Seamless Layer-2 Handoff in IEEE 802.11 using Two Radios

Sangho Shin, Andrea G. Forte, Henning Schulzrinne
Email: {ss2020, andreaf, hgs}@cs.columbia.edu

I. Introduction

A number of algorithms have been proposed to achieve seamless layer-2 handoff. However, none of them eliminated handoff delay completely although some of them improved handoff time significantly, albeit with change to the infrastructure or 802.11 standard. We propose a handoff algorithm which achieves seamless layer-2 handoff using two radios in a mobile node. The scanning time takes more than 90% of the total handoff time [1]. And the break during scanning is totally eliminated by scanning APs using one radio while the other radio continues communication.

II. Selective Passive Scanning

Two scanning methods are defined in the IEEE 802.11 standard [2]: active scanning and passive scanning. In active scanning, mobile nodes broadcast probe request frames on each channel, and Access Points (APs) send back probe response frames to the mobile node. Active scanning takes between 100 ms and 500 ms to scan all the channels in IEEE 802.11b [1]. In passive scanning, mobile nodes listen to beacon frames periodically sent by APs and measure the signal strength. Thus, the scanning time depends on the beacon interval configured on the APs. When the beacon interval is 100 ms, it takes 1.1s in IEEE 802.11b to scan all channels. Active scanning scans APs faster, but it consumes more power than passive scanning. In our approach, we use passive scanning because scanning time is not a problem in handoff using two radios and it consumes less power.

The disadvantage of the passive scanning is the long scanning time. Even if the long scanning time does not affect communication in our approach, it can causes false handoff. False handoff means that the mobile node can miss the best AP and associates with the second best AP. False handoff happens among three APs when they are deployed closely (Fig. 1). P1 is the middle of the AP2 and the AP3, and before P1 the best AP is AP2. At P2, which is the handoff point of the mobile node, the best AP is the AP3. Therefore, false handoff can happen when handoff happens after P1 ($3 \cdot d/2 < r$). For example, the mobile node scans channel 11 right before P1, and the best AP is still AP2. If the mobile node has no time to scan channel 11 again before handoff at P2 happens, it will associate to the second best AP, AP2.

False handoff probability (pf) can be calculated as followings:

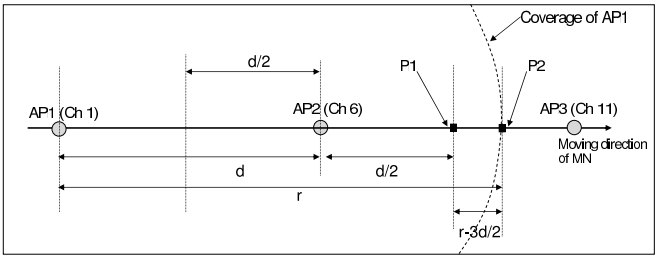

Fig. 1. AP arrangement where false handoff can occur with passive scanning

$$pf = \frac{\text{cases that mobile node cannot scan the best AP during } x}{\text{total cases of a cycle of scanning}} = \frac{n_t - n_x}{n_t} = \frac{n_t - \frac{r-3\cdot d/2}{s\cdot b}}{n_t}$$

$$\text{Here, } t_x = \frac{x}{s} = \frac{r - 3\cdot d/2}{s} \quad (x = r - 3\cdot d/2 \text{ in Fig. 1}) \quad (1)$$

$$n_x = \frac{t_x}{b} = \frac{\frac{r-3\cdot d/2}{s}}{b} = \frac{r - 3\cdot d/2}{s\cdot b} \quad (2)$$

d = distance between APs (m)
r = radio coverage of an AP (m)
x = distance between P1 and P2 (m)
t_x = time to move between P1 and P2 (s)
n_x = number of channels scanned during t_x
n_t = total number of channels to scan
b = beacon interval (s)
s = mobile node speed (uniform and straight movement) (m/s)

For example, when $r = 10$, $d = 6$, $s = 3$, $b = 0.1$ in indoor wireless networks, the false handoff probability is 0.7 with the normal passive scanning. If we put 0 to pf, we can get the scanning time (t_t) to avoid false handoff as following:

$$b \cdot n_t (= t_t) = \frac{r - 3\cdot d/2}{s} \quad (3)$$

In the above example, according to the Eq. 3 the maximum scanning time to avoid false handoff is 0.33 s. This introduces a limit on the maximum number of channels (n_t) that the mobile node can scan in one cycle.

