WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2006; **6**:127–135
Published online 9 January 2006 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.

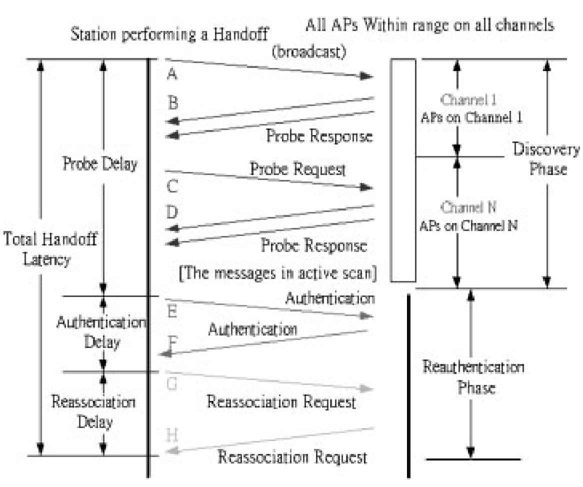

Fig. 1. The IEEE 802.11 handoff procedure.

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.

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:

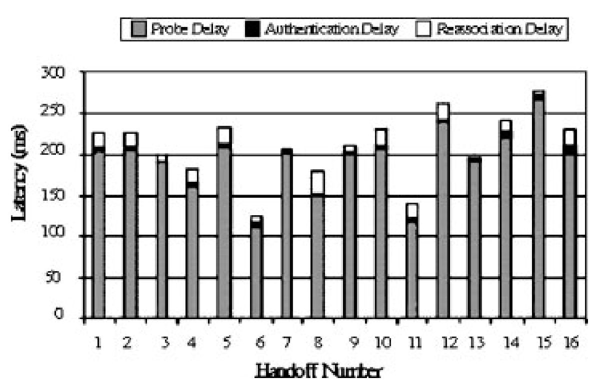

Fig. 2. Handoff latencies—zoomair STA with cisco AP.

1. The STA performs a scan to see what APs are available. The result of the scan is a list of APs together with physical layer information, such as signal strength.
2. The STA chooses one of the APs and performs a join to synchronize its physical and MAC layer timing parameters with the selected AP.
3. The STA requests authentication with the new AP. For an 'Open System', such authentication is a single round-trip message exchange with null authentication.
4. The STA requests association or re-association with the new AP. A re-association request contains the MAC-layer address of the old AP, while a plain association request does not.

Note that in most existing 802.11 implementations, steps 1–4 are performed by firmware that is on-board the 802.11 PCMCIA card. This might make it impossible for the host to take any actions (including sending or receiving IP packets) before the handoff is complete. Also note that there is no guarantee that an AP found during step 1 will be available during step 2 because RF conditions can change dramatically from moment to moment. The STA may then decide to associate with a completely different AP. Usually, this decision is implemented in firmware and the attached host would have no control over which AP is chosen.

There is no standardized trigger for step 1. It may be performed as a result of decaying RF conditions on the current AP or at other times as determined by local implementation decisions. Usually this step will be performed autonomously by firmware in the NIC using proprietary scanning algorithms.

The coverage area of a single AP is known as a basic service set (BSS). Note that both APs in the above description are considered to belong to the same extended service set (ESS). This is to trigger a re-association (rather than plain association) from the STA, which contains information about both the old and new APs. All APs should therefore broadcast the same ESSID. If two APs belong to different administrative domains, this may require some inter-domain coordination of the ESSID. Otherwise, there may not be sufficient information to construct the link-layer triggers required by some handoff mechanisms. A change of BSS within an ESS may or may not require an IP-layer handoff, depending on whether the APs provide STAs access to different or the same IP subnets.

