24

Increasing the Time Connected to Already Deployed 802.11 Wireless Networks while Traveling by Subway

Jaeouk Ok, Pedro Morales, Masateru Minami and Hiroyuki Morikawa
The University of Tokyo
Japan

1. Introduction

Recently, an increasing number of people retrieve various contents via the Internet using a publish/subscribe service such as podcasts. Typical usage of those applications is to subscribe to as many favorite sites as possible, and selectively enjoy the automatically downloaded latest episodes. Newly available portable multimedia players enable people to easily enjoy downloaded video/audio contents in a variety of places, and the added communication functionality such as 3G or 802.11 (IEEE Standard 802.11, 1999) makes it possible to retrieve the latest episodes as soon as they are published on the web.

Service like podcasts are especially beneficial to people traveling by subway[1] considering their idle time in a subway train. However, most of subway tunnels in Tokyo are unfortunately covered by neither 3G nor 802.11 as of December 2008. Wireless connection can be established when a subway train stays under coverage areas at a station[2], but it will be repeatedly interrupted each time the subway train passes through non-coverage areas in the tunnels while traveling along a railroad. This interruption limits the time under coverage areas, which reduces the maximum possible connected time. This time is further reduced by current implementation exploiting the intermittent connectivity poorly. In this chapter, we focus on the 802.11 wireless connection management while traveling by subway because of its higher throughput, lower subscription cost, and larger variety of 802.11-enabled portable devices than 3G.

We aim to increase the time connected to already deployed 802.11 wireless networks for podcast-like applications while traveling by subway in Tokyo. To understand the target environment, we investigated the commercial 802.11 HOTSPOT networks (NTT Communications HOTSPOT, [Online]) deployed in Tokyo Metro. One of the findings

[1]Tokyo Metro carries average 6.22 million passengers per day as of 2007 (Tokyo Metro, [Online])

[2]In Tokyo, for example, approximately 97% of subway stations are densely covered by three different service providers as of December 2008 (NTT Communications HOTSPOT; NTT DoCoMo Mzone; NTT EAST FLET'S SPOT, [Online])

against the common belief regarding long distance mobility is that the main factor to the diminishment of available connected time is link layer connection management, not IP layer mobility support because of the deployed VLANs across the target networks. We propose an optimized solution for this subway environment to increase the connected time by reducing the following two types of delay. The one delay is experienced when establishing the wireless connection after coming out of non-coverage area in the tunnel, and the other when switching the wireless connection to the next AP while crossing overlapping coverage areas at stations.

Our method reduces the establishment delay by building a chain that links the last AP in the previous station before the tunnel with the first AP in the next station after the tunnel, called *border APs* in this chapter. By referring to this chain when leaving a station, a client can reduce the delay to establish the connection through the use of passive scan only on the channel corresponding to the upcoming border AP. The switching delay is reduced by building a list of the APs available at each station for which a client has connection authorization, called *preferred APs* in this chapter. By referring to this list when crossing overlapping coverage areas in a station, a client can reduce the delay to switch the connection through the use of unicast scan using *Authentication Request* frames to the limited number of preferred APs. This is feasible by taking advantage of the key attributes of the target environment: strong mobility pattern along a railroad and limited number of APs at each station. In our analysis, the delay obtained by our method is 94.4% smaller than the one obtained by passive scan when establishing terminated wireless connections, and 94.2% smaller than the one obtained by active scan when switching wireless connection to the next AP.

The rest of this chapter is organized as follows. Section 2 describes the findings from investigating the commercial 802.11 HOTSPOT networks deployed in Tokyo Metro. We propose a method to increase the connected time to already deployed 802.11 wireless networks while traveling by subway in Tokyo in Section 3. Section 4 analyzes the increased connected time by our proposed method in comparison with related work. Section 5 presents the effectiveness of our system through implementation and experiments. Section 6 concludes the chapter, and shows future work.

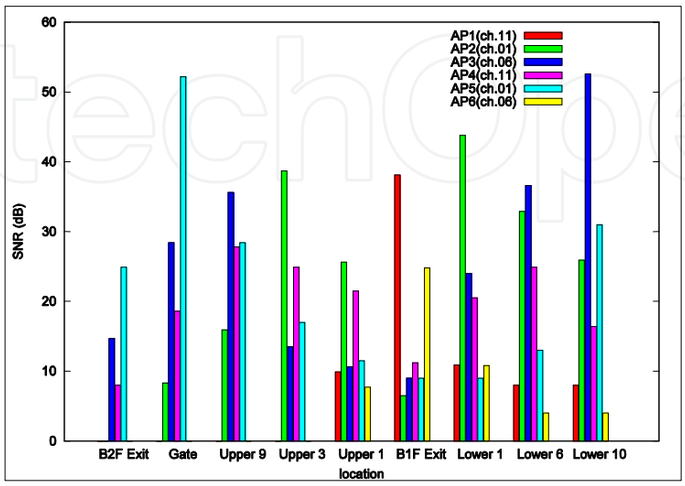


Fig. 1. Averaged SNR values of beacon frames measured at different locations in Waseda (T4) station. The names of location refer to Fig. 2.

