Reachability and Goodput Enhancement via Fragmentation in Public IEEE 802.11b WLAN

Seongkwan Kim†, Jongseok Kim†, Se-kyu Park†, Sunghyun Choi†, Jaehwan Lee§, and Hanwook Jung§§
†School of Electrical Engineering and INMC, Seoul National University
‡Cambridge Silicon Radio (CSR) Korea
§Department of Computer Science, University of Maryland
§§Convergence Project Team, Korea Telecom

{skim,jkim}@mwnl.snu.ac.kr, kevin.park@csr.com, schoi@snu.ac.kr, jhlee@cs.umd.edu, hamuk@kt.co.kr

Abstract

In wireless packet networks, such as IEEE 802.11 Wireless LAN, users can suffer from bad channel quality at cell boundaries, and wireless stations may not overcome the bad communication condition, in spite of using the lowest transmission rate via link adaptation. Unless handoff is considered due to the deployment of APs, the case of initial access to a WLAN network, and so on in such an area, fragmentation can be a unique and compatible solution for coping with the channel limitation. We have evaluated a public WLAN service network, called NESPOT, which is operated by Korea Telecom, especially the case of initial access. We evaluate delay and error performances of NESPOT initial access procedure via both mathematical analysis and simulations. From the results, we conclude that WLAN users can experience enhanced goodput, enlarged reachability, and shortened delay via fragmentation. We also propose a practical method, TCP Maximum Segment Size spoofing to get the same effect as fragmentation. Finally, we propose a policy, called Cut-off delay, for WLAN users not to wait too long time to get an IP address without severe performance degradation.

1. Introduction

During last few years, IEEE 802.11 WLAN (WLAN) has become one of the most prevailing solutions for broadband wireless access network [3]. Now, WLAN is widely used in hotspots, in-building regions and campus-wide networks as well as Internet service provider (ISP) provisioning networks.

In Korea, there is a broadly serviced ISP provisioning WLAN network based on IEEE 802.11b, called NESPOT [4]. Korea Telecom (KT), the largest telecommunication and Internet service company in Korea, has operated NESPOT since early 2002 [1]. As of early 2005, there are over 420,000 subscribers of NESPOT and about 15,000 hotspots with about 39,000 access points (APs) in operation. However, as the number of subscribers and deployed APs increase, KT has been encountering a number of issues related to service quality of NESPOT and has made efforts to remove the obstacles.

In this paper, we analyze the initial access procedure of NESPOT and show that Dynamic Host Configuration Protocol (DHCP) could take the longest time among protocols comprising the NESPOT initial access procedure. Based on the analysis, we propose a Medium Access Control (MAC) layer level fragmentation which is specified in [3] as a mandatory feature for the purpose of enhancing reachability, goodput, and delay performance in marginal area (i.e., bad channel quality region). It is not the first attempt to apply fragmentation for the purpose of goodput enhancement. Qiao and Choi proposed an optimal link adaptation scheme combining dynamic fragmentation and ideal Physical layer (PHY) rate adaptation [11]. However, they do not focus on goodput and delay performance at marginal areas. In [11], fragmentation is just considered as a supporting scheme for ideal link adaptation, and the authors actually conclude that the fragmentation is not as effective as PHY rate adaptation.

We believe that this work is the first attempt to analyze public WLAN (KT NESPOT) access procedure with respect to the link quality, especially at marginal areas as well as to adapt IEEE 802.11 fragmentation scheme practically. As a more practical solution, we also propose TCP Maximum Segment Size (MSS) spoofing which can obtain the same effect as the fragmentation in the case of TCP traffic. In spite of the enhancement, users can still suffer from very long waiting time to receive a DHCP failure notification as far as signal quality decreases at marginal area. Accordingly, we propose a practical notification of DHCP failure, called Cut-off delay for user not to wait too long time in such an area where the successful network access probability is very low.

The rest of the paper is organized as follows. NESPOT initial access procedure and IEEE 802.11 fragmentation are described in Section 2 and 3, respectively. In Section 4, we evaluate the performance of NESPOT initial access procedure and propose schemes to enhance reachability, delay performance and success probability. Finally, this paper concludes with Section 5.

2. Initial Access Procedure in KT NESPOT

The initial access procedure of NESPOT is composed of IEEE 802.11 association process, IEEE 802.1x authentication process, and DHCP protocol, which occur in order. In the following, each process will be described in detail.
2.1. IEEE 802.11 Association Process

IEEE 802.11 association process can be divided into three steps, namely, scanning, authentication, and association [3]. The objective of scanning is to find the potential APs to associate with, in all available channels\(^1\). After scanning, STA attempts to get authenticated and associated with the selected AP. The left figure in Fig. 1 shows the frame exchange sequence for the 802.11 association.

