Using Shared Beacon Channel for Fast Handoff in IEEE 802.11 Wireless Networks

Jaeouk OK(*), Pedro MORALES(*), Andreas DARMAWAN(**), and Hiroyuki MORIKAWA(*, **)

(*)Graduate School of Frontier Sciences, The University of Tokyo, Japan
(**)Graduate School of Electrical Engineering, The University of Tokyo, Japan
okjaeouk@mlab.t.u-tokyo.ac.jp

Abstract—Handoff process in IEEE 802.11 wireless networks must be accomplished with as little interruption as possible to maintain the required quality of service (QoS). Previous research reported that channel scanning phase accounts for more than 90% of the overall link-layer handoff latency, ranging from 350 to 500 msec. In order to eliminate the time-consuming channel scanning phase we propose a stand-alone, shared beacon channel, where stations (STAs) can update information about neighboring access points (APs) via an extra receiver. Our proposed method contributes to completely eliminate the channel scanning phase, therefore, realizing fast handoff in IEEE 802.11 wireless networks. In this paper, we implement our proposed method on FreeBSD 6.1R kernel with Atheros AR5212-based 802.11 a/b/g chipsets. From experimental results, we find that it takes 6.063 msec delay on average during handoff from 802.11b AP to 802.11a AP while transmitting/receiving 480 byte ICMP frames with an interval of 10 msec.

I. INTRODUCTION

In IEEE 802.11 wireless networks [1], to achieve mobility stations (STAs) must quickly discover access points (APs) and select one which provides the highest level of quality of service (QoS). In real-time applications, it is particularly important to have fast handoff so that its occurrence stays unnoticed by users. Current standard, however, has no mechanism to enable fast handoff, because an AP in infrastructure mode was designed to provide wireless connectivity for fixed, portable, and moving STAs mainly within a Basic Service Set (BSS).

Link-layer handoff is composed of four sequential phases: detection, channel scanning, link-layer authentication, and reassociation. Previous works reported that channel scanning latency accounts for more than 90% of the overall handoff latency, ranging from 350 msec to 500 msec [2]. This amount of delay is unacceptable for highly interactive multimedia applications. Thus, our work focuses on minimizing the channel scanning latency.

The current channel scanning phase in IEEE 802.11 wireless networks is not suitable for fast handoff due to the following two reasons. First, IEEE 802.11 wireless networks operate based on Carrier Sense Media Access/Collision Avoidance (CSMA/CA). Unlike cellular system, STAs can not scan other channels while exchanging data frames with currently associated AP, because it would cause frame loss. To attack this problem, related works have tried to utilize Power Saving Mode (PSM) [3] or multiple network interface cards (NICs) [4]. Though these approaches enable an STA to maintain a list of candidate APs before the connection to prior AP is terminated, the acquired information may become outdated by the time of handoff decision, which would cause improper selection of the following AP if radio condition is rapidly time-varying.

Second, beacon interval is too far apart for fast handoff (100 msec by default). Since an STA lacks knowledge about which channel its nearby APs are operating on, it should redundantly scan every single channel regardless whether any AP exists on that channel. Though shorter beacon interval or active scan enable an STA to locate its nearby BSSs more quickly, these approaches increase overhead to the already limited bandwidth. Previous works also tried to provide an STA with nearby AP information approximated by APs collaboratively [5]. In this approach in order to increase the accuracy of the selection of channels to scan provided by an AP to an STA, higher support is required from the wired network side, which would break the distributed characteristics of IEEE 802.11 wireless networks.

Our goal is to realize fast handoff by enabling STAs to perform channel scanning while exchanging data frames with a currently associated AP like cellular system, yet keeping distributed characteristics of IEEE 802.11 wireless networks. We believe that there should be a dedicated extra channel to advertise AP’s existence, where STAs can update information about geographically nearby APs via an extra receiver. There are three points to be considered towards our goal. Firstly, a practical frequency band management strategy is needed. Though multiple transceivers can be easily implemented in a single card, as PHS (PCS in Japan) widely did, assigning new frequency band is a costly issue in practical perspective. Secondly, the dedicated extra channel should be backward compatible with currently deployed IEEE 802.11 wireless networks. Finally, care must be taken when deciding the frame contents to advertise AP on the dedicated extra channel, and the way to process the advertisement on STA side. With these considerations, STAs without an extra receiver also should be able to reduce channel scanning latency with the dedicated extra channel.