2. Target Environment Investigation

In order to find out the factors that decrease the possible connected time, we investigate the commercial 802.11 HOTSPOT network in Tokyo Metro. All experiments were performed with a windows XP machine while walking at stations and moving by subway in November 2008. NetStumbler (NetStumbler, [Online]), Wireshark (Wireshark, [Online]), and built-in Wireless Auto Configuration were used to monitor beacon frames, analyze IP packets and manage 802.11 wireless network connections. The findings are classified by the points of our interest: link layer handoff, IP mobility support, and restrictions on application layer. This section discusses each of them in detail.

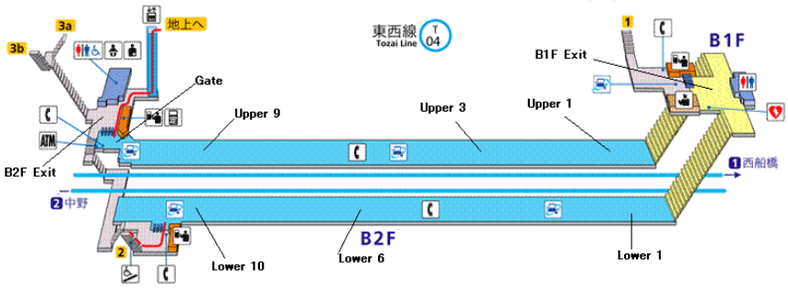


Fig. 2. Waseda (T4) station structure (Tokyo Metro, [Online]) There are six 802.11g APs installed on channel 1, 6 and 11 to collaboratively cover the station including entrances, ticket gates, platforms, etc.

2.1 Link Layer Handoff

To find the necessity of link layer handoff in 802.11 HOTSPOT[3], we studied coverage areas at stations by measuring the averaged SNR values of beacon frames at different locations in 10 stations[4]. In each station, multiple APs ranging from four to seven are installed to collaboratively cover entrances, ticket gates, platforms, passages for transfer, etc. Figure 1 shows an example of the measured results in Waseda (T4) station on Tozai line, whose structure is as shown in Figure 2. From the figure we observe that: 1) the coverage area of a single AP is not large enough to cover the entire station, and 2) each location is under coverage areas of multiple APs. Therefore, while a client moves around at stations, it is necessary to switch the wireless connection across overlapping wireless coverage areas. For example, let us assume that a subway train comes in from right in Figure 2. The clients in the train get associated to AP2 according to Figure 1. For some clients staying in the train, the established wireless connection will be switched from AP2 to AP3, when the train moves to the left for the next station. For others getting off the subway train at Lower 1 on the platform and walk out B1F Exit, the wireless connection will be switched from AP2 to AP1.
Unlike stations with overlapping coverage areas, there are non-coverage areas in each tunnel between stations. To show non-coverage areas in tunnels, we measured the time

[3]In Tokyo Metro, NTT Communications HOTSPOT provides 173 subway stations among 179 with IEEE 802.11 b/g wireless access service. (Tokyo Metro, [Online])

[4] Yoyogi-uehara (C1), Yoyogi-koen (C2), Meiji-jingumae (C3), Omote-sando (C4), Takatanobaba (T3), Waseda (T4), Kagurazaka (T5), Kasumigaseki (M15), Ginza (M16), Tokyo (M17), and Otemachi (M18) station

stamps of received beacon frames while moving by subway through seven stations from Nihombashi (T10) to Waseda (T4) station on Tozai line. The measured results are shown in Table 1. From the table we observe that: 1) there exist non-coverage areas in each tunnel, and 2) the time length under non-coverage areas is approximately one third of the total moving time on a railroad. This is explained by different speeds of subway when passing above two areas: high speed within large non-coverage areas in the tunnels and low speed within small coverage areas in the stations. Though there is large period of time spent under coverage of 802.11 wireless networks even while traveling by subway, the wireless connection is repeatedly interrupted due to non-coverage areas in the tunnel. Therefore, it is necessary to establish disconnected wireless connection whenever the client enters the following coverage areas.

Station	Coverage Area	Non-coverage Area
Nihombashi (T10)	83 sec	20 sec
Otemachi (T9)	66 sec	56 sec
Takebashi (T8)	69 sec	36 sec
Kudanshita (T7)	70 sec	29 sec
Iidabashi (T6)	81 sec	53 sec
Kagurazaka (T5)	81 sec	55 sec

Table 1. Non-coverage areas in the tunnels

2.2 IP Mobility Support

To find the necessity of IP mobility support, we studied IP network configuration by dumping and analyzing IP packets. After a successful association using the proper ESSID (i.e., 0033) and WEP key, a global IP address is assigned via Dynamic Host Configuration Protocol (DHCP) (Droms, 1997). The DHCP server has multiple ranges of address pool. It is possible to have various addresses assigned with the same client and AP at different times. To show the range of DHCP address pool, we collected the obtained TCP/IP address configuration with a single AP at different times in Yoyogi-uehara (C1) station on Chiyoda line. Part of the collected information is shown in Table 2.

Host address	Subnet Mask	Default Gateway
210.162.9.65	255.255.254.0	210.162.9.1
211.0.159.54	255.255.254.0	211.0.159.1
61.127.100.37	255.255.254.0	61.127.100.1

Table 2. The range of DHCP address pool

Once an IP address is assigned in the beginning of a session, the same address is repeatedly assigned not only from different APs in the same station, but also from the APs in other stations by another DHCP request during the DHCP lease length. We confirmed this fact by starting a session at Yoyogi-uehara (C1) station, and receiving the same IP address from two different APs in the same station and also receiving it in other stations such as Yoyogi-koen (C2), Meiji-jingumae (C3), Omote-sando (C4), etc.

