

A Reliable Active Scanning Scheme for the IEEE 802.11 MAC Layer Handoff*

Wei Li, Qing-An Zeng and Dharma P. Agrawal
 Center of Distributed and Mobile Computing,
 Department of Electrical & Computer Engineering and Computer Science,
 University of Cincinnati, Cincinnati, OH, 45221-0030
 {liw0, qzeng, dpa@ececs.uc.edu}

Abstract—In the IEEE 802.11 wireless local area networks (WLANs) with fixed access points (APs), handoff occurs when a mobile station (MS) with a communication in progress changes its associated AP from one to another. It is important to minimize the handoff latency because the active communications of a MS are interrupted before the handoff completes. Such a design needs to take into consideration the high error rate of WLANs. The IEEE 802.11 medium access control (MAC) protocol recommends an active scanning mode for the handoff process. The probe delay of the active scanning may increase greatly if the probe request is lost. However, the successful transmission of the probe request is very unpredictable due to the high collision probability and the lack of any acknowledgement. In this paper, we propose a highly reliable active scanning scheme which can be implemented with the current IEEE 802.11 channel scanning procedure. It is indicated to efficiently increase the reliability of channel scanning, especially in a noisy environment, by performing the probe request loss detection and retransmission. Furthermore, the proposed scheme reduces the overall handoff latency by providing a higher priority for management frames over data frames.

I. INTRODUCTION

One of the most striking changes in the recent use of technology has been the explosive growth in the use of wireless networks for Internet and local network access. As wireless local networks support mobility with high-speed information access, the IEEE 802.11 wireless local area network (WLAN) is being widely accepted for many different environments [1].

In the infrastructure-based mode, the IEEE 802.11 network is composed of fixed network access points (APs) and a number of mobile stations (MSs) associated with each AP. Whenever a user of an ongoing communication moves out of the radio range of one AP, and enters the range of a neighboring AP, handoff occurs. The word “handoff” in the IEEE 802.11 medium access control (MAC) layer refers to the process of a MS changing its associated AP from one to another. During a handoff process, the MS cannot send (receive) data frames to (from) its current associated AP because of the change of its working channel (frequency). Besides, in order to find and associate with a new AP, management messages are exchanged between the MS and

APs. As the active communications of a MS are interrupted before the handoff completes, there is a latency involved in the handoff process. It is important that the handoff process is performed without unacceptable disruption of ongoing communication sessions. As WLANs are being widely deployed, there is a trend to accept it for interactive real-time applications, such as mobile Internet audio, mobile video conferencing, etc. These multimedia applications make this problem more important since they require better quality of service (QoS) and are very sensitive to the connectivity loss.

The IEEE 802.11 MAC protocol recommends an active scanning mode for the handoff process. The effectiveness of the active scanning strongly depends upon whether the AP can successfully receive the probe request from the MS. Unfortunately, the transmission of the probe request is very unreliable due to the high collision probability and the lack of any acknowledgement. In this paper, we propose a simple and efficient reliable active scanning (RAS) scheme that performs probe request loss detection and fast retransmission. We observe that the proposed scheme can result in a significant probe delay decrease in a noisy environment by increasing the probability that an AP is successfully detected on an active channel. In addition, the frame scheduling mechanism included in the RAS scheme further decreases the overall handoff latency by providing the management frames higher priority than the data frames. The proposed scheme can be implemented with the existing IEEE 802.11 channel scanning procedure.

The rest of the paper is organized as follows. In Section II, we describe the handoff procedure of the IEEE 802.11 WLAN. We present the RAS scheme in Section III. Section IV is the simulation results and discussions. Conclusions are added in Section V.

II. IEEE 802.11 HANDOFF MECHANISMS

In the infrastructure-based network, when a MS moves away from the current AP, the signal-to-noise ratio of the link decreases and eventually it drops below a threshold value, which triggers the MS to initiate a handoff. The complete handoff process in the IEEE 802.11 MAC layer can be divided into three distinct sub-processes: scanning to obtain a suitable AP, authentication and re-association [2]. Fig. 1 shows the detail of the handoff procedures.