4. Geographical Fingerprint Architecture with Neural Network Consideration

4.1. Triangulation Methodology Based on Artificial Neural Networks

The propagation theory [16] is suitable in free space model. The radio signal strength measurement is used as the mainstream of local positioning technology. But, because of small-scale fading and shadowing effect in physical environment, we can not evaluate the value exactly. Now we provide a better solution using artificial neural networks (ANN). In the beginning we have been trying to make a simple experiment for testing. We adopt the most common multi-layer perceptron (MLP) architecture (Figure 3). We used the back-propagation neural network. It consists of three layers, an input layer with four neurons, a hidden layer with six neurons and an output layer with two neurons. Four inputs are radio signal strength index (RSSI) of each AP. Sigmoid function (Eq. 1) is adopted as the activation function and supervised learning rule is used to train the data.

$$a = \frac{1}{1 + e^{-n}} \tag{1}$$

4.2. Experimental Testbed

In this section, we present the experimental environment and equipments. Subsequently, we will detail our proposed mechanism and show the result. The model number and parameters of the devices are shown in Table II. We could find that the equipments used are the same in the item 1 to 3. The item 4 is the older hardware, but it is still working fine. The parameters of 'distance between APs' are all small.

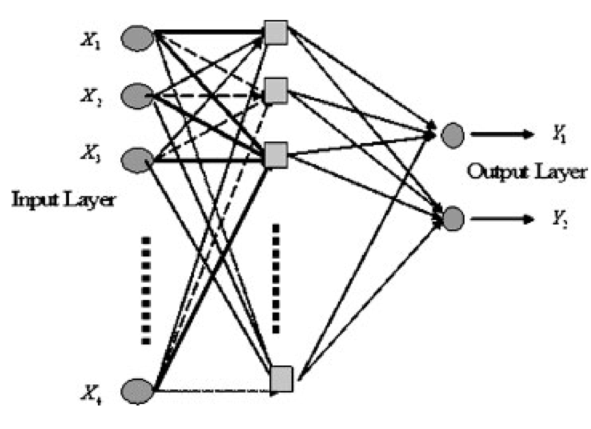

Fig. 3. Multi-layer networks.

Table II. Equipment list.

Name	Equipment
AP-001	AP-3 + PC card gold
AP-002	AP-3 + PC card gold
AP-003	AP-3 + PC card gold
AP-004	AP-1000 + PC card bronze + AIN24-OD-0202 (wavelan ranger extender antenna)
Mobile node	Clevo 1820N + PC card gold

The last one is a notebook running Microsoft Windows XP and installed 'avaya wireless client manager' [17]. We will use this to record all information of RF signal. Furthermore, their specifications are list in Table III.

4.3. Simulation in Physical Environment

First, we will need to collect the signal strength. The floor has dimension of 14.3 m by 13.6 m and is covered by four wireless APs. And the list is signal strength information, we gathered in each node, and there are total 49 nodes. Data acquisition involves measuring manually during a period (about 150–200 seconds), and record information per 2 seconds. As a result, there are about 90 records in each node. And what is more, it takes 50 records randomly for computing an arithmetic mean.

Based on 49 nodes, we could choose 4 nodes respectively, 16, 26, 27 and 44 as handoff points if mobile node moves around like Figure 4. For easy

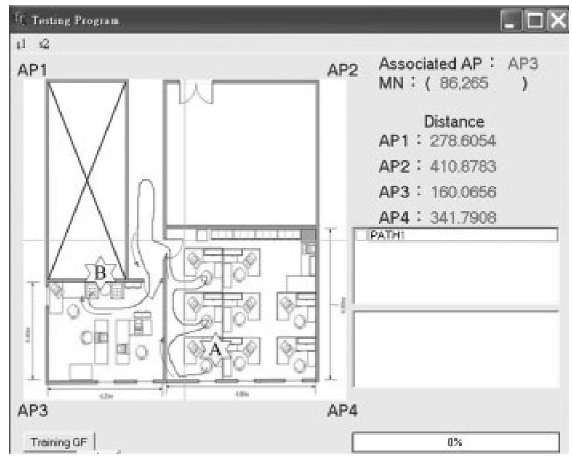

Fig. 4. User movement.

Table III. Specifications list.