From above two experiments, we observe that HOTSPOT implements Virtual Local Area Network (VLAN) (IEEE Standard 802.1Q-2003, 2003) to accommodate multiple subnets in

each physical LAN, and therefore, IP layer mobility support is unnecessary. The initially assigned IP address does not need to be changed, as long as it performs DHCP lease renewal every lease length (i.e., 5 minutes). In order to prevent DHCP renewal from failing in the non-coverage areas in the tunnels, it is necessary to perform DHCP renewal with a shorter interval: (lease length) - (the maximum time spent in the non-coverage areas). As shown in Table 1, the time spent in non-coverage areas in the tunnels are much shorter than the lease length, therefore, we can perform the DHCP discovery only once in the beginning of the session, and skip it later on by renewing DHCP with the above shorter interval.

2.3 Restrictions on Application Layer

NTT Communications HOTSPOT implements web-based authentication to complement the open system authentication. Despite a successful TCP/IP address configuration via DHCP, a client is unable to send and receive data traffic outside the network. To gain Internet access outside the network, users are required to enter a username and password in an authentication web page, to which the first attempt to access any web page after launching a web browser is automatically redirected. We also found that the web authentication expires when there is no traffic sent or received during DHCP lease length (i.e., 5 minutes). Again, as the time spent in non-coverage areas in the tunnels are much shorter than the lease length, it needs to be done only once in the beginning of the session in our subway mobility scenario. Moreover, a download manager such as DownThemAll (DownThemAll, [Online]) is necessary to automatically *resume* broken downloads due to the intermittent connectivity.

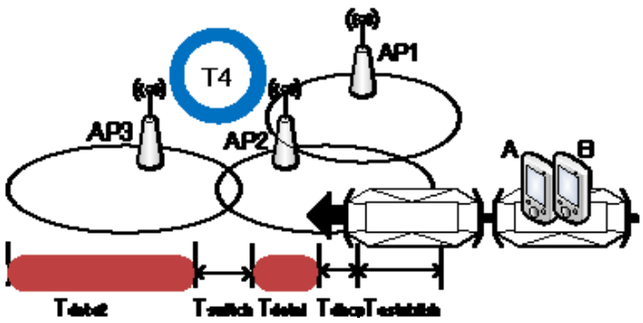


Fig. 3. Mobility scenario

3. Increasing Time Connected while Traveling by Subway

In this section, we describe our proposed method to increase the time connected to 802.11 wireless networks while traveling by subway. We look into the detailed composition of the main factor to the diminishment of available connected time, and propose a method to address them.

3.1 Problem Statement

To clarify the problems arising from utilizing 802.11 wireless connection while traveling by subway, consider the following scenario depicted in Figure 3. Assume that two clients (A and B) took a subway train in the previous T5 station downloading subscribed podcasts with 802.11-enabled portable devices. The wireless connection is terminated while passing through

the non-coverage area in the tunnel. When the train is entering T4 station, the devices discover that they become under coverage area, scan available APs, and get connected to AP2. When the train stops at T4 station, client A gets off and walk to the coverage area of AP1, but client B stays in the train and moves to the next station passing through the coverage area of AP3.
Given that we do not modify the commercially deployed APs to enlarge coverage areas, the maximum connected time of devices passing through T4 station (e.g., client B) is limited shown in Figure 3, and only some parts T_{data} of it is used to download subscribed podcasts. This limited time is also used to recognize the coverage area of the firstly appearing AP and establish link layer connection to it ($T_{establish}$), to check the availability of a previously used IP address via DHCP Request message (T_{dhcp}), and switch link layer connection to a closer AP (T_{switch}). Since DHCP request can be skipped by DHCP renew with shorter interval as shown in the previous section, the main factor to the diminishment of available connected time is composed of $T_{establish}$ and T_{switch} for the link layer connection management.

Fig. 4. An example of a chain of border APs and a list of preferred APs in T3, T4 and T5 stations

3.2 Proposed Method

In order to reduce the delay experienced when managing link layer connection, we take advantage of the following key attributes of the target environment: 1) strong mobility pattern along a railroad, and 2) limited number of APs at each station.

3.2.1 Fast Connection Establishment after Coming out of Non-coverage Areas

In order to reduce the delay experienced when establishing link layer connection ($T_{establish}$), a client needs to discover that it came out of non-coverage areas in the tunnel, and find the AP to associate to with less scanning delay. Because the standard does not define the behavior when no AP is found during scanning process, periodical active scanning is commonly implemented for a general purpose. For example, Wireless Auto Configuration in Windows XP, executes active scanning every 60 seconds (Microsoft Technet, [Online]) when no preferred AP is found during channel scanning phase. However, this periodic scanning makes $T_{establish}$ up to in the magnitude of tens of seconds in subway mobility scenario due to this coverage area recognition delay. Therefore, it is necessary to perform channel scanning continuously, when no AP is found in the tunnel.
We reduce $T_{establish}$ by continuously performing selective passive scan, which does not generate excessive management traffic under non-coverage area in the tunnel. Taking advantage of a strong mobility pattern along a railroad, we build a chain that links the last AP in the previous station before the tunnel with the first AP in the next station after the

tunnel, called border APs. By referring to this chain when leaving a station, a client can reduce $T_{establish}$ through the use of passive scan only on the channel corresponding to the upcoming border AP. For example, back in Figure 1, AP2 in T4 station is the border AP appearing at the end of non-coverage area in the tunnel from T5 station. A part of a chain of border APs regarding T3 (1 border AP), T4 (2 border APs), and T5 (2 border APs) stations is shown in Figure 4. The border APs are related by arrows with the information of BSSID, channel number, and PHY type.

