# A Neighbor Caching Mechanism for Handoff in IEEE 802.11 Wireless Networks

Chung-Sheng Li , Yung-Chih Tseng and Han-Chieh Chao

Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan, R.O.C

Email: majorlee@mail.ndhu.edu.tw, m9223037@em92.ndhu.edu.tw, hcc@niu.edu.tw

## Abstract

Seamless handover in IEEE 802.11 for Quality of Service (QoS) demanding applications is one of the critical issues because of handover latency. In this paper, we proposed the Neighbor Graph Cache (NGC) mechanism to reduce scanning latency while a mobile station tries to make a link-layer handover. The handoff latency can be greatly reduced through NGC algorithm. We use OPNET modeler as the simulation tool. The simulation results show that the handover delay by NGC is 2.614 ms. It is less than 50 ms and able to meet the criteria of VoIP application.

Keyword: Handoff, Neighbor Graph, Neighbor Graph Cache, Probing Latency

## 1. Introduction

Mobility support in conventional IEEE 802.11 is not a prior consideration, since a single access point is often sufficient in a home or small office network. For QoS demanding application, such as VoIP, multimedia, seamless handover in mobility support has become an important issue while a portal device is moving from one AP to another. Our motivation is to study the impact of handoffs for delay sensitive applications. From our evaluation results, they show that conventional handover are not effective to meet the QoS requirements. So we propose Neighbor Graph Cache mechanism to reduce the handover latency for QoS applications.

## 2. 802.11 Handoff Process

Access points (APs) provide wireless connectivity by bridging packets from the wireless domain to an internal network. Due to mobility, a device may move and lose the signal from its AP. In that case, the mobile user should change to a new AP in order to maintain its wireless connectivity. Fig. 1 shows the main elements involved in a layer 2 handoff: the station (STA), the old AP, the new AP, and the distribution system (DS). It can be observed that basic service sets (BSS1 and BSS2) must belong to the same extended service set (ESS1). In the same way, radio channels of each cell (CHX, CHY) shall be none mutually interfering channels. The operation to change an association from one AP to another is known as a handover. Original design of the IEEE 802.11 standard [1] just considered the handoff signaling in the wireless part. The handover procedure can be divided into three phases: discovery, reauthentication and reassociation[2].

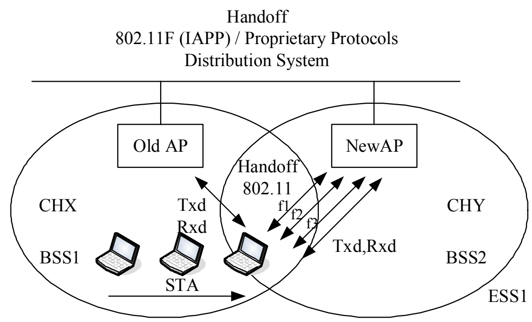


Fig. 1 Involved elements in layer 2 handover

**Phase 1: Discovery**

The discovery process can be ether passive or active. Passive scanning consists of waiting for a beacon message, which is a frame periodically sent by APs as shown in Fig. 2 Passive scanning. Usually, the beacon transmission period is configured at 100 ms, which makes the APs discovery in the scale of a second since there are 11 channels defined in the IEEE 802.11 standard, and the MN must scan channel one by one.

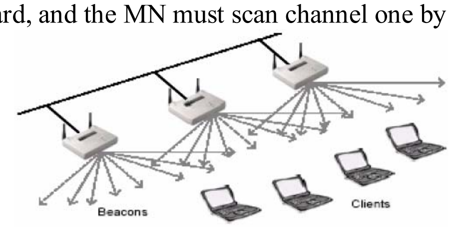


Fig. 2 Passive scanning

Active scanning mode as shown in Fig. 3, in order to determine whether an AP is operating on a particular channel, a MN periodically sends Probe Request messages. When an AP receives a Probe Request, it replies with Probe Response message. By this method, a MN pro-actively discovers the presence of APs. The

2007 International Conference on Multimedia and Ubiquitous Engineering(MUE'07)
0-7695-2777-9/07 $20.00 © 2007 IEEE

duration of the scanning stage strongly depends on the number of channels which a MN has to probe.

