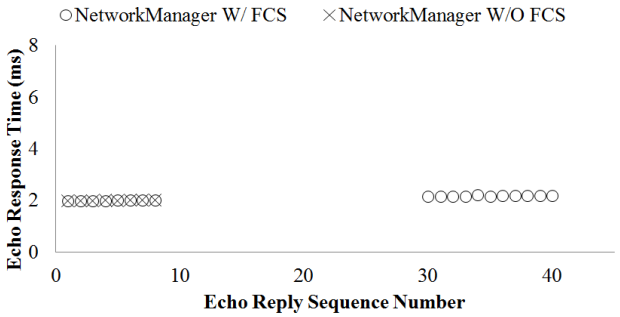

Fig. 6 Intra-ESS/Inter-Subnet handoff latency of mobile station.

connect to a router with different subnets and set with identical ESSID (raESS/erSubnet). On the other hand, AP1 and AP2 may also be configured to share the same subnet but different ESSIDs (erESS/raSubnet).

B. *Intra-ESS/Inter-Subnet Handoff with FCS*

This experiment aims to identify the effectiveness of FCS when performing a raESS/erSubnet handoff. As Fig. 5 shows, AP1 and AP2 share the same ESSID but are configured with different subnets. MS first connects to AP1 and send ICMP echo requests to probe CN periodically. CN will respond MS with ICMP echo reply on receiving each echo request. Then we shut AP1 down and MS starts creating a link with AP2. The experimental results show that NetworkManager with FCS continues receiving echo replies after handoff because NetworkManager can detect the change of subnet. FCS allows NetworkManager sending ARP requests to the IP address associated with previous gateway and thus identifies the erSubnet handoff.

C. *Gateway Probing Latency of NetworkManager with FCS*

Since FCS sends APR requests to probe the previous gateway after handoff, the timeout of each probing request should be clarified. MS in this experiment sends an APR request to previous gateway after handoff every second and total 1000 ARP requests are sent. As Fig. 7 shows, 95% of ARP requests are received within 20 ms and 99% are received

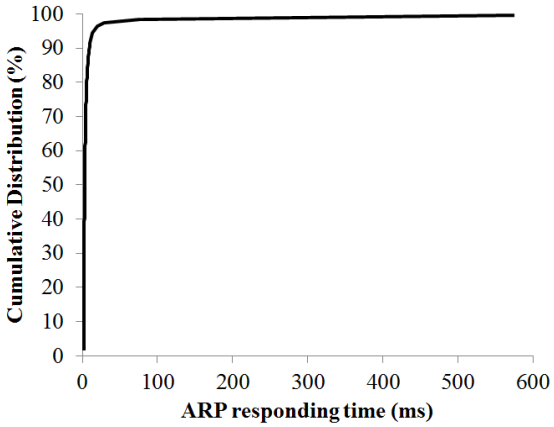

Fig. 7 The operation of NetworkManager with WLAN interface.

within 100ms. As a result, a timeout with 100 ms is desired. According to [1], a redundant layer-3 handoff cost about 3 second. NetworkManager with FCS can eliminate unnecessary latency of erESS/reSubnet handoff compared to the conventional NetworkManager.

V. CONCLUSION

This study proposes Further Check Scheme (FCS) that not only detects the change of subnet after a raESS handoff, but also eliminates unnecessary latency after an erESS handoff. FCS utilizes ARP requests to distinguish a raSubnet handoff from an erSubnet handoff. The recipient of ARP reply represents a raSubnet handoff while a timeout implies an erSubnet handoff. The experimental results confirm that FCS outperforms the conventional implementation of NetworkManager under Linux in terms of handoff latency.

ACKNOWLEDGMENT

This work was supported in part by National Science Council under Grants NSC 101-2221-E-009 -028 -MY3 and NSC 100-2221-E-009-031-MY3.

REFERENCES

[1] L.-H. Yen, H.-H. Chang, S.-L. Tsao, C.-C. Hung and C.-C. Tseng, "Experimental study of mismatching ESS-subnet handoffs on IP over IEEE 802.11 WLANs," in *2011 Eighth International Conference on Wireless and Optical Communications Networks (WOCN)*, pp. 1-5, 2011.

[2] K. El Malki, Ed., *Low-Latency Handoffs in Mobile IPv4*, 2007: Internet RFC 4881.

[3] S.-M. Yoon, S.-J. Yu, and J.-S. Song, "Cross-layer fast and seamless handoff scheme for 3GPP-WLAN interworking," in *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*, T. Sobh et al., Eds. Netherlands: Springer, 2007, pp. 437–442.

[4] S. Tran-Trong, S. Tursunova, and Y.-T. Kim, "Enhanced vertical handover in Mobile IPv6 with Media Independent Handover services and advance Duplicate Address Detection," in *KNOM Conference*, 2008.

[5] *NetworManager*, [Online]. Available: http://projects.gnome.org/NetworkManager/