The connection establishment process is performed in the following steps. When a client can not find any APs after being disconnected from a border AP (e.g., 00:0F:90:FC:4E:10 AP in T5 station), it assumes that it is passing through non-coverage area in the tunnel and looks up its chain of border APs to find next border AP (e.g., 00:0F:90:FF:6E:10 AP in T4 station). Then, it sets up its interface to the desired channel and PHY type (e.g., channel 1 and 11b/g), and waits for a beacon from the next border AP. If a beacon from the border AP arrives within the maximum time spent in the non-coverage area, a client executes authentication and association phase. Otherwise, standard active scan is excuted to handle this unexpected case where the pre-built chain of border APs can not reflect the real situation due to changes in infrastructure or unexpected non-coverage area, etc.

The delay of selective passive scan is as follows. Under the best case scenario the beacon arrives as soon as the device enters the coverage area, so the delay is 0. The worst case happens when the device just missed beacon when it enters the coverage area, so the delay is the same as beacon interval, 100 msec by default. Therefore, the highest $T_{establish}$ will be composed of one beacon interval for the selective passive scan, one RTT for authentication, and one RTT for association phase.

3.2.2 Fast Connection Switching across Overlapping Coverage Areas

In order to reduce the delay experienced when switching link layer connection T_{switch} across overlapping coverage areas, a client needs to find the next AP to handoff with less scanning delay. Because a client has flexible mobility patterns in a station, referring to a chain of border APs can not tell clients staying in the train to go to next station from ones getting off to go to other direction, leading to executing active scan. Active scan takes long, because it tries to acquire the information about all nearby APs regardless of a client's connection authorization. Therefore, it is necessary to perform channel scanning only to the target APs that the client has connection authorization.

We reduce T_{switch} by performing multiple open system authentication only to target APs at each station, called AuthScan (Ok et al., 2008). Taking advantage of limited number of APs at each station, we build a list of the APs available at each station for which a client has connection authorization, called preferred APs. By referring to this list when crossing overlapping coverage areas in a station, a client can reduce T_{switch} through the use of unicast scan using *Authentication Request* frames to the limited number of preferred APs. For example, back in Figure 1, there are only six APs of which a client has connection authorization in Waseda (T4) station. A part of a possible preferred AP list regarding T3 (7 APs), T4 (6 APs), and T5 (6 APs) stations is shown in Figure 4. The information is composed of BSSID, channel number, and PHY type. In addition, other common beacon information such as capability information, SSID, supported rates, PHY parameter sets, and WPA parameters needs to be saved for the successful handoff completion.

The connection switching process is performed in the following steps. When detecting the need for switching the current link based on its policy (e.g. signal strength, transmission rate, missed beacon number, retransmission number, etc), a client looks up its preferred AP list and selects one except its currently associated AP in the same station as a target AP. Then, it sets up its interface to the desired channel and PHY type, transmits an *Authentication Request* frame to the target AP, and waits for an *Authentication Response* during *MinChannelTime*, a time parameter involved in active scan long enough to guarantee the reception of a *Probe Response* frame. This process is repeated for all the remaining APs in the list. After the next AP is selected by comparing the Received Signal Strength Indications (RSSIs) measured when receiving *Authentication Response* frames from each AP, a client executes authentication and association phase. The algorithmic flow of our system including selective passive scan and AuthScan is shown in Figure 5.