2.2. IEEE 802.1x Authentication Process

After sending an acknowledgement (Ack) frame as the reply of an association response frame, the STA starts IEEE 802.1x authentication by transmitting an EAPOL (EAP over LAN)-start\(^2\) frame to the associated AP, and an exchange of 802.1x frames follows as shown at the right side of Fig. 1 [5]. Besides this figure, there is an illustrated 802.1x authentication entity, RADIUS (Remote Authentication Dial In User Service) server which is called authentication server in IEEE 802.1x terminology, while STA and AP are named by supplicant and authenticator, respectively [13]. After the AP receives an EAP Response-identity frame, the AP forwards it to its RADIUS server, and hence the next exchange of frames follows.

As shown in Fig. 1, EAP-MD5 uses user identification and password to authenticate the user. However, current Windows OS such as Windows XP does not support EAP-MD5. Therefore, a software which takes care of the EAP-MD5 authentication is needed. For NESPOT users, KT connection manager (CM) to support various WLAN devices such as laptops, PDAs, and so on. By using the CM, a NESPOT user authenticated via EAP-MD5 can access the network.

2.3. DHCP Process

When IEEE 802.1x authentication is initiated, Dynamic Host Configuration Protocol (DHCP) is also launched at the same time in NESPOT initial access procedure [8]. As shown in Fig. 2, DHCP protocol consists of four-way handshaking of broadcast frames, after initial random waiting time (randomly chosen between 1 and 10 seconds). However, as all the uplink packets are sent by unicast transmission in IEEE 802.11 infrastructure mode, there are downlink acknowledgements (Acks) in terms of the two uplink transmissions of DHCP such as DHCP Discover and DHCP Request. Accordingly, there can be MAC level retransmissions for the two uplink transmission, while downlink transmissions (i.e., DHCP Offer and DHCP Ack) are still sent via broadcast. In [8], four times of retransmission in terms of DHCP Discover and DHCP Request are defined as an automatic repeat request (ARQ) with exponentially increasing backoff times. That is, if the first DHCP Discover packet is not sent correctly, STA retransmits DHCP Discover after 4 seconds and after that, 8, 16, and 32 seconds are used to retransmit it, and the DHCP delay can be up to 2 minutes. This is the reason why DHCP process is dominant with respect to delay performance\(^3\).

In this paper, we propose modified DHCP processes such as unicast DHCP and unicast-fragmented DHCP in order to improve the delay performance and successful rate of NESPOT initial access at marginal area. The idea of unicast-fragmented DHCP stems from relative large size of DHCP packets compared to that of 802.1x and 802.11 frames. The larger the frame size, the higher the frame error rate (FER), and hence we pay attention to the fragmentation capability of IEEE 802.11 WLAN. However, as DHCP packets should be transmit via broadcast intrinsically, MAC level fragmentation is not valid. Therefore, we assume that AP can translate MAC addresses in DHCP Offer and DHCP Ack packets because AP can already know it through the previous DHCP Discover or DHCP Request packets. The overhead of this translation is just implementation issue and the translation itself may be easily implemented on AP. Accordingly, the four-way DHCP process can be dealt via unicast, and we assume that the unicast translation function is implemented on AP when we analyze the performance of NESPOT initial access procedure in Section 4\(^4\).

\(^1\)There are two types of scanning methods: active and passive. In KT NESPOT, active scanning is mainly used.

\(^2\)Extensible Authentication Protocol - Message Digest 5 (EAP-MD5) is used in NESPOT-802.1x authentication and its detailed operation is out of scope of this paper [6].

\(^3\)We omit IEEE 802.1x ARQ which is modified slightly in NESPOT, because it affects minor portion on NESPOT delay performance, as mentioned in Section 4.

\(^4\)In this paper, we have just focused on the initial operation of DHCP, even though a number of other functions and descriptions are defined in [8].
3. Fragmentation in IEEE 802.11

The process of partitioning a MAC service data unit (MSDU) into smaller MPDUs is called fragmentation [3]. Generally, fragmentation creates MPDUs smaller than the original MSDU length to increase reliability, by increasing the probability of successful transmission of the MSDU in cases where channel characteristics limit reception reliability for longer frames. The process of recombining fragmented MPDUs into a single MSDU is referred to as defragmentation. Defragmentation is accomplished at each immediate recipient, which is the STA or AP receiving those MPDUs. When a unicast MSDU is received from the upper layer, i.e., 802.2 Logical Link Control (LLC) in case of 802.11, with a length greater than a fragment threshold, the MSDU shall be fragmented. The minimum fragment threshold value is defined to be 256 octets. In Section 4, we use the minimum fragment threshold, i.e., 256 octets, to evaluate how effective fragmentation is.

