WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. (in press)
Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/wcm.273

Efficient IEEE 802.11 handoff based on a novel geographical fingerprint scheme

Tin-Yu Wu*,†, Cheng-Chia Lai and Han-Chieh Chao

Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan, Republic of China 97401

Summary

The effective coverage distance of wireless LAN (WLAN) being small, users may leave the coverage area of the specific access point (AP) from time to time while roaming. However, the wireless network is a shared medium. The air is open for everyone. In general there is collision if a few users attempt to transmit with the same channel that is more rigorous during handoff period because of active scan mode. The active scan will perform requests for searching available AP. Unfortunately, this function consumes too much resource in wireless communication, and also affect total performance. We will propose an advanced active scan to improve it. In our proposal, we convert RF signal distribution to a simple classification problem, like as XOR classifier with artificial neural network (ANN). We combine ANN with active scan to achieve our goal. And the weight, which trained by ANN presents the connection character of geography. Moreover, the weight could be stored in AP for reusing and is called geographical fingerprint. The average enhancement of reducing the active scan area is about 62%. Copyright © 2006 John Wiley & Sons, Ltd.

KEY WORDS: active scan; geographical fingerprint; GPS-less; neural network; handoff

1. Introduction

A wireless LAN (WLAN) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure. Over the last 7 years, wireless local area network solutions (WLANs) have gained strong popularity in a number of vertical markets, including the health-care, retail, manufacturing, warehousing and academic arenas. The applications of wireless communication are very mature. WLANs have been an important trend in our life. The effective coverage distance of WLAN being small, users may leave the coverage area of the specific access point (AP) from time to time while roaming. The connection will be broken. There are two solutions:

1. Increase the power of access point.
2. Increase the number of AP deployment.

But, we can find the problems for those two solutions respectively. In Solution 1, it is impossible to establish a huge AP to cover a city or a country. So it is not a good idea to solve the limitation of radio. In Solution 2, we deploy more stations to increase the coverage of

*Correspondence to: Tin-Yu Wu, Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan, Republic of China 97401.
†E-mail: tyw@mail.ndhu.edu.tw

Contract/grant sponsor: National Science Council of Taiwan; contract/grant number: NSC 91-2219-E-259-004.

RF signal. Because of statistical fluctuations in signal strength due to fading, mobile node (MN) may be repeatedly handed off back and forth between neighboring AP before it is associated with a single station (STA), or is forced to terminate as the signal strength falls below acceptable levels.

It is called Ping-Pong effect. Frequent handoffs affect connection quality and increase the load on the wireless network. Even worse, if a user moves through the boundary of a station, it will perform a handoff mechanism that changes the associated AP from old to new one. If new AP and old one are not within the same IP Domain, MN will obtain the different IP. Therefore, the packets can not be transmitted through the original route. Some services like FTP and Telnet, will then be disconnected.

Several manners can solve the problem caused by above mentioned mobility issues.

1. Mobile IP [1]
2. Mobile IPv6 [2]
3. Cellular IP [3]

The performances of those protocols are not that obvious in dealing handoff issues. Many groups therefore aim to enhance them. For example:

1. Hierarchical mobile IPv6 mobility management (HMIPv6) [4]
2. Fast handovers for mobile IPv6 [5]
3. Registration revocation in mobile IPv4 [6]
4. Mobile IPv6 Fast handovers for 802.11 networks [7]
5. Localized mobility management requirements [8]

In previous phase, most people may be satisfied with their efficiency [9]. But improvement is still needed. It is our goal to achieve a seamless handoff. We take two measures to ameliorate handoff by IEEE 802.11 MAC layer function.

1. Location-aware mobility
2. Analyzable active scan mode

For the first item, some researches take global positioning system (GPS) [10] for locating. The GPS solves the problem of localization in outdoor environments. In this paper, we plan to take GPS-less localization [11] through neural network consideration.

For the second item, handoff latency is dominated by active scan mode [Section 3.1]. The efficiency is better if the frequency of active scan is decreased. We hope to analyze signal strength, which is received by user node. This is the same as above, using neural network technique to assist our proposal architecture.

The above text is Introduction. The remainder of this thesis is organized as follows: Section 2 reviews two related works regarding our proposal. Section 3 presents the details of MAC layer handoff process. Section 4 is the proposed mechanism, and the measurement results are thoroughly presented. Section 5 is the conclusion about this research.

2. Related Works

2.1. RADAR: An In-Building RF-Based User Location and Tracking System [14]

In this paper, RADAR, is a radio-frequency (RF) based system for locating and tracking users inside buildings. RADAR operates by recording and processing signal strength information at multiple base stations positioned to provide overlapping coverage in the area of interest. It combines empirical measurements with signal propagation modeling to determine user location and thereby enable location-aware services and applications.