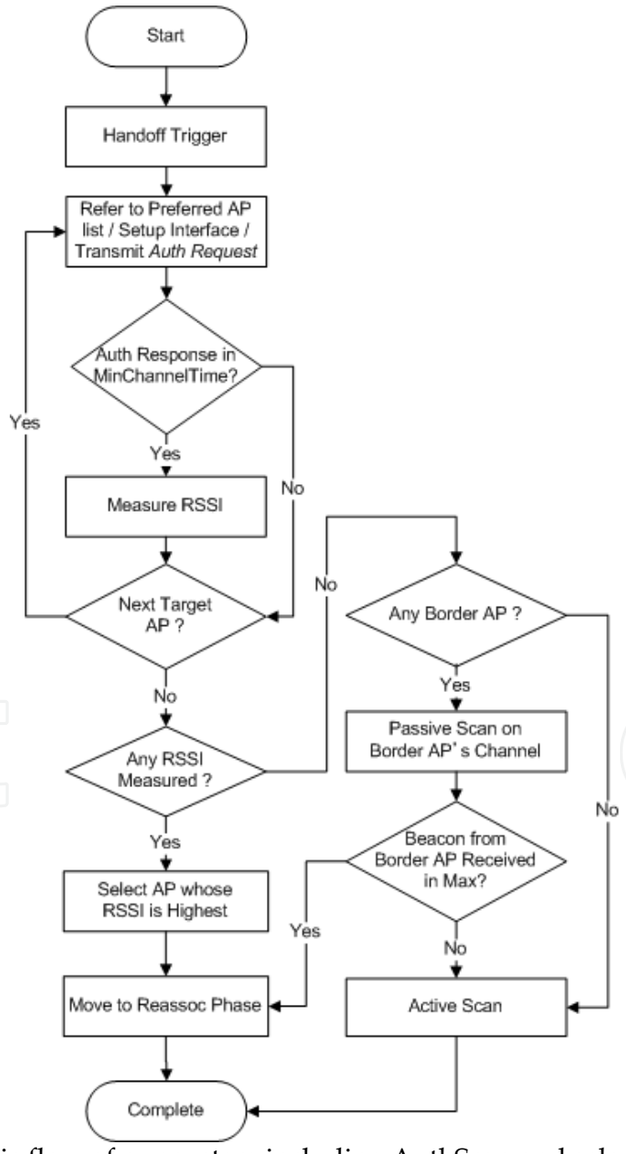


Fig. 5. The algorithmic flow of our system including AuthScan and selective passive scan

The delay of AuthScan is as follows. Assuming at least one of the target APs is available and can fulfill the handoff policy, it takes M * RTT + (N - M) * *MinChannelTime*, where N is the number of target APs that exclude the associated AP before handoff in the preferred AP list at each station, and M is the number of *Authentication Response* frames received. The total connection switching delay T_{switch} will be composed of M * RTT + (N - M) * *MinChannelTime* due to the scanning process, one RTT for authentication, and one RTT for association phase. This achieves channel scanning with lowest delay among the approaches to work under subway's intermittent connectivity without modifying deployed APs as shown in the next section.

4. Increased Connected Time Comparison

In this section, we introduce the related work and analyze the increased connected time by our proposed method in a subway mobility scenario.

4.1 Limitations of Related Work

Many approaches have been proposed to address the channel scanning issues, and can be classified into two groups as below. The first group tries to eliminate the necessity for the channel scanning phase. Some approaches decouple the time-consuming channel scan from the actual handoff phase and scan earlier for maintaining a list of candidate APs with their handoff metrics before the connection to the current AP is terminated (Ramani & Savage, 2005; Wu et al., 2007). Other approaches enable scanning while communicating with the currently associated AP utilizing multiple NICs (Brik et al, 2005; Ok et al, 2007). Though the total handoff delay of these approaches in the first group is shorter than that of our proposed method, none of the above related work can be applied in our subway environment. (Ramani & Savage, 2005; Wu et al., 2007; Brik et al, 2005) can not generate a list of candidate APs with their handoff metrics before the connection to the current AP is terminated under subway's intermittent connectivity. (Ramani & Savage, 2005; Ok et al, 2007) require modification to APs, and (Brik et al, 2005; Ok et al, 2007) require extra hardware on a client.

The second group tries to improve the efficiency of the channel scanning phase. The first way to do this is to reduce the number of channels that are effectively going to be scanned by the client. This can be achieved through various methods such as a cache (Shin et al., 2004), Neighbor Graph (NG) (Mishra et al., 2004), sensor overlay network (Waharte et al., 2004), etc. Another way to improve the efficiency is by reducing the time waiting at each channel. In order to do this, a client is provided with an AP list, and only scans target APs in a unicast fashion to reduce the time to wait at each channel (Ok et al., 2008; Kim et al., 2004; Jeong et al., 2003; Huang et al., 2006). The performance of these approaches depend on the number of channels to scan or deployed APs, but this is not an issue in our target environment, where there are limited number of APs available. Among these, AuthScan achieves the lowest handoff delay, one RTT less than selective unicast scan (Kim et al., 2004) without modifying standard.

4.2 Performance Comparison

To show the increased connected time by our method, we estimate the interrupted time under coverage areas ($T_{establish}$ and T_{switch}) by various methods. Firstly, we compare $T_{establish}$ of passive scan and selective passive scan, which do not generate excessive management traffic under

non-coverage area in the tunnel. Assuming that a client starts to scan at the benining of coverage area, total delay to establish wireless connection of each method is as follows.

- Passive Scan: 18[5] * *Beacon Interval* + 2 * RTT
- Selective Passive Scan: 1 * *Beacon Interval* + 2 * RTT

For example, in the case of T4 station where a single border AP exists on channel 1, as depicted in Figure 3, $T_{establish}$ of above two methods are compared in Table 3, where RTT is 0.6 msec, beacon interval is 100 msec.

Method	$T_{establish}$
Passive Scan	18 * 100 + 2 * 0.6 = 1801.2 msec
Selective Passive Scan	1 * 100 + 2 * 0.6 = 101.2 msec

Table 3. Connection establishment delay

Secondly, we compare T_{switch} of active scan, selective active scan, selective unicast scan, and AuthScan, which expedite scanning process by generating extra management traffic across overlapping coverage area at station. Assuming that there are M target APs on N channels and all of them response to requests, total delay to switch wireless connection of each methods are as follows, where *MaxChannelTime* is a time parameter involved in active scan long enough to guarantee the reception of the *Probe Response* frames from multiple APs available in the same channel.

- Active Scan: *MaxChannelTime* * N + *MinChannelTime* * (18 - N) + 2 * RTT
- Selective Active Scan: N * *MaxChannelTime* + 2 * RTT
- Selective Unicast Scan: M * RTT + 0 * *MinChannelTime* + 2 * RTT
- AuthScan: M * RTT + 0 * *MinChannelTime* + 1 * RTT

For example, in the case of T4 station where five target APs exist on three channels as depicted in Figure 3, T_{switch} of above four methods are compared in Table 4, where RTT is 0.6 msec, beacon interval is 100 msec, *MaxChannelTime* is 15 msec, and *MinChannelTime* is 1024 μ sec (Jeong et al., 2003).