Name	Specifications				
Avaya AP-3 (AP-2000)	1. IEEE 802.1x enhanced security 2. Wireless distribution system support 3. Dual PC card slots 4. Web-based SNMP management, embedded telnet/CLI support 5. Power-over-ethernet (PoE) support 6. Wide coverage range 7. WEP and 128 RC4 encryption and MAC address control table and radius authentication				
ORiNOCO AP-1000	1. Dual PC card slot architecture 2. Wireless-to-wireless bridging 8. 10/100 Mb ethernet bridging 9. IEEE 802.11b (Wi-Fi) compliant 10. Spanning tree algorithm 11. IEEE 802.1D transparent bridging 12. Selective protocol filtering 13. Access control table 14. DHCP and BOOTP 15. Multi-channel support 16. Roaming support 17. RC4 based encryption support				
Avaya wireless PC card gold	Frequency band	2.400–2.4835 GHz			
	Modulation technique	Direct sequence spread spectrum (CCK, DQPSK, DBPSK)			
	Spreading	11-chip barker sequence			
	Bit error rate	Better than 10–5			
	Speed options (Mbit/s)	11	5.5	2	1
	Range in open office (m)	160	270	400	550
	Range in semi open office (m)	50	70	90	115
	Range in closed office (m)	25	35	40	50
Lucent wireless PC card bronze	Most are the same as avaya gold, but no WEP and just only 2 Mbit/s maximum				

Table IV. Handoff points from observation nodes list.

Node	AP-001 (dBm)	AP-002 (dBm)	AP-003 (dBm)	AP-004 (dBm)
16 (Initial)	−52.31	−29.04	−64.08	−55.28
26	−50.7	−50.34	−59.3	−58.66
27	−53.88	−62.14	−66.5	−56.52
44	−56.62	−65.62	−59.48	−66.4

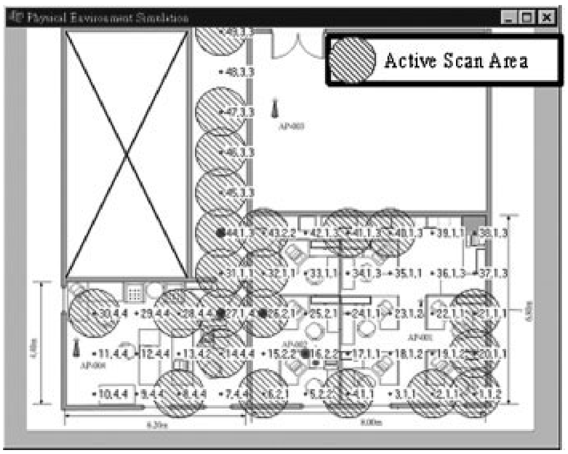

Fig. 5. Blue circle of observation nodes simulation.

reading, we extract them into Table IV. Our implemented methodology measurements are to include one or more AP signal. We used the same way and equipments to measure and examine these signals all the time.

We import the RSSI of four APs as input data to our proposed model for training neurons. And output will indicate associated AP. Subsequently, we will explain step by step the results of experiment. In Figure 5, it would be marked by blue circle if signal strength of node were lower than defined threshold. By the way, it is also called active scan area, because mobile node will perform an active scan for searching available AP. Therefore, it is our goal to decrease this area and the probability of active scan will be reduced.

Let's continue to talk about the red part in Figure 6. It is represented that associated AP taken by signal strongest is different from associated AP determined through ANN. And it also implies that there is handoff issue in these nodes.

The intersection of the red area and the blue area is coincident with the above two conditions. And this simulation result fits our goal. We found original active scan area is decreased from 22 down to 7

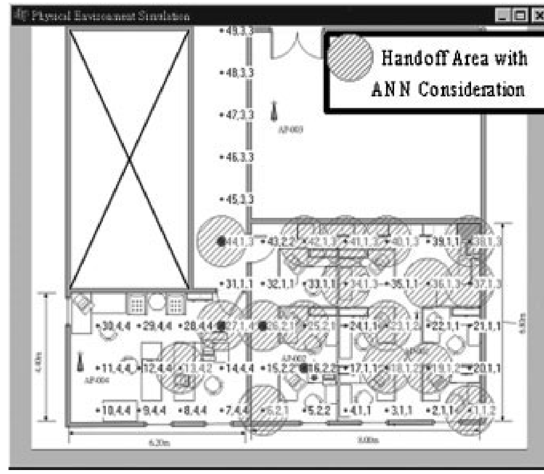

Fig. 6. Red circle of observation nodes simulation.