* This work has been supported by the Ohio Board of Regents, Ph.D. Enhancement Funds and the National Science Foundation under grant CCR-0113361.

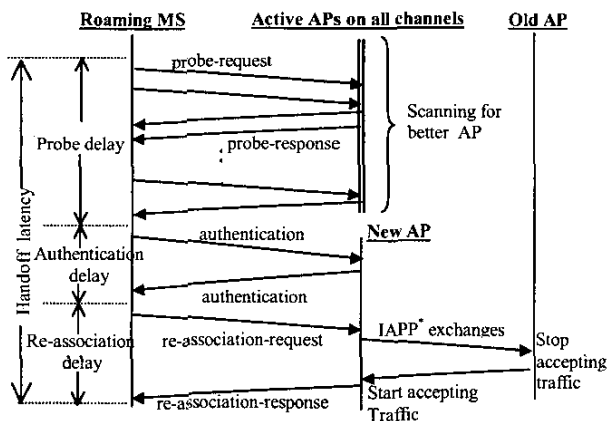


Fig. 1. Typical handoff procedures of the IEEE 802.11 MAC layer

A MS obtains a better AP by performing a series of scans on different channels. In WLAN, depending upon the regulatory domain, an AP can use one of up to 13 different channels. According to the IEEE 802.11 standard, scanning can be accomplished using either the passive or active scanning mode. In the passive scanning mode, the MS moves to each channel on the channel list and waits for the beacon signal. The passive scanning saves battery power but takes longer time. A fast way is to do active scanning. In the active mode, a MS actively broadcasts additional probe request frames on the channel scanned and expects to receive probe response from AP(s), apart from listening to beacon messages. The MS stays on each channel scanned for *minChannelTime* or *maxChannelTime*, depending on if the channel is active. The *minChannelTime* is the minimum time that a MS spends on each channel when scanning. It is the time to detect whether or not the channel is active. The *maxChannelTime* is the maximum time that a MS spends on each channel when scanning. It is the time to collect all possible probe responses on the channel if the channel has been detected active by *minChannelTime*.

Some channels may have no active AP while others may have more than one active AP. After the scanning process, the MS may obtain several available APs on different active channels. It chooses the best one in terms of signal strength or signal-to-noise ratio and enters the authentication process (Pre-authentication may be done to reduce the authentication delay [3]). When the new AP successfully authenticates the MS, re-association is performed. After that, the MAC layer handoff procedures are completed and all the packets from/to the MS will be relayed by the new AP.

III. RAS SCHEME

The IEEE 802.11 MAC layer handoff latency is the sum of probe delay, authentication delay and re-association delay. It can range from hundreds of millisecond to several seconds [4]. Previous studies [5][6] have shown that the probe is the primary contributor to the overall handoff latency. Generally, the probe delay accounts for more than 90% of handoff

latency. To reduce the probe delay, the active scanning mode is used. However, the efficiency of the active scanning strongly depends upon whether the AP can successfully receive the probe request from the MS. One major characteristic of wireless channel is error-prone. The probe request frame may be lost due to noise or collision. Because the probe request is a kind of broadcast message which does not require an acknowledgment (ACK), the MS cannot know immediately whether or not the transmission is successful. On the other hand, the request-to-send/clear-to-send (RTS/CTS) reservation mechanism cannot be used for broadcast transmissions. It makes the transmission of the probe request highly unreliable. If the MS detects an active channel within the *minChannelTime* but the probe request frame is lost, the MS will waste the whole *maxChannelTime*. Such channel may be re-scanned after the *maxChannelTime* expires, which results in a great increase in the probe delay.