In this paper, we propose a novel fast handoff method that enables channel scanning while exchanging data frames with a currently associated AP by utilizing a shared beacon channel. Our proposed method ideally enables STAs to keep track of nearby APs operating on any PHY types and any channels in a distributed manner. We present the design architecture of
our proposed method and evaluate its performance by handoff experiments across two BSSs operating on different channels and different PHY types while transmitting/receiving 480 byte ICMP frames with the interval of 10 msec.

The rest of this paper is organized as follows. In the next section, we begin with a brief review of link-layer handoff process and channel assignment in Japan. Section III describes our proposed method to use a shared beacon channel. Implementation and experimental results are explained in section IV. Section V concludes the paper.

II. BACKGROUND

In this section, we present a brief review of link-layer handoff process required to reestablish the interrupted link connectivity. We also introduce the channel assignment of IEEE 802.11 wireless networks in Japan.

A. Link-Layer Handoff

Link-layer handoff process consists of four sequential phases: detection, channel scanning, link-layer authentication, and reassociation.

Detection is the phase where the need for handoff is discovered. The detection latency can be completely eliminated by adopting soft detection method, which uses signal strength reported from the physical layer.

Channel scanning is the phase to acquire the information about geographically nearby APs which may be operating on different channels. The standard defines two methods: passive scan and active scan. In passive scan, an STA listens to each channel for beacon frames. In active scan, an STA broadcasts Probe Request frames and waits for Probe Response frames on each channel. Though active scan can make channel scanning phase faster by causing extra traffic, it still takes 350 msec to 500 msec [2].

Link-layer authentication is the phase to verify the identity of each other between an AP and an STA. The standard defined two algorithms: open system and shared key authentication. The latency of each phase sums up to about one and two Round Trip Time (RTTs) respectively.

Reassociation is the phase for an STA to acquire permission to access the wired network over an AP. Because an STA is only allowed to be associated with a single AP at a time, it must disassociate with its prior AP before associating with the new one.

B. Channel Assignment in Japan

IEEE 802.11b/g uses 2.4 GHz Industrial Science Medical (ISM) band that allows any devices to access the frequency without licenses. Figure 1 shows the channel assignment in IEEE 802.11b wireless networks in Japan with the bandwidth of each channel being 22 MHz. The center frequency of channel 1 is 2.412 GHz, and following channels are with interval of 5 MHz except channel 14. Note that channel 14 is 12 MHz away from the adjacent channel 13, instead of 5 MHz. Including channel 14, which is allowed for IEEE 802.11b only in Japan, there are 4 non-overlapping channels, (i.e. 1, 6, 11, and 14). The other standard, IEEE 802.11a uses 5 GHz band, and 4 non-overlapping channels (i.e. 34, 38, 42, and 46) in Japan. The number of available channels depends on each country’s frequency band governing policy. North America uses frequency band from channel 1 to channel 11, and Europe from channel 1 to channel 13 in IEEE 802.11b.

III. SHARED BEACON CHANNEL

In this section, we describe our proposed handoff method to use a shared beacon channel. The requirements for integrating a shared beacon channel into the current standard, i.e. frequency band management strategy, backward compatibility, and handling the required information for AP advertisement on the dedicated extra channel are addressed here.

A. Frequency Band Management Strategy

Regarding frequency assignment for a shared beacon channel in Japan, we take advantage of the fact that allocation of channels for AP usage is distributed, but unbalanced in IEEE 802.11 wireless networks. This imbalance can be seen in the following experiment. Channel 14 is a good example of this imbalance. The usage of channel 14 is relatively very low, because IEEE 802.11g, which is the high rate version compatible with 802.11b, does not employ channel 14. Also, since channel 14 is only allocated in Japan, most of the 802.11b products for international market do not support channel 14. Due to this, we predict that the usage of channel 14 will decrease over time.