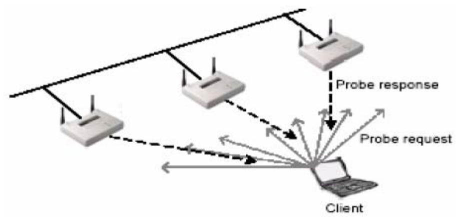


Fig. 3 Active scanning

In active discovery, the number of channels selected for Channel List defines two kinds of scans. The full-scan that sweeps all usable channels and the short-scan that sweeps only a subset of the channel spectrum.

**Phase 2: Reauthentication**

In this phase, the STA authenticates with the best discovered AP in phase 1. Authentication is a necessary prerequisite to association. However, IEEE 802.11 standard neither requires that authentication must immediately proceed to association nor the authentication must immediately follow a channel scan cycle. For this reason, some vendors have implemented preauthentication schemes, e.g., discovery with preauthentication and IAPP based preauthentication. In the first scheme, the STA authenticates with the new AP immediately after the scan cycle finishes, getting anticipate the moment of reassociation. The second scheme is accomplished even with greater anticipation; it is performed as soon as the STA associates with the first AP in the ESS. In that moment, IAPP sends through the distribution system, authentication information to all APs in the ESS, thus, when reassociation is required, the STA is already authenticated with any AP. IAPP based preauthentication is achieved even before STA enters to the discovery state, thus, it does not contribute to handoff latency.

**Phase 3: Reassociation**

Reassociation is the process for transferring associations from one AP to another. Once the STA authenticates with the new AP, the reassociation can be started. According to [3], reassociation process is a six step process.

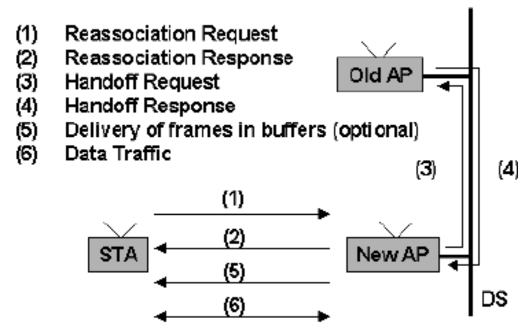


Fig. 4 Steps in the reassociation process

Fig. 5[9] summarizes the handover procedure. The overall delay is the summation of scanning delay, reauthentication delay and reassocation delay. According to [2], the 90% of handoff delay comes from scanning delay. To reduce scanning delay means to improve the handoff efficiency. The range of scanning delay can be represented by (1).

$$N \times T_{min} \leq T_{scan} \leq N \times T_{max} \quad (1)$$

where N is the total number of channels which used in a country, $T_{min}$ is MinChannelTime, $T_{max}$ is MaxChannelTime, $T_{scan}$ is the total measured scanning delay. In this paper, we focus on how to reduce the scanning delay.

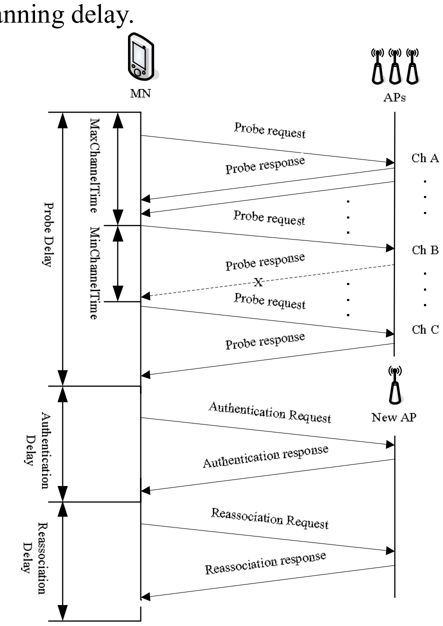


Fig. 5 802.11 handover procedure

## 3. Neighbor Cache Graph


0-7695-2777-9/07 $20.00 

For decreasing the scanning delay, equation (1) shows to have to reduce the values of MinChannelTime, MaxChannelTime, or *N*. MinChannelTime and MaxChannelTime can be optimized as described in [7], but *N* is fixed in each country because the frequency ranges are subject to the geographic-specific regulatory authorities. However, the channels which are occupied by APs are not same in all Basic Service Areas (BSAs) or Extended Service Areas (ESAs). Thus, if we know the used channels in each site in advance, STAs do not need to scan all channels. The NG proposed in [6] uses the topological information on APs. But our algorithm needs to use not only topological information but also cache beacon frames and channels of APs. Thus, we define the data structure of NGC in (2).

$$\begin{aligned} &G' = (V', E), \\ &V' = \{v_i : v_i = (ap_i, \text{beacon frame and channel}), v_i \in V\}, \\ &e = (ap_i, ap_j), \\ &NC(ap_i) = \{ap_{ik} : ap_{ik} \in V', (ap_i, ap_{ik}) \in E\} \end{aligned} \quad (2)$$

Where *G'* is the modified NGC, and *V'* is the set which contains APs with beacon frames.

Because we have already precached beacon frames of neighbor APs, a MN can go to phase 2 directly while performing handoff. It can save time consuming for scanning channels. But if all associations failed, the MN has to enter the phase 1 to scan channels. Equation (1) can be rewritten to equation $\sum_{N'}^{i=l}(T_{min} \times \lambda_i + \delta) \le T_{scan} \le \sum_{N'}^{i=l}(T_{max} \times \lambda_i + \delta)$ (3).

$$\sum_{N'}^{i=l}(T_{min} \times \lambda_i + \delta) \le T_{scan} \le \sum_{N'}^{i=l}(T_{max} \times \lambda_i + \delta) \quad (3)$$

where *N'* is the number of selected channels, $T_{min}$ is MinChannelTime, $T_{max}$ is Max ChannelTime, *n* is the number of cached channels, $\lambda_i$ is association successful number, $\delta$ is association delay and $T_{scan}$ is the total measured scanning delay. If association is successful, $\lambda_i$ is equal to 0. Otherwise, $\lambda_i$ is equal = 1 for full scanning process. Therefore, from the equation $\sum_{N'}^{i=l}(T_{min} \times \lambda_i + \delta) \le T_{scan} \le \sum_{N'}^{i=l}(T_{max} \times \lambda_i + \delta)$ (3) in comparison with equation (1), when all $\lambda_i$=0, it can greatly reduce handoff delay because the scanning delay is unnecessary. The value of $\delta$ is less than 5 ms[4] for each association. If *N'* is less than 7, the handover can be less than 50 ms. It means the handoff delay of NGC is less than the delay criteria for VoIP[5].

According to equation (3) and analysis above, we design a flow chart as shown in Fig. 6. When $\lambda_i$=0, it means that a STA can fetch a candidate AP instead of scanning. If association with this AP succeeded until *i*. is equal to *n*, the total delay of handover equals $n \times \delta$ .

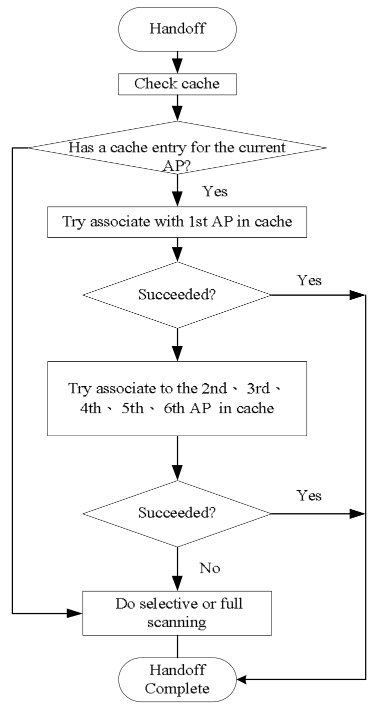


Fig. 6 Neighbor Caching Table Mechanism

## 4. Simulation Result

We used OPNET as a simulation tool to analyze five layer 2 handoff schemes and proposed Neighbor Caching scheme. The results are shown in the following.

A. The Five Methods of L2 Handoff Mechanisms

In this section, five different L2 handoff methods are simulated. They are Passive, Fast passive, Active, Fast active and Neighbor Graph Cache. The purpose of discussing the five introduced method, is to compare the result of different handoff method. Here we will propose different scenarios, and will discuss the results of employing these five handoff methods.

B. Simulation Set Up and Discussion of the Results

2007 International Conference on Multimedia and Ubiquitous Engineering(MUE'07)
0-7695-2777-9/07 $20.00 © 2007 IEEE