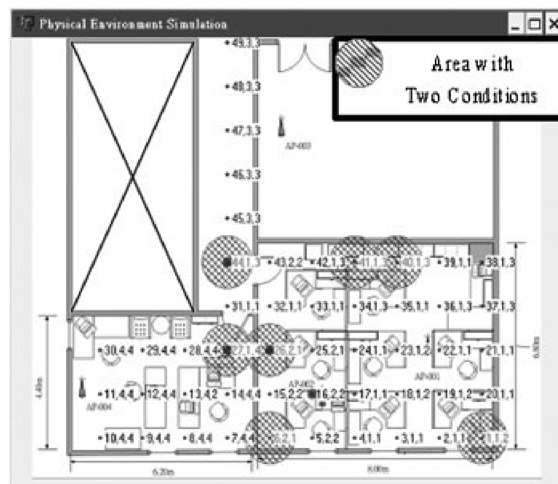

Fig. 7. The intersection area of red and blue.

(Figure 7), total enhancement is about 68%. These statements also could verify the advantages of our proposal. It is possible to reduce Active Scan Area. By surveying simulation procedure in this section, four Handoff Points extracted from test pattern were appointed as input. However, it isn't appropriate for physical environment. Therefore, we take another manner of sampling Handoff Points in the next section. It will be more suitable for physical and by the way, we will talk about reusability of neurons weight.

4.4. Simulation with Another Assumption in Physical Environment

In the previous section, we took simple static data to verify our proposal with two phases. One was for data

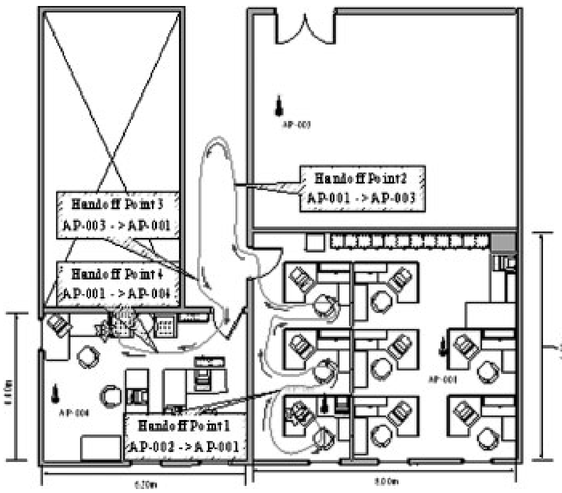

Fig. 8. Handoff points analysis for new sample.

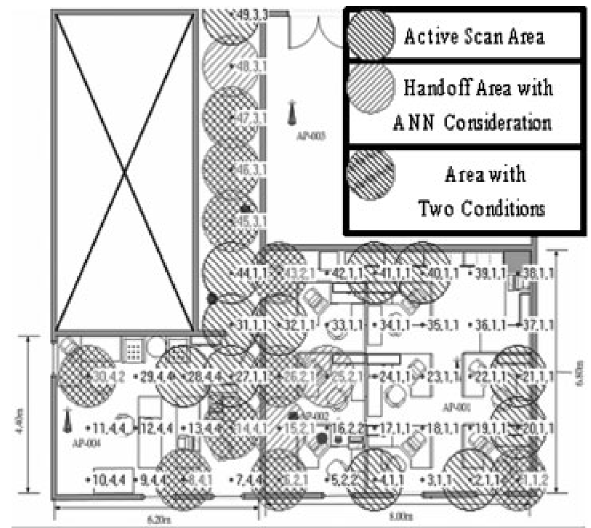

Fig. 9. The result with another assumption in physical environment.

mining and another for analysis. But in this stage, handoff points would be taken by another way, not the same as previous section. What is new? We move again around the path like Figure 4 with the same equipment and gather signal strength through 'Avaya Wireless Client Manager'. All data are listed in detail in Table III. Our target is to verify whether this architecture will fit arbitrary environment.

How to define handoff points during movement? We just need to observe a change for associated AP. If its associated AP is changed, we will log the position as shown in Figure 8. After handoff point analysis, the same as above, we import new signal strength of handoff point to neural network model for training the weight. The simulation will train all new weight. Therefore, we can take this proposal into arbitrary environment.

Subsequently, the result as seen in Figure 9, active scan area is reduced from 22 down to 10, about 55% improvement. Although we take the different data for training, yet the effect are similar.

Finally, following all the above mentioned, we found that acquisition of handoff point could be through movement path. And it has considered to be saved in AP. While mobile node is associated with new AP, a user could download information for assistant of determining associated AP. Furthermore, the information, which is stored in AP is not only handoff point but also weight. The computation will be decreased if we take weight as storage. In conclusion, we could call them geographical fingerprint because they are corresponding to connection state in physical environment.