Therefore, increasing the probability that the probe request is received by the AP within the *maxChannelTime* will help to reduce the probe delay. This is the strategy we have adapted in designing the reliable active scanning scheme. The RAS has two steps: response detection and traffic detection (see Fig. 2). In response detection, a short period is reserved exclusively for the AP to send the probe response. If the MS does not detect any transmission during that period, it considers this channel is inactive or the probe request frame is not correctly received by the AP. The traffic detection is performed if the MS fails to detect any transmission in the response detection period. If the MS successfully detects traffic on the channel by *minChannelTime*, it concludes that this is an active channel while the probe request is lost. Consequently, the probe request is retransmitted immediately without waiting for a *maxChannelTime* to expire.

A. Frame scheduling scheme for AP

In order to support the RAS scheme, we propose a frame scheduling scheme for the AP. In the IEEE 802.11 standard, there is no time limit for the AP to reply the probe response upon receiving the probe request. One factor affecting the time at which the probe response is transmitted is the service order by the AP when there are also data packets ready for transmission. We separate the management and data frames into two queues, management queue and data queue. A management frame has higher priority than any data frame to

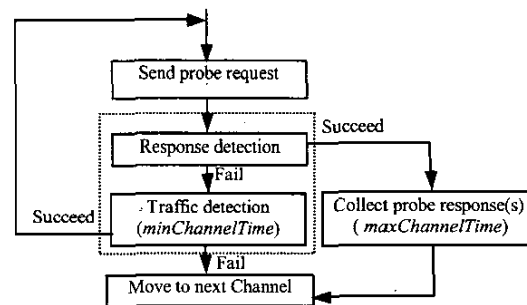


Fig. 2. Reliable active scanning

* Inter-Access Point Protocol

be serviced. Amongst management frames, the beacon signal and the probe response have the highest priority. (A regular beacon signal plays the similar role to the probe response, i.e., in the passive scanning mode.). Therefore, when the AP receives the probe request, it will send the probe response first. Since the handoff process involves a sequence of management frame exchanges between the MS and APs, the provision of high priority for management frames reduces the overall handoff latency and prevents ongoing connections from being broken, especially under higher traffic load conditions.

To comply with the standard, the two queues share the same contention window (CW). In the IEEE 802.11 standard, the CW takes an initial value of CW_{min} and exponentially increases every time an unsuccessful transmission occurs until it reaches the value of CW_{max} . We slightly modify such CW-adjustment approach in our scheme. When the AP is transmitting a management frame, the CW is reset to and fixed at CW_{min} . There is no exponential increase after an unsuccessful transmission of a management frame. This gives the AP high priority to gain access to the channel while transmitting management frames. Our objective is to drain the management queue as quickly as possible and reduce the queuing delay for the frames in the data queue. Moreover, the backoff timer, if applicable, is set to zero if the management frame to be sent is the beacon signal or it is the first transmission of the probe response. This ensures that the probe response is transmitted instantly after the channel is detected idle for a distributed interframe space (DIFS) period.

B. Response detection

In our scheme, a MS detects the transmission of the probe response to ensure the status of the probe request frame. A short period δ is defined as the response detection time, which immediately follows a DIFS after the transmission of the probe request (see Fig. 3). δ can be the length of several symbols such that traffic, if any, can be safely detected. According to the proposed frame scheduling scheme, the AP replies the probe response right away after the channel is detected idle for a DIFS interval upon receiving the probe request. Furthermore, we prevent other MSs from transmitting during the period δ . Therefore, if traffic is detected during the response detection time, the MS considers that this is an active channel and the transmission of the probe request succeeds. Otherwise, it considers either the channel is inactive or the probe request is lost.

The IEEE 802.11 MAC layer uses the physical carrier sensing as well as virtual sensing mechanism to avoid collision. The latter implements a network allocation vector (NAV), whose value indicates to each station the amount of

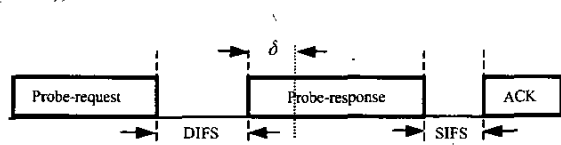


Fig. 3. Response detection in RAS

time that remains before the channel will become idle. All frames contain a Duration field and the NAV is updated according to this field value in each frame transmitted. To prevent other MSs from competing the channel with the AP during the response detection time δ , the Duration field of the probe request frame is set to $DIFS+\delta$. The AP neglects this value. Other MSs receiving the probe request update their NAV settings, which prevents them from transmitting during the period of $DIFS+\delta$.