Their experimental testbed is located on the second floor of a 3-storey building. The floor has dimension of 43.5 m by 22.5 m, an area of 980 sq. m, and includes more than 50 rooms. There are three base stations, BS1, BS2 and BS3 in the layout. They record information about the RF signal as a function of user's location, then use the signal information to construct and validate models for signal propagation during offline analysis.

Next, it uses the empirical data obtained in the off-life phase to construct the search space. The empirical method performs significantly better than both of the other methods. What is different between RADAR and our proposal? RADAR records signal strength information of dots through neural network, then tracks locations of the user based on it. But in our proposal, we just use several handoff points for training neurons. Therefore, it will save the training time and the function will be restricted into the associated AP classifier. Detailed comparisons are shown in Table I.

2.2. An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process [15]

This paper presents an empirical study of handoff process at the link layer, with a detailed breakup of the

Table I. Comparisons between RADAR and proposed method.

	RADAR	Proposed method
Objective	Location aware and tracking user	Looking for the best handoff points and choose the most appropriate associated AP
Computation	Heavy	Relative light
Accuracy	High	Moderate low
AP memory consumption	Large	Relative small
Real-time capability	Low	High

latency into various components. In particular, it shows that a MAC layer function—probe, is the primary contributor to the overall handoff latency; and observe that the latency is significant enough to affect the quality of service for many applications (or network connections).

A handoff occurs when a mobile station moves beyond the RF range of one AP, and enters another BSS (at the MAC layer). During the handoff, management frames are exchanged between the station (STA) and the AP. Also, the APs involved may exchange certain context information (credentials) specific to the station. Consequently, there is latency involved in the handoff process during which the STA is unable to send or receive traffic.

Figure 1 shows the sequence of messages typically observed during a handoff process. The handoff process starts with the first probe request message and ends with a reassociation response message from an AP. The entire handoff latency will be divided into three delays that are detailed below.

1. **Probe delay**. Messages A to E are the probe messages from an active scan. Consequently, we call the latency for this process, probe delay. The actual number of messages during the probe process may vary from 3 to 11.
2. **Authentication delay**. This is the latency incurred during the exchange of the authentication frames (messages E and F). Authentication consists of two or four consecutive frames depending on the authentication method used by the AP.
3. **Reassociation delay**. This is the latency incurred during the exchange of the reassociation frames (messages G and H). Upon successful authentication process, the station sends a reassociation request frame to the AP and receives a reassociation response frame and completes the handoff.

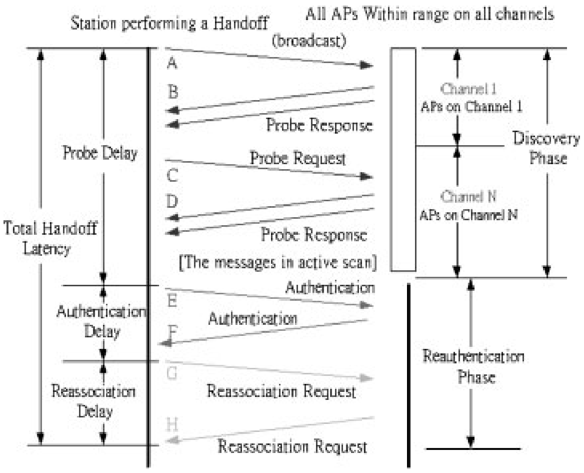

Fig. 1. The IEEE 802.11 handoff procedure.

The wireless hardware used (AP, STA) affects the handoff latency. The variation is from low 30 ms to high 550 ms. We take a combination for example in Figure 2. We find that probe delay is the primary contribution of the handoff latency. Therefore, effectively narrowing down the active scan area can reduce the probe delay.

3. MAC Layer Handoff Process

An 802.11 handoff takes place when an STA changes its association from one AP to another ('re-association') [12,13]. This process consists of the following steps:

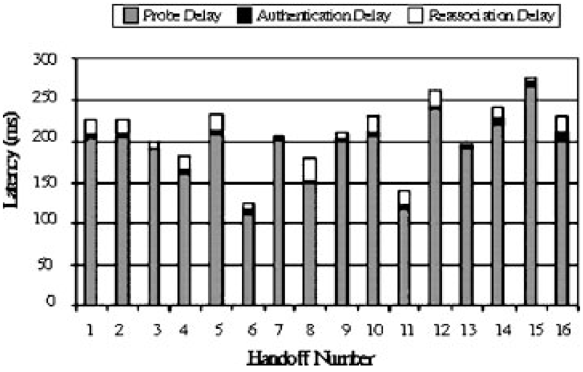

Fig. 2. Handoff latencies—zoomair STA with cisco AP.