We propose the selective passive scanning to overcome the disadvantage. In the selective passive scanning, mobile nodes scan the non-overlapping channels first [3]. And, mobile

nodes do not need to scan the current hannel because the same channels cannot be assigned to two neighbor APs due to co-channel interference. Mobile nodes need to scan also overlapping channels just in case such channels are used. We allow mobile nodes scan one overlapping channel after it scans all non-overlapping channels to minimize the scanning time. When APs are found in overlapping channels, the channels are added to the active channel list to keep track of such APs. Following such algorithm, we reduce the scanning time to 300 ms in IEEE 802.11b where mobile nodes scan three channels in a cycle of scanning (three non-overlapping channels: 1, 6 and 11, minus the current channel, plus one overlapping channel).

Algorithm 1 Selective Passive Scanning

```
active_channels ← non-overlapping channels
inactive_channels ← overlapping channels
used_inactive_channels ← NULL
loop
  if scanning_channel = the last active channel then
    scanning_channel ← next inactive channel
  else
    scanning_channel ← next active channel
  end if
  if scanning_channel = the current channel then
    scanning_channel ← next active channel
  end if
  Scan scanning_channel
  if scanning_channel is in inactive_channels and AP
  is found then
    Add scanning_channel to active_channels
    Remove scanning_channel from inactive_channels
    Add scanning_channel to used_inactive_channels
  end if
  if scanning_channel is in used_inactive_channels and
  AP is not found then
    Remove scanning_channel from active_channels
    Add scanning_channel to inactive_channels
  end if
end loop
```

III. Implementation and experiments

To emulate two radios, we used two wireless cards, and implemented the selective passive scanning using the hostap wireless card driver [4]. We have confirmed that there is no packet loss or additional delay during layer-2 handoff using our algorithm via experiments.

IV. Consideration of using two radios in IEEE 802.11i environment

When Wi-Fi Protected Access (WPA) or IEEE 802.11i is involved in the layer-2 handoff, the handoff time increases significantly. We have confirmed via experiments that it takes more than 1 s when EAP-TLS [5] is used. We can improve the handoff time dramatically by using two radios in such environments. When the next AP is selected after scanning, one radio (radio1) starts association to the new AP (Fig. 2). Communication is not interrupted by the association because the association is performed on radio1 while another radio (radio2) keeps communicating with the old AP. During the association, various keys are generated and exchanged between the mobile node and the AP and the authentication server. When radio2 finishes the association with the new AP, it starts to transmit data to the new AP while radio1 keeps just listening on the old channel until radio2 starts to receive frames from the new AP. In this way, we can overcome the break usually caused by the bridging delay [3].

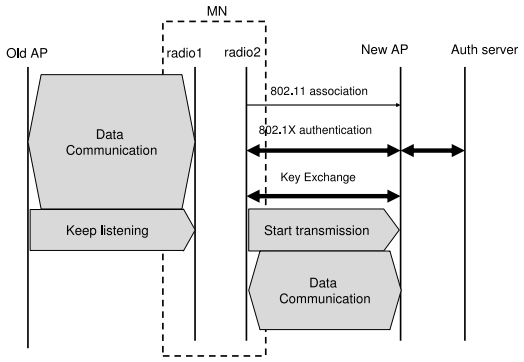

Fig. 2. layer-2 handoff with IEEE 802.11i after selective passive scanning

V. Conclusions

In this paper, we achieve seamless layer-2 handoff using two radios. We also propose a selective passive scanning algorithm to reduce the false handoff probability. Selective passive scanning reduces the scanning time significantly by scanning non-overlapping channels first, and the shorter scanning time reduces the probability of false handoff. When IEEE 802.11i is used for security, the break of communication due to layer-2 handoff is about 1 s, and it is totally eliminated by using two radios. While using two radios achieve seamless handoff, mobile nodes consume more power to maintain the second radio on. We can minimize the power consumption by turning the second radio on only when handoff is required. As further work, we will investigate how much additional power is consumed in our approach by the second radio.

References

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

[2] *Wireless LAN Medium Access Control (MAC) and Physical (PHY) specifications*, IEEE, 1999.

[3] S. Shin, A. G. Forte, A. S. Rawat, and H. Schulzrinne, "Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs," in *MobiWac '04*. New York, NY, USA: ACM Press, 2004, pp. 19–26.

[4] J. Malinen. Host ap driver for intersil prism2/2.5/3. [Online]. Available: http://hostap.epitest.fi/

[5] *RFC2716, PPP EAP TLE Authentication Protocol*, IEEE, 1999.