The MS may consider the probe request is lost if the transmission of the probe response is delayed (e.g. by the transmission of a hidden station). In such a case, the MS will retransmit the probe request if it has been able to detect traffic by $minChannelTime$. The retransmission will be cancelled if the MS receives the probe response before the retransmission happens.

It should be noted that in our scheme the MS considers the probe request is successfully received by the AP as long as it detects traffic during the period of response detection time. Such implementation is very simple yet highly efficient. It is unnecessary to know for sure that the traffic detected is the probe response, which can only be done by correctly receiving the probe response frame. However, the probe response may be damaged by the noise or due to collision. The AP retransmits the probe response if it fails to receive ACK frame within the $ACK_timeout$ period. Therefore the MS does not have to worry about the correctness of the probe response.

C. Traffic detection

The traffic detection is executed if no traffic is detected during the response detection time. The MS keeps monitoring the channel until $minChannelTime$ expires. If no traffic is detected, the MS considers the channel is inactive; otherwise the MS claims that the channel is active but the probe request is lost.

The $minChannelTime$ should be large enough so that traffic is likely to be detected within $minChannelTime$ if the channel is active. The probe request frame is probably corrupted because no traffic has been detected during the response detection time. According to the IEEE 802.11 standard, a MS will defer until the medium is determined to be idle without interruption for an extended interframe space (EIFS) interval when the last frame detected on the medium was not received correctly [4]. Stations that do not receive the corrupted frame may initiate transfer during the EIFS. Therefore, in order to have a good probability of detecting traffic on this channel, the value of $minChannelTime$ should satisfy:

$$minChannelTime = EIFS + A, \quad (1)$$

where A is an additional time following the EIFS and should be larger than the smallest backoff time of those MSs desiring to start transmission after the EIFS (see Fig. 4).

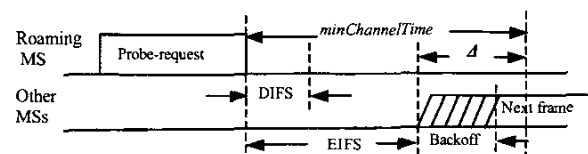


Fig. 4. Traffic detection in RAS

If traffic is detected within $minChannelTime$, the MS claims that the channel is active but the previous transmission of the probe request has failed. Consequently, the MS retransmits the probe request and repeats the response detection and traffic detection procedures. The probe request may be retransmitted many times before $maxChannelTime$ expires. However, there should be enough time remaining in the $maxChannelTime$ to allow transmission of the probe response plus the ACK. If no traffic is detected by $minChannelTime$, the MS considers the channel is inactive and moves to the next one.

IV. SIMULATION RESULTS AND DISCUSSIONS

In this section, we compare the proposed RAS scheme against the basic active scanning scheme of the IEEE 802.11 standard. We implement the RAS scheme in the network simulator ns2 [7]. In all the simulations, the MS performs a full channel scanning and the total number of channels scanned is 11. Two of them, including the current one, are active. Each active channel has one AP and 30 MSs communicating at background. All the parameters used in our simulations follow the specifications in the standard and some of them are listed in Table 1. Both schemes use the same values of $minChannelTime$ and $maxChannelTime$.

$minChannelTime = EIFS + SlotTime * CW_{min} = 984\mu s$,
 $maxChannelTime = 30ms$.

In RAS, the response detection time δ is $20\mu s$. The inter-arrival time and burst time of data frames are taken from exponential distributions. We do not consider the data processing time in the simulations.