We tried collecting beacons on the campus of The University of Tokyo using NetStumbler application [6]. We found 507 APs where 420 APs were operated on 2.4 GHz, and the other 87 APs were on 5 GHz. The sorted result of channel distribution for APs is presented in Figure 2. The x-axis shows the channels available in Japan and the y-axis shows the number of APs that we found on campus. This graph shows well how unbalanced the channels are assigned in real use. According to our observation channel 1, 6, and 11 were used by 100 (19.7%), 97 (19.1%), 126 (24.9%) APs respectively, while channel 14 was virtually unused. This imbalance of channel allocation is originated from the fact that groups who have certain controls in different aspects are working separately. Those groups are government (control over country’s frequency band policy), manufacturers (control over wireless NIC features), and network administrators (control over network management).

Note that channel 14 is almost not used at all even though it is a non-overlapping frequency band like the more commonly
used channels 1, 6, and 11. Despite the fact that channel 14 is only overlapped by less number of adjacent channels (i.e. 12 and 13), which makes it relatively “empty”, only strengthens further the fact that the costly frequency band between 2.473 GHz and 2.495 GHz is wasted in realistic perspective. Therefore, we propose a novel usage of channel 14 as a stand-alone, shared beacon channel, where STAs can receive updated information about nearby APs via an extra receiver. The use of channel 14 can address frequency band issue without having new frequency band assigned in Japan. For international standardization, we believe that the unused spectrum in lower frequency band can be a good option [7].

B. Nearby AP Information Update

We use shared beacon channel, called BeaconChannel, to broadcast each AP’s existence to geographically nearby STAs. In our approach, each AP periodically transmits extended format beacons, called eBeacon, in BeaconChannel via an extra NIC. Even though all APs in range try to use BeaconChannel, CSMA/CA enables access to the shared media controlled in a distributed manner. Beacons on each traditional data channel should remain to guarantee backward compatibility with the existing single channel wireless networks. As long as an STA is equipped with an extra receiver tuned to BeaconChannel, it is able to keep receiving eBeacons periodically.

The handling of the eBeacon works in the following way. Each AP extends a normal beacon explicitly including the channel and PHY type information used for data frame exchange. Since eBeacons from various APs are transmitted in a single extra dedicated channel, the channel number and PHY type information for exchanging data frame with the APs are not readily available to the STA. Each STA has to adjust RSSI based on its PHY types to utilize it as a metric for estimating link quality. Because 5 GHz frequency range has shorter transmission distance compared with that of 2 GHz, RSSI of eBeacon from 11a APs needs to be devaluated when comparing it with that from 11b/g APs. Taking these into account, we address our backward compatibility and eBeacon content selection and processing.

As an added value, the RSSI of eBeacon can be used as a good metric to select the next AP, because an STA can acquire RSSI from each candidate AP right before handoff decision. Also, BeaconChannel provides APs with means to deliver useful information in eBeacon to STAs. APs can transmit eBeacons including, but not limited to, various other metrics besides RSSI to indicate how busy each AP is, as well as Access Router information (AR-Info) needed for network-layer handoff (i.e. router’s MAC address, IP address, and prefix) without negatively affecting data frame exchanges. The specification for Fast Handover for Mobile IPv6 (FMIPv6)[8] assumes that BSSID and handoff metrics are available while associating to Previous Access Router (PAR). Not only can our approach satisfy this assumption, but it also skips the phase to resolve AP identifiers to subnet router information, because (AP-ID, AR-Info) tuple is maintained via eBeacons all the time.

\[ \text{HandoffLatency} = T_{interface\_setup} + T_{authentication} + T_{association} \]  

where \( T_{interface\_setup} \) is the time to set up the NIC following the channel and PHY type of the next AP, \( T_{authentication} \) and \( T_{association} \) are the time to perform authentication and association with the next AP.

STAs which are not equipped with an extra receiver can also improve its channel scanning latency by changing the order of channels to scan, i.e. channel 14 first, during channel scanning phase. Since eBeacon includes the same contents of original beacon, an STA can identify nearby APs which transmit eBeacon in BeaconChannel. In the condition where all APs transmit eBeacons, an STA can reduce the number of channels to scan from 18 (14 for 802.11b and 4 for 802.11a) down to only one, which is BeaconChannel.

Power consumption is an issue not to be overlooked, because an extra receiver would be a big power-drain especially for a battery-operated STA. It has been reported that in receiver mode, a wireless NIC requires as much as 70% of the amount of power required in transmitter mode [9]. Turning on the extra receiver only when it is needed to scan on demand can reduce

![Fig. 2. Channel 14 is one of the non-overlapping channels in Japan, but its usage is relatively very low.](image-url)
the power consumption on STA side. To realize this approach, we need to predict handoff timing correctly with the following simple algorithm. When RSSI from currently associating AP falls below $RSSI_{\text{turnon}}$, it switches on the extra receiver and receives all eBeacons from available APs. Since the value of $RSSI_{\text{turnon}}$ depends on how fast the candidate set of APs available in range can be updated, eBeacon interval must be carefully determined. While the shorter “wake-up” time saves much more energy on STA side, the longer “wake-up” time provides an STA with better metrics of signal quality by monitoring the change of RSSI from each nearby AP.

IV. IMPLEMENTATION & PERFORMANCE EVALUATION

In this section, we explain the implementation of the shared beacon channel and its performance evaluation from experiments in an actual network environment.

A. Implementation

We implemented our proposed method that realizes fast link-layer handoff on FreeBSD 6.1R kernel with Atheros AR5212-based 802.11 a/b/g chipsets. We use IBM Thinkpad X31 (CPU Pentium M 1.7GHz, 1GB RAM) equipped with a mini-PCI NIC and a cardbus NIC as both AP and STA. We built eBeacon transmitter in IEEE 802.11 protocol stack on AP side. An eBeacon receiver on STA side was built into the IEEE 802.11 protocol stack and $i$fath Atheros device driver.

An AP has two NICs, one is called $NIC_{\text{data}}$ for exchanging data frames, and the other is $NIC_{\text{ctrl}}$ for transmitting eBeacon frames in channel 14. We allocate memory space for the eBeacon and write down the content of eBeacon in it within the IEEE 802.11 protocol stack. The same beacon transmitted in the original channel through $NIC_{\text{data}}$ is also added to the eBeacon so that STAs without an extra receiver can reduce scanning latency with BeaconChannel. The additional beacon information is composed of channel, PHY type and BSSID of $NIC_{\text{data}}$, and eBeacon interval. As optional information, we chose the total number of association id for load information and AR-Info for network layer handoff information. The format of eBeacon is depicted in Figure 3. The eBeacon frame is sent through $i$fath device driver periodically.

An STA also has two NICs called $NIC_{\text{data}}$ and $NIC_{\text{ctrl}}$. For our implementation we replaced the extra receiver with a normal NIC on STA side. $NIC_{\text{ctrl}}$ is waiting for eBeacons in channel 14. When an eBeacon frame arrives at $i$fath device driver, function $ath\_rx\_proct$ changes struct ieee80211com interface information from $NIC_{\text{ctrl}}$ into $NIC_{\text{data}}$ so that IEEE 802.11 protocol stack processes the eBeacon frame as if it came from $NIC_{\text{data}}$. In IEEE 802.11 protocol stack, function ieee80211_recv_mgmt$()$ changes channel information from 14 to the one tuned by AP’s $NIC_{\text{data}}$ based on the channel bit in extended information, before updating struct ieee80211_node node information and a look-up table. Look-up table manages the information about available APs in range per-BSSID of AP’s $NIC_{\text{data}}$. It includes MAC addresses of NICs, RSSI, received time stamp, eBeacon interval, PHY type, channel of $NIC_{\text{data}}$, ESSID, the total number of association id, and AR-Info. Look-up table is updated whenever eBeacon arrives at STA.

B. Performance Evaluation

In order to evaluate the performance of our proposed method in an actual network, we set up the following experimental environment. We built two overlapping BSSs, where two APs are located at line-of-sight (LOS) with the distance of 80 meters. An 11b AP ($AP_{\text{prior}}$), was operating on channel 11, and the other 11a AP ($AP_{\text{posterior}}$) on channel 38. Each AP was equipped with an extra 11b NIC ($NIC_{\text{ctrl}}$) on channel 14 for BeaconChannel, on which eBeacon were transmitted every 100 msec. The APs and a target device were connected by 100 Base-T wired lines, and these two APs were working as a bridge between the wireless and wired network in link-layer level under shared key authentication.

We moved the STA at normal walking speed towards $AP_{\text{posterior}}$ while transmitting ICMP Echo Request frames to the target device in the same subnet. We set ICMP frame size 480 bytes, and interval 10 msec, corresponding to a constant bit rate of 384 Kbit/s suitable to support both video and audio. As the STA got closer to $AP_{\text{posterior}}$, the degradation of RSSI, which was measured from the last one second of beacons arriving at $NIC_{\text{data}}$, triggered link-layer handoff to $AP_{\text{posterior}}$ with better signal quality on channel 38.

Figure 4 shows how RTT, playing a critical role in QoS of real-time interactive applications, changes during our handoff experiment. The x-axis shows the ICMP sequence number and the y-axis shows the RTT in millisecond. The RTT, required to transmit/receive 480 bytes of ICMP frames at the 10 msec interval, is measured by means of the ping command in a series of experiments, while the STA moves from $AP_{\text{prior}}$ to $AP_{\text{posterior}}$. From the figure, we find that the average RTT while associating to 11b $AP_{\text{prior}}$ (1.534 msec) is almost twice as long as while associating to 11a $AP_{\text{posterior}}$ (0.704 msec) because of different data rates. We can see that handoff from $AP_{\text{prior}}$ to $AP_{\text{posterior}}$ occurs at 5214th frame, and its RTT in the presence of handoff is kept well below 6.299 msec. We can also see that the RTT of 1488th frame reaches 14.324 msec, which is much larger than that of the handoff. This is thought to be caused by retransmissions of frames due to temporarily
deteriorated wireless link. From this observation, we can state that our proposed method contributes to reduce the negative effect of handoff under shared key authentication smaller than wireless link noise in terms of RTT.

We dumped all frames before and after the link-layer handoff using a tcpdump application on STA side. With an assumption that the interface setup time $T_{\text{interface\_setup}}$ in (1) described in section III-C is small enough compared to RTT, we determine the handoff latency as the interval between the first authentication request frame and association response success frame. The handoff latency from tcpdump analysis is presented in Figure 5. The x-axis shows the experiment number and the y-axis shows the handoff latency in millisecond. We can find that the handoff procedure can be accomplished within 6.063 msec of delay on average under shared key authentication, associated to authentication (5.5386 msec, 91.35%) and reassociation (0.5244 msec, 8.65 %) phases. This link-layer handoff delay is much less than the recommended maximum to prevent excessive jitter, 50 msec, by ITU[10].

V. CONCLUSION

In this paper, we propose a handoff method using a shared beacon channel to enable STAs to perform channel scanning while exchanging data frames with a currently associated AP, yet keeping distributed characteristics of IEEE 802.11 wireless networks. From experimental results, we find that our proposed method contributes to completely eliminate channel scanning phase, reducing link-layer handoff down to 6.063 msec on average under shared key authentication during handoff across BSSs operating on different channels/PHY types. The main contribution of this paper is in identifying the potential of a stand-alone, shared beacon channel to keep track of APs of any types and any channels in range in the IEEE 802.11 wireless networks. It is a trade-off between the requirements of extra bandwidth and hardware for faster handoff performance. We believe that the advantage of a shared beacon channel will be much greater when our approach is applied to handoff process between different subnets with the combination of network layer mobility support protocols such as FMIPv6.

Future work will be focused on evaluating the effect of dedicating channel 14 for BeaconChannel in terms of interference, and exploration of a solution concerning the use of the unused spectrum in the lower frequency band. Further implementation should be done including network-layer handoff using FMIPv6 across different subnets.

VI. ACKNOWLEDGEMENT

This work was supported by Ministry of Internal Affairs and Communications, Japan.

REFERENCES