Method	T_{switch}
Active Scan	3*15+15*1.024+2*0.6=61.56 msec
Selective Active Scan	3 * 15 + 2 * 0.6 = 46.2 msec
Selective Unicast Scan	5 * 0.6 + 2 * 0.6 = 4.2 msec
AuthScan	5 * 0.6 + 1 * 0.6 = 3.6 msec

Table 4. Connection switching delay

[5]Additional 4 channels (52, 56, 60, and 64ch) in 5.3GHz (W53) and 11 channels (100, 104, 108, 112, 116, 120, 124, 128, 132, 136, and 140ch) in 5.6GHz (56W) were added to the conventional 4 channels in 5.2 GHz (52W) for 11a in 2005 and 2007, respectively. Therefore, the total number of channels to scan sums up 33 channels. However, we focus on the conventional 18 channels, which most of devices in Japan support, in this chapter.

From the two tables, we can observe that the combination of selective passive scan and AuthScan achieves the lowest interrupted connection time. The delay obtained by selective passive scan is 94.4% smaller than the one obtained by standard passive scan when establishing terminated wireless connections. The delay obtained by AuthScan is 94.2% smaller than the one obtained by active scan when switching wireless connection to the next AP. The increased connected time will become larger in proportion to the number of wireless connection establishment and switching while traving by subway. Besides the aforementioned parameters, there are hardware induced delays such as interface setup time. These delays are not considered in the previous analysis, because they vary from maker to maker and, therefore, are unsettled. In fact, the real delay observed in experiments is even larger than the values obtained in the analysis.

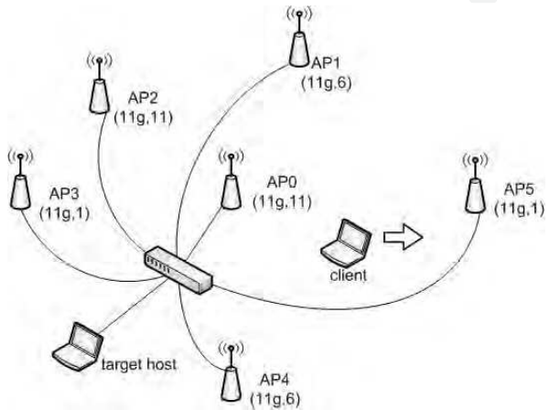


Fig. 6. Experimental setup

5. Implementation and Experiments

We have implemented a prototype of our proposed method on an IBM Thinkpad X31 (CPU Pentium M 1.7GHz, 1GB RAM) with an Atheros AR5212-based wireless interface. It runs Debian Linux 4.0 Etch with a 2.6.18-5 kernel, modified madwifi (MadWifi, [Online]) as the wireless interface driver, and modified wpa_supplicant (Linux WPA/WPA2/IEEE 802.1X Supplicant, [Online]) as the application software. We also implemented an active scan enabled client[6] to scan all 18 channels in an active manner for a comparison purpose. Since the delay of selective passive scan in $T_{establish}$ is probabilistically determined between 0 and 100 msec as shown in Section 3, our experiments focus on the delay to switch wireless connection T_{switch} of our prototype.

In order to evaluate the performance of our prototype in an actual network, we set up the following experimental environment. We build six overlapping BSSs in an office[7]: AP0(11g, ch.11), AP1(11g, ch.6), AP2(11g, ch.11), AP3(11g, ch.1), AP4(11g, ch.6), and AP5(11g, ch.1), as described in Figure 6. The APs and a target host (IBM Thinkpad X31) are connected by 100

[6]Because of regulatory reasons, wpa_supplicant is implemented to passively scan channel 12, 13, 14, 34, 38, 42 and 46.

[7]There are 19 802.11 a/b/g APs on seven channels sharing the same medium with our experimental APs.

Base-T cable, and all APs are working as a bridge between the wireless and wired network in link layer level under open system authentication.
We evaluate our prototype's performance by measuring 1) its average delay to switch wireless connection on the application level, and 2) RTTs during handoff in comparison with active scan in the following experiment scenario. A client with an IEEE 802.11 a/b/g NIC is associated to AP0. The client moves towards AP5 while using *ping* command to transmit ICMP Echo Request frames to the target host in the same subnet. We set the ICMP frame size as 480 bytes, and the interval between frames as 10 msec. Then, we reduce the transmission power of AP0, while increasing that of AP5 to emulate a mobility scenario in a limited space. As the client gets closer to AP5, the degradation of signal strength from AP0 triggers handoff to AP5. Figure 7 shows the average delay to switch wireless connection from ten runs of the handoff scenario since the sending of the *Authentication Request* frame to the first AP scanned (2AQ in the graph). The x-axis shows the steps in the authentication scanning process. They correspond to the sending of the *Authentication Request* frame (AQ), reception of the *Authentication Response* frame (AS), sending of the *Reassociation Request* frame (RQ) and reception of the *Reassociation Response* frame (RS). The number before each of them is the actual AP name being checked. The y-axis is the time delay in milliseconds measured in the application in order to get the handoff delay from the user's perspective. We added a checkpoint right before calling the driver *ioctl*, in the case of the AQ and RQ, and right after receiving the driver's informational event for the AS and RS.