Each fragment is sent as an independent transmission and is acknowledged separately. Therefore, if there is no acknowledgement, the fragment is retransmitted. Once a station has contended for the medium, it shall continue to send fragments with SIFS (short inter-frame space) gap between the Ack reception and the start of the subsequent fragment transmission until either all the fragments of a single MSDU have been sent, or an Ack frame is not received. The process of sending multiple fragments after contending for the medium is called fragment burst. However, if any fragment transmission fails, STA shall attempt to retransmit the failed fragment after a backoff procedure.

Table 1. MPDU size used in each protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Size of MPDU (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.11 association</td>
<td>34 ~ 46</td>
</tr>
<tr>
<td>IEEE 802.1x authentication</td>
<td>41 ~ 68</td>
</tr>
<tr>
<td>DHCP</td>
<td>364 ~ 384</td>
</tr>
</tbody>
</table>

4. Performance Evaluations

In this section, we analyze NESPOT initial access procedure via both mathematical analysis and simulations. Even though 802.11 association and 802.1x authentication processes are ahead of or start simultaneously with DHCP process, the formers do not severely affect initial access error and average initial access delay of NESPOT. That is, at the marginal areas, DHCP protocol is the dominant process, which influences the error and the average delay due to its relatively large packet size. Table 1 shows packet sizes of each protocol used in NESPOT initial access procedure. In all the results shown in later subsections, however, the whole processes are reflected.

For simulation, we use the ns-2 simulator [2]. We have added IEEE 802.11 association, IEEE 802.1x EAP-MD5 authentication and DHCP protocols as mentioned in Section 2 in the ns-2 simulator. We use MAC retry limit as 7 times and consider all the parameter used in analysis and simulations as standard values recommended in [3, 4]. We have simulated 1,000 times in order to average out the delay at every distance and every DHCP mode when the error probability is not too bad (i.e., under 0.9), while we have repeated 10,000 times at the marginal area where the error probability is above 0.9\(^5\). We do not consider the effect of contention at the MAC, because it must be relatively minor compared with the long delaying DHCP process. For the effective analysis of the lazy ARQ performance of DHCP protocol, we omit initial random waiting time of DHCP mentioned in Section 2.3 in mathematical analysis and simulations.

4.1. IEEE 802.11b PHY Model

We have used empirical bit error rate (BER) curves vs. signal-to-noise ratio (SNR) provided by Intersil for its chip called HFA3861B [9]\(^6\). These curves have been used to estimate frame error rate (FER) in both mathematical and simulation analysis. Fig. 3 shows FER vs. SNR for three different frame sizes when the 1 Mbps mode of IEEE 802.11b PHY is used. We assume that the lowest PHY transmission rate, i.e., 1 Mbps may be mainly used at marginal area by means of the traditional link adaptation scheme such as automatic rate fallback (ARF) [10]. To reflect a path loss effect, we use the log-distance path loss model with the path loss exponent of four [12], which is suitable for indoor office environments.

Considering low power devices, such as PDAs and laptops, link asymmetry condition can easily occur. For example, if a STA uses low transmission power, uplink and downlink goodput performance will not be the same at marginal area. This kind of environment is not hard to find. To quantify the degree of asymmetry, we adapt the concept of balance index introduced in [7] to reflect the unfair throughput achieved by STA and AP. Let \( B_i \) be the throughput at entity \( i \), then the balance index \( \beta \) is defined as

\[
\beta = \frac{\left( \sum B_i \right)^2}{n \left( \sum B_i^2 \right)}
\]  

\(^5\)At marginal area, there can be discordance between the average delays from mathematical and simulation results due to small size of delay samples. To achieve higher resolution of results, we simulate 10 times more compared with good channel quality region.

\(^6\)The BER curves for the HFA3861B are measured in an AWGN environment without any channel fading.
where \( n \) is the number of entities, which are AP and STA in this case. The balance index is 1 when AP and STA have the same throughput and tends to \( 1/n \) when the throughput is severely unbalanced, i.e., link asymmetry. We consider the link asymmetry environment in which STA has the half of the transmission power of AP as well as link symmetry environment. That is, when the link asymmetry is considered, the transmission powers of AP and STA are set to 100 mW and 50 mW, respectively. By applying (1) and asymmetric powers, we can get the degree of asymmetry as shown in Fig. 4.

### 4.2. Mathematical Evaluation

As the failure of IEEE 802.11 association and 802.1x authentication process have negligible contribution to the result, we present only DHCP process in this section, even if the whole processes are considered in real calculation. We first derive the failure probability of DHCP process. The successful transmission probability of a single frame within a given transmission retry limit, \( M \), can be represented by \( 1 - p^M \), where \( p \) is the frame error probability.

Let us consider that DHCP Discover and Offer packets to be transmitted up to \( K \) and \( L \) times, respectively, which include the initial attempt as well as the subsequent \((K-1)\) and \((L-1)\) retransmissions. (i.e., in case of unicast or broadcast, this value can be 8 or 1, respectively.) Moreover, DHCP client can retransmit packets up to \((M-1)\) times. (In NESPOT, \( M \) is set to 5.)

It should be noted that the first two packets, i.e., DHCP Discover and Offer, operate exactly the same as DHCP Offer and Ack in terms of DHCP ARQ policy and packet size. Let \( P_{f_1} \) and \( P_{f_2} \) be the failure probabilities of DHCP Discover and Offer packets, respectively. Accordingly, failure probability \( P_{fail} \) of overall DHCP process is given by

\[
P_{fail} = 1 - [1 - (1 - P_{f_1}^K) \cdot (1 - P_{f_2}^L)]^M. \tag{2}
\]

If we assume link symmetry, \( P_{f_1} \) and \( P_{f_2} \) become the same. Considering unicast-fragmented DHCP, the failure probability of each DHCP packet can be represented by

\[
P_{f_{frag}} = 1 - \prod_{k=1}^{n} \left(1 - P_{f_{frag(k)}}^8 \right) \tag{3}
\]

where all \( P_{f_{frag(k)}} \) (\( 1 \leq k \leq n-1 \)) have the same value possibly except for that of the last fragment due to a potentially different frame size.

Next, we compute the average delay of DHCP process. Let us denote the average DHCP delay as \( \overline{D} \). When a DHCP process with \( MK \) or \( ML \) time retransmissions is successfully completed, there exist a lot of possible combinations of probability and delay. We define a set which has combinations of probability and delay mentioned above as elements, and denote it as \( A_{pd} \) (i.e., it means probability-delay set of process \( A \)). We also define a notation, \( x \), to calculate \( \overline{D} \) effectively, and the operation can be written by

\[
A_{pd} \times B_{pd} = \{(p_a \cdot p_b, d_a + d_b) \mid (p_a, d_a) \in A_{pd} \text{ and } (p_b, d_b) \in B_{pd}\} \tag{4}
\]

where \( p_a \) is the probability when delay is \( d_a \) in set \( A \).

For simplicity of presentation, we assume MAC frame (re)transmission delay to be zero second due to the negligibly small time scale, even though it is reflected in real calculation. By applying (3), \( D_{pd} \) (i.e., probability-delay set of success DHCP process) can be obtained as

\[
D_{pd} = D'_{pd} \times D''_{pd} \tag{5}
\]

where \( D'_{pd} \) is probability-delay set of the process until DHCP Offer is transmitted.

\[
D''_{pd} = \bigcup_{k=1}^{5} \{( (1 - P_s)^{n-1, P_s, D_k} \} \tag{6}
\]

where \( P_s \) is the success probability until DHCP Offer is transmitted, and \( D_k \) means the delay when the number of DHCP retransmissions is \( k \) times.

Therefore, the average DHCP delay can be obtained as

\[
\overline{D} = \sum_{(p,d)\in D_{pd}} p \cdot d \tag{7}
\]

### 4.3. Results and Discussion

Figs. 5 and 6 present the initial access error probability and average initial access delay of NESPOT, respectively. In each figure, three modes of DHCP are illustrated as mentioned in Section 2.3, such as broadcast DHCP, unicast DHCP and, unicast-fragmented DHCP in each of symmetric and asymmetric link cases.\(^8\) Both of the mathematical and simulation results are also shown in the figures. The two results, i.e., error probability and average delay, are calculated and simulated at the same time. Therefore, we can draw one line of mathematical analysis and points of simulation results after one run of calculation and simulation in each mode. In the case of symmetric link, we can easily confirm the utility of unicast DHCP and unicast-fragmented DHCP compared to the original DHCP. For example, with the similar error probability of 10\% approximately, we can get four meters gain by applying unicast-fragmented DHCP.

In average delay (Fig. 6), a similar example can be found. Comparing original and unicast-fragmented DHCP with

\(^8\)We assume 612-byte for each DHCP MPDU size, which is the maximum value of DHCP packet size [8]. Note that this is different from the one in Table 1.
about 5 seconds delay, we also confirm that we can get 5 meters range extension with proposed DHCP (from 77 to 82 meters). However, there is no gain for unicast DHCP compared with the original broadcast DHCP in the asymmetric link case, while there exists one or more meter gain with unicast-fragmented DHCP. This is because the uplink is the bottleneck in the asymmetric link case, and hence it does not matter whether the downlink packets are transmitted via broadcast or unicast.

Figs. 7 and 8 show probability mass functions (PMFs) at particular positions. We have generated PMFs at every position shown in Fig. 5 and 6, i.e., from 65 to 85 meters, and four of them are illustrated in Figs. 7 and 8. In both figures, the first PMF is calculated and simulated at a relatively better channel quality area, while the second PMF is from a relatively worse condition. As the unit of horizontal axis, multiples of 20 and ‘Error’ are used. Every point represents that the sum of number of samples between the horizontal coordination and the next, while the last, i.e., ‘Error’ represents the portion of number of error samples. As illustrated in vertical axis, all the points are normalized by the total number of simulations. The first point or bar of the first PMF of each figure has relatively high portion with respect to the overall distribution. That is the reason why the cases of the first, the second and no retransmission of DHCP process (DHCP discover or DHCP request) are considered altogether in the first point or bar. However, the portion of over 12 (the 2nd retransmission) seconds delays can be observed more often at the second PMF of each figure. As shown in all the PMFs, unicast-fragmented DHCP has the best delay performance than others. Unicast DHCP takes shorter delay than original DHCP in symmetric case, while this gain is not shown in asymmetric case.

As proposed above, the reachability of NESPOT can be improved via fragmentation. On the other hand, fragmentation must be also used for normal data frames, which could have larger sizes up to 1500-byte. Otherwise, the data transmission performance after a successful initial access could be unacceptable as one can easily imagine from Fig. 3.

### 4.4. Practical Approach – TCP MSS spoofing

In spite of the advantage of fragmentation mentioned above, it is not easy to use it practically, because it implies that AP and STA should agree on the functionality altogether. Even though implementation of the fragmentation is mandatory, the usage of it is optional. Accordingly, it is of no use if it is not activated at STA, even though AP wants to use it.

As an alternative and practical approach, we propose **TCP MSS spoofing**. An end device can inform a specific MSS it wants to use during the TCP connection establishment process. The end device, which chooses to do so, includes a TCP option, called MSS, in its SYN message header. The other device receives this option and records the MSS for the connection. Each device can specify the MSS it wants for the segments and receives independently. By using this, AP can spoof the TCP SYN message during the connection establishment process and change its MSS value considering the current channel quality between AP and target STA. For example, the value of MSS should be 180 bytes (MSS is the maximum amount of application-level data in the segment) to achieve the same effect of fragmentation with the minimum fragment threshold:

\[
180\text{-byte application-level data} + 20\text{-byte TCP header} + 20\text{-byte IP header} + 8\text{-byte LLC header} + 28\text{-byte MAC header} = 256\text{ bytes}
\]

### 4.5. Need for Cut-off Delay

As shown in Fig. 7 and 8, the worst case of DHCP delay can be about 120 seconds, even if the average delay is saturated with above 40 seconds as shown in Fig. 6. Users of NESPOT can be annoyed if they should wait for at most 2 minutes to get an IP address. Moreover, it is basically impossible to communicate normally in such a long latency region, as shown in Fig. 5, even if STA can get an IP address. For example, average delay to get an IP address at 82 meters is above 35 seconds, while the access error probability is above 95%.

From this observation, we concentrate on how user’s waiting time to get an IP address can be reduced without severe performance degradation. Concerning MAC level retransmission of 7 times (specified in [3]), the fact that DHCP retransmission occurs implies that the channel condition is not good basically. However, if any DHCP retransmission is not considered, reliability of DHCP protocol decreases severely when collision of broadcast DHCP packets (DHCP Discover and Request packets) occurs. Consider-
5. Conclusion

In this paper, we propose a MAC-level fragmentation scheme to enhance reachability and goodput when WLAN user tries to access NESPOT at marginal areas. Using mathematical analysis and simulations, we demonstrate that the range extension of several meters with similar error probability and average delay can be achieved by using unicast-fragmented DHCP. This enhancement must be also reinforced for normal data frame transmissions since the data frame size could be much larger than DHCP packet size.

In spite of the range extension, users can still suffer long delay to get a DHCP failure message at the extremely low signal quality area. Accordingly, we propose a heuristic policy to shorten the user’s waiting time, called Cut-off delay. Using the heuristic method, the waiting time to recognize DHCP failure can be dramatically reduced.

Acknowledgment

This research was jointly supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment), and KT (Korea Telecom). Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the view of KT.

References