TABLE 1
PARAMETERS USED IN SIMULATIONS

Slot Time	SIFS	DIFS	CW_{min}	CW_{max}	Data Rate	Basic Rate
$20\mu s$	$10\mu s$	$50\mu s$	31	1023	11Mbps	1Mbps

We first perform simulation to evaluate the probe delay by changing the bit error rate (BER) of the channels. In our simulation, if the MS has detected traffic on a channel but failed to receive the probe response during a $maxChannelTime$, it rescans this channel immediately. The simulation results are shown in Fig. 5, which indicates that in a noisy wireless environment (i.e. $BER > 10^{-4}$), the RAS achieves significant improvement on probe delay as compared to the basic active scanning scheme. This is because the RAS scheme can successfully complete scanning an active channel within one $maxChannelTime$ most of the time while the basic active scanning scheme will use more than one $maxChannelTime$ to scan an active channel if the probe request is lost.

Fig. 6 shows the average measurements of the overall handoff latency. We simulate the scenarios in which the channel is error-free ($BER=0$) and the channel is noisy ($BER=2 \times 10^{-4}$). In both scenarios, the proposed scheme achieves smaller handoff latency than the basic active scanning scheme. The difference increases as the offered traffic load increases. In RAS, there is little queuing delay for management frames. For the basic active scanning scheme, management and data frames are serviced in the first-in-first-out (FIFO) discipline. Queuing

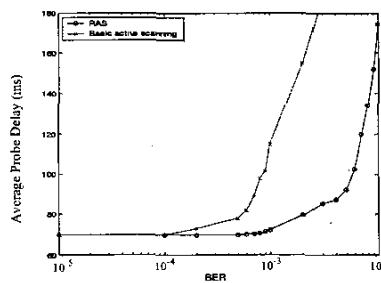


Fig. 5. Average probe delay versus BER

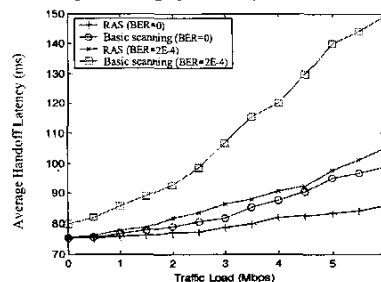


Fig. 6. Average handoff latency versus traffic load

delay of management frames increases the handoff latency. Such queuing delay increases dramatically in the noisy channel, in which frequent frame retransmissions take place.

V. CONCLUSIONS

One challenge of wireless communication is to minimize the handoff latency. In the basic active scanning method of the IEEE 802.11 standard, the unreliable transmission of probe request frame results in a great increase in handoff latency. In this paper, we presented a simple yet highly efficient reliable active scanning scheme for the IEEE 802.11 MAC layer handoff. The proposed scheme greatly decreases the probe delay in a noisy environment by performing probe request loss detection and retransmission. Also, our scheme decreases the overall handoff latency by giving management frames higher priority than data frames.

REFERENCES

- [1] D. P. Agrawal, Q-A Zeng, *Introduction to wireless and mobile system*, ISBN No. 0534-40851-6, 438 pages, Brooks/ Cole publishing, 2003.
- [2] IEEE. Part 11 "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" IEEE Standard 802.11, 1999.
- [3] S. Pack and Y. Choi, "Fast Inter-AP handoff using predictive authentication scheme in a public wireless LAN," *Networks*, Atlanta, 2002.
- [4] N. Montavont and T. Noël, "Handover Management for Mobile Nodes in IPv6 Networks," *IEEE Communications Magazine*, pp. 48-54, August 2002.
- [5] H. Yokota, A. Idoue, T. Hasegawa and T. Kato, "Link Layer Assisted Mobile IP Fast Handoff Method over Wireless LAN Network," *MobiCom*, Sep. 2002.
- [6] A. Mishra, M. Shin and W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," www.cs.umd.edu/~waa/pubs/handoff-lat-acrn.pdf.
- [7] K. Fall and K. Varadhan, "The ns Manual," University of California, Berkeley, April 2002.