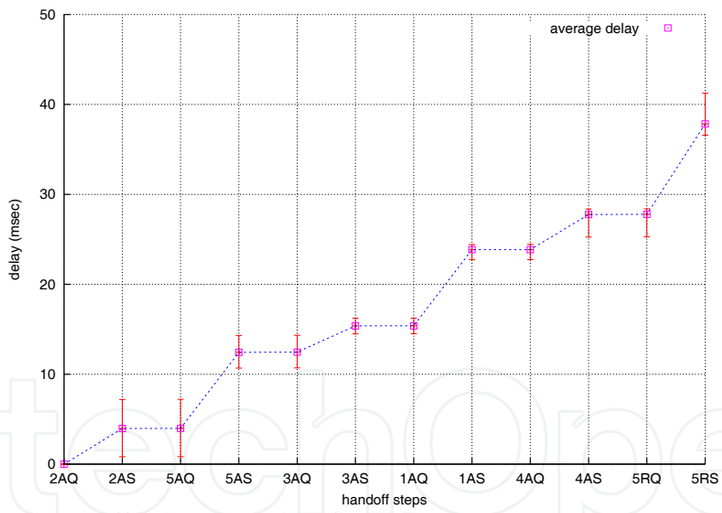


Fig. 7. The average handoff delay checking five APs

The total handoff delay in the application level obtained when checking five APs with open system authentication is 37.84 msec in average. This includes hardware induced delay such as interface setup time, delay introduced by system calls and events that flow between userland and kernel space, and 1 RTT for *Authentication Request* and *Authentication Response*. It takes 3.60 msec in average to check APs on the same channel (from AP 0 to AP2, from AP5 to AP3, from AP1 to AP4), while it takes 8.46 msec in average to check APs on the different channel(from AP 2 to AP5, from AP3 to AP1). Therefore, the AuthScan client saves 4.86 msec to setup the interface into the desired channel, each time checking APs on the same channel consecutively in our experiment.

Figure 8 shows one example of the way RTT changes during handoff from AP0 to AP5. The upper graph corresponds to one run by an AuthScan client, and the lower by an active scan client. The x-axis shows the ICMP sequence number and the y-axis shows the RTT in milliseconds. Handoff takes place between the 682nd and 686th frames (A) in the case of the AuthScan client (i.e., 3 frames dropped, 30 msec disrupted), and between the 3637th and 3924th frames (B) for the active scan client (i.e., 286 frames dropped, 2860 msec disrupted). Therefore, the AuthScan client drops approximately 98.95% fewer frames than the active scan client in the experiment.

6. Conclusion

In order to increase the time connected to already deployed 802.11 wireless networks while traveling by subway in Tokyo, we have developed a system equipped with two scanning modes: 1) passively scanning on a selected channel, and 2) scanning with multiple open authentication. Through analysis and experiments, we have shown that our method increases the time connected to 802.11 wireless networks by establishing wireless connection when coming out of non-coverage area in the tunnel and switching its wireless connection across overlapping coverage area at station with less delay.

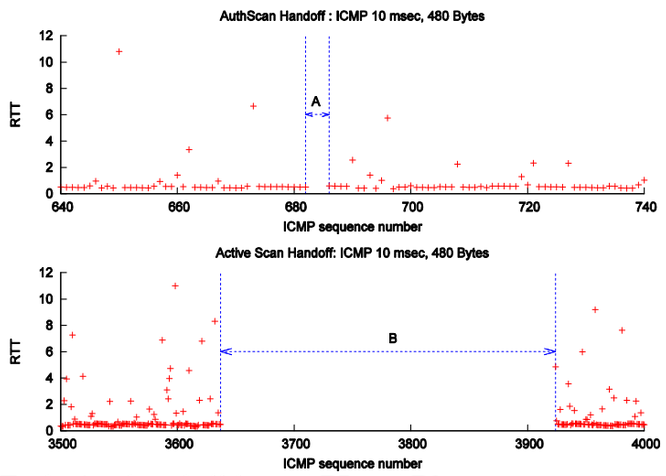


Fig. 8. Profile of RTTs during handoff from AP5 to AP0

The main contribution of this chapter is two-fold:

- We investigated the commercial 802.11 HOTSPOT wireless networks deployed in Tokyo Metro, and clarified the main factor to the diminishment of available connected time.
- We proposed an optimized solution for the subway's intermittent connectivity environment, and analyzed the increase connected time by our method. In addition, we showed the effectiveness of our system through experiments in comparison with standard active scan.

Our proposed method will work under similar subway 802.11 wireless network environments in any other cities. Our future efforts will be oriented to build a more sophisticated chain of border APs, and list of preferred APs. A chain of border APs including interrupted time under non-coverage area in the tunnels can save power by sleeping the interface before performing selective passive scan. A list of preferred APs built per AP at each station can save unicast scanning time even further.