5. Conclusion

Reading through Section 3, we know that handoff latency will be improved by reducing active scan area. Wireless LANs are a shared medium, meaning that bandwidth is shared among users. Therefore total throughput will be increased if we reduce the probability of executing active scan.

We take a novel approach to solve that. We try to convert active scan to passive analysis of associated AP. The proposed scheme is using neural network model to record RF signal strength distribution. It is worked for determining associated AP in Sections 4.3 and 4.4. The areas that perform active scan are decreased. So there are 68% and 55% enhancement respectively, through simulation results. In brief, we transfer available AP scanning to a classifier, like as XOR problem.

The signal strength which is dominated in this proposal architecture is Mac Layer function. Thus, if Mobile Node could receive Signal from any AP with different ESSID, we don't care forwarding between different domains, like as IP Layer. But unfortunately, the software we have used doesn't support this, so that it is necessary to configure ESSID as the same. Following this issue, the stability of AP is important because our proposal strongly depends on Signal Strength. That means if the position of AP is changed all the time or the power is varied, they will affect our outcome seriously. Such a situation, the neurons must be

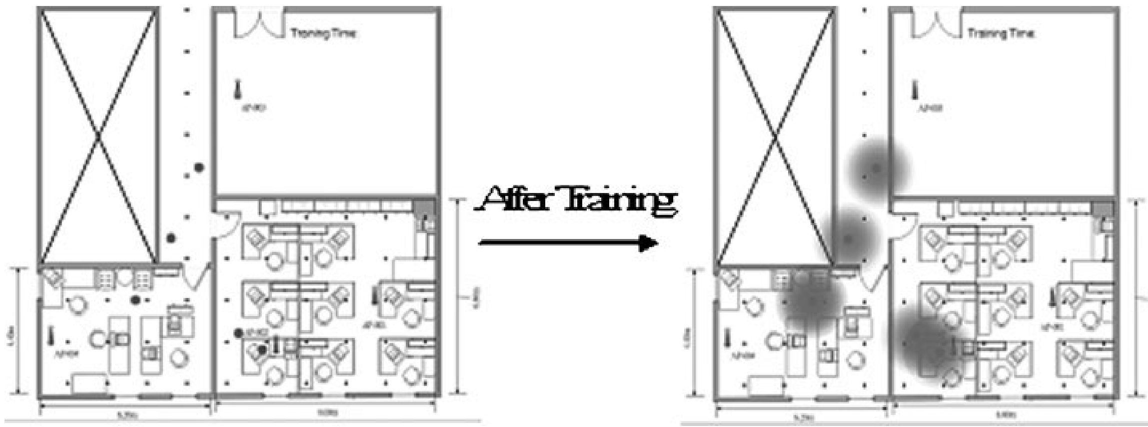

Fig. 10. The ink concept.

retrained to follow with variation of AP, and there is penalty time for retraining. We average the training time in different platforms. AMD XP 2400+ and Celeron 433 got about 330 ms and 2.002 seconds respectively. According to research in Section 4.3, the wireless hardware used (AP, STA) affects the probe delay. The variation is from low 30 ms to high 550 ms.

Finally, we have introduced the concept about geographical fingerprint. In our proposal, we just used several Handoff Points for training neurons. Take Figure 10 as an example, you visualize the floor plan like a white paper and handoff points are like ink drops. Subsequently, we drip four handoff points on this paper. The ink will be dispersed. It becomes several blocks naturally across all nodes. Our goal for classifying associated AP is achieved.

Acknowledgment

Authors thank Hong-Jie Wang and Chang-Chun Cheng for their comments on the neural network model. This work is partially supported by National Science Council of Taiwan, under grant number NSC 91-2219-E-259-004.

References

1. Perkins C (ed.). RFC3220. ‘IP mobility support for IPv4’, January, 2002.
2. Johnson DB, Perkins C, Arkko J. ‘Mobility Support in IPv6’, draft-ietf-mobileip-ipv6-21.txt, February 26, 2003.
3. Campbell A, Gomez J, Wan CY, Kim S, Turanyi Z, Valko A. ‘Cellular IP’, < draft-ietf-mobileip-cellularip-00.txt >, December, 1999.
4. Hesham S. Ericsson, Claude Castelluccia, INRIA Karim El-Malki, Ericsson Ludovic Bellier, INRIA, ‘Hierarchical Mobile IPv6 mobility management (HMIPv6)’, < draft-ietf-mobileip-hmipv6-07.txt >, October, 2002.
5. Koodli R. Nokia Research Center, ‘Fast Handovers for Mobile IPv6’, < draft-ietf-mobileip-fast-mipv6-06.txt >, 1 March 2003.
6. Glass S, Microsystems Sun, Chandra M, Cisco Systems, ‘Registration revocation in mobile IPv4’, < draft-ietf-mobileip-reg-revok-05.txt >, February 2003.
7. McCann P. Lucent Technologies, ‘Mobile IPv6 fast handovers for 802.11 networks’, < raft-mccann-mobileip-80211fh-01.txt >, October 2002.
8. Williams C (ed.). MCSR Labs, ‘Localized Mobility Management Requirements’, March 2, 2003.
9. Teerapabkajorndet W. Proposed to Prashant Krishnamurthy Department of Information Sciences and Telecommunications University of Pittsburgh. ‘*Handoff Algorithms based on Neural Nets in Cellular Digital PacketData Network*’.
10. Hofmann-Wellenhof B, Lichtenegger H, Collins J. *Global Positioning System: Theory and Practice* (4th edn). Springer Verlag: New York, 1997.
11. Bulusu N, Heidemann J, Estrin D. GPS-less low-cost outdoor localization for very small devices. *IEEE Personal Communications* [see also IEEE Wireless Communications] 2000; **7**(5): 28–34.
12. IEEE standard 802.11, Wireless LAN Medium Access Control and Physical Layer Specifications: IEEE, Inc, 1999.
13. http://people.morrisville.edu/~drewwe/wireless/How_it_Works. htm.
14. Bahl P, Padmanabhan VN. ‘RADAR: an in-building RF-based user location and tracking system’, Microsoft Research.
15. Mitra A, Shin M, Arbaugh W. CS-TR-4395, University of Maryland, Department of Computer Science, ‘An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process’, September, 2002.
16. Rappaport TS. *Wireless Communications Principles and Practice*. Communications Engineering and Emerging Technologies Series (2nd edn). Prentice Hall: UK, 1996.
17. http://www.avaya.com

Authors' Biographies

Tin-Yu Wu is currently serving as the chief of Operation Division in the University Computer and IT Center at National Dong Hwa University (NDHU), Hualien, Taiwan. He received his M.S. degree in Electrical Engineering from National Dong Hwa University, Hualien, Taiwan, in 2000. His research interests focus on the next generation internet protocol, mobile computing and wireless networks. He is now a Ph.D. student in Department of Electrical Engineering, NDHU.

Cheng-Chia Lai is a software engineer of Compal Communications, Inc. His research interests are in embedded system, wireless networks and IPv6 based networks. He received his M.S. degree in Electrical Engineering from National Dong Hwa University, Taiwan, in 2003.

Han-Chieh Chao is a full professor and chair of the Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan. His research interests include high speed networks, wireless networks and IPv6 based networks. He received his M.S. degree and Ph.D. in Electrical Engineering from Purdue University in 1989 and 1993 respectively. He has authored or co-authored three books and has published about 100 refereed professional research papers. He has completed 28 MSEE thesis students. He has received many research awards, including Purdue University SRC awards, and NSC research awards (National Science Council of Taiwan). He also received many funded research grants from NSC, Ministry of Education (MOE), Industrial Technology of Research Institute, Institute of Information Industry and FarEasTone Telecommunications Lab. He has been invited frequently to give talks at national and international conferences and research organizations. He is also serving as an IPv6 Steering Committee member and co-chair of R&D division of the NICI (National Information and Communication Initiative, a ministry level government agency which aims to integrate domestic IT and telecom projects of Taiwan), co-chair of the technical area for IPv6 Forum Taiwan, the executive editor of the *Journal of Internet Technology* and the editor-in-chief for *International Journal of Internet Protocol Technology* and *International Journal of Ad Hoc and Ubiquitous Computing*. He is an IEEE senior member.