7. References

Brik, V.; Mishra, A. & Banerjee, S. (2005). Eliminating handoff latencies in 802.11 WLANs using multiple radios: Applications, experience, and evaluation, *Proceedings of ACM/USENIX IMC 2005*, Berkeley, CA, October 2005

DownThemAll. [Online].
Available: http ://www.downthemall.net/

Droms, R. (1997). Dynamic Host Configuration Protocol, RFC 2131, Internet Society

Huang, P.; Tseng, Y. & Tsai, K. (2006). A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks, *Proceedings of IEEE VTC 2006-Spring*, Melbourne, Australia, May 2006

IEEE Standard 802.11. (1999). IEEE. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

IEEE Standard 802.1Q-2003. (2003) IEEE Standards for Local and Metropolitan Area Networks, Virtual Bridged Local AreaNetworks

Jeong, M.; Watanabe, F. & Kawahara T. (2003). Fast active scan for measurement and handoff, Technical report, DoCoMo USA Labs, Contribution to IEEE 802, May 2003

Kim, H.; Park, S.; Park, C.; Kim, J. & Ko, S. (2004). Selective Channel Scanning for Fast Handoff in Wireless LAN using Neighbor Graph, *Proceedings of* ITC-CSCC 2004, Sendai, JAPAN, July 2004

Linux WPA/WPA2/IEEE 802.1X Supplicant. [Online].
Available: http://hostap.epitest.fi/

MadWifi - a Linux kernel device driver for Wireless LAN chipsets from Atheros. [Online].
Available: http://madwifi.org/

Microsoft Technet. [Online].
Available: http ://technet.microsoft.com/en-us/library/cc757419.aspx

Mishra, A; Shin, M. & Arbaugh, W. (2003). An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process, *ACM SIGCOMM Computer Communication Review*, Vol. 3, April 2003, pp. 93-102

Mishra, A.; Shin, M. & Arbaugh, W. (2004). Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network, *Proceedings of IEEE INFOCOM 2004*, Hong Kong, March 2004

NTT Communications HOTSPOT. [Online].
Available: http://www.hotspot.ne.jp/

NTT DoCoMo Mzone. [Online].
Available: http://www.nttdocomo.co.jp/service/data/mzone/

NTT EAST FLET'S SPOT. [Online].
Available: http://flets.com/spot/

NetStumbler. [Online].
Available: http://www.netstumbler.com/

Ok, J.; Morales, P.; Darmawan, A. & Morikawa, H. (2007). Using Shared Beacon Channel for Fast Handoff in IEEE 802.11 Wireless Networks, *Proceedings of IEEE VTC2007-Spring*, Dublin, Ireland, April 2007

Ok, J.; Morales, P. & Morikawa, H. (2008). AuthScan: Enabling Fast Handoff across Already Deployed IEEE 802.11 Wireless Networks Mobility, *Proceedings of IEEE PIMRC 2008*, Cannes, France, September 2008

Ramani, I. & Savage, S. (2005). SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks, *Proceedings of IEEE INFOCOM 2005,* Miami, FL, March 2005

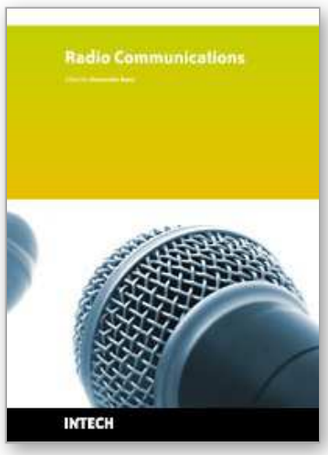
Shin, S.; Forte, A. G.; Rawat, A. S. & Schulzrinne, H. (2004). Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs, *Proceedings of MobWiac 2004*, Philadelphia, PA, September 2004

Tokyo Metro. [Online].
Available: http://www.tokyometro.jp/global/en/about/outline.html

Waharte, S.; Ritzenthaler, K. & Boutaba, R. (2004). Selective Active Scanning for Fast Handoff in WLAN using Sensor Networks, *Proceedings of* MWCN 2004, Paris, France, October 2004

Wireshark. [Online].
Available: http://www.wireshark.org/

Wu, H.; Tan K.; Zhang, Y. & Zhang, Q. (2007). Proactive Scan: Fast Handoff with Smart Triggers for 802.11 Wireless LAN, *Proceedings of IEEE INFOCOM 2007*, Anchorage, Alaska, May 2007



Radio Communications

Edited by Alessandro Bazzi

ISBN 978-953-307-091-9
Hard cover, 712 pages
Publisher InTech
Published online 01, April, 2010
Published in print edition April, 2010

In the last decades the restless evolution of information and communication technologies (ICT) brought to a deep transformation of our habits. The growth of the Internet and the advances in hardware and software implementations modified our way to communicate and to share information. In this book, an overview of the major issues faced today by researchers in the field of radio communications is given through 35 high quality chapters written by specialists working in universities and research centers all over the world. Various aspects will be deeply discussed: channel modeling, beamforming, multiple antennas, cooperative networks, opportunistic scheduling, advanced admission control, handover management, systems performance assessment, routing issues in mobility conditions, localization, web security. Advanced techniques for the radio resource management will be discussed both in single and multiple radio technologies; either in infrastructure, mesh or ad hoc networks.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Jaeouk Ok, Pedro Morales, Masateru Minami and Hiroyuki Morikawa (2010). Increasing the Time Connected to Already Deployed 802.11 Wireless Networks while Traveling by Subway, Radio Communications, Alessandro Bazzi (Ed.), ISBN: 978-953-307-091-9, InTech, Available from: http://www.intechopen.com/books/radio-communications/increasing-the-time-connected-to-already-deployed-802-11-wireless-networks-while-traveling-by-subway

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen