A Novel Hidden Station Detection Mechanism in IEEE 802.11 WLAN

Youngsoo Kim, *Student Member, IEEE*, Jeonggyun Yu, *Student Member, IEEE*, Sunghyun Choi, *Senior Member, IEEE*, Kyunghun Jang

***Abstract*— The popular IEEE 802.11 Wireless Local Area Network (WLAN) is based on a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), where a station listens to the medium before transmission in order to avoid collision. If there exist stations which can not hear each other, i.e., hidden stations, the potential collision probability increases, thus dramatically degrading the network throughput. The RTS/CTS (Request-To-Send/Clear-To-Send) frame exchange is a solution for the hidden station problem, but the RTS/CTS exchange itself consumes the network resources by transmitting the control frames. In order to maximize the network throughput, we need to use the RTS/CTS exchange adaptively only when hidden stations exist in the network. In this letter, a simple but very effective hidden station detection mechanism is proposed. Once a station detects the hidden stations via the proposed detection mechanism, it can trigger the usage of the RTS/CTS exchange. The simulation results demonstrate that the proposed mechanism can provide the maximum system throughput performance.**

***Index Terms*— IEEE 802.11, WLAN, hidden station.**

I. Introduction

During the last few years, IEEE 802.11 Wireless LANs (WLANs) have become very popular among nomadic users for the Internet access using their portable devices. The performance of the 802.11 WLAN is severely degraded when there are some stations which are in the same network but can not hear each other since they are far from each other. For example, if two stations are located in the opposite boundaries in the same cell, these two stations can communicate with their access point (AP), which is located at the center of the cell, but they might not hear each other. These stations are called "hidden stations." Since the IEEE 802.11 WLAN is using CSMA/CA, the hidden stations may increase the potential collisions. One solution to remedy the hidden station problem is that the stations can use the Request-to-Send/Clear-to-Send (RTS/CTS) exchange before a data frame transmission. However, using the RTS/CTS does not provide a better performance if the hidden stations do not exist. Therefore, the best policy is to use the RTS/CTS exchange only when hidden stations exist. In this letter, we present a simple hidden station detection mechanism using acknowledgment (ACK) frames and the length field in PHY Layer Convergence Procedure (PLCP) header. With the proposed scheme, a station can easily detect the hidden stations when they exist.

The rest of the letter is organized as follows: A brief overview of IEEE 802.11 is presented in Section II. The definition of hidden station and a hidden station detection mechanism are presented in Section III. After evaluating the effectiveness of the hidden station detection mechanism via simulation, we conclude the letter in Section IV.

This research was in part supported by Samsung and Information Technology Research Center (ITRC). The authors are with the School of Electrical Engineering and INMC, Seoul National University, Seoul 151-744, Korea.

II. IEEE 802.11 Overview

In this section, we briefly review the characteristics of IEEE 802.11 [1]. Under the default 802.11 MAC, called Distributed Coordination Function (DCF), when a station has a frame to transmit, it detects whether the medium is idle or not. If it detects that the medium is occupied by another station, it defers the frame transmission until the medium becomes available for the transmission. After the station detects that the medium is idle for a certain period of time, which is the DCF Interframe Space (DIFS), it starts a backoff operation with a randomly-selected backoff count value. This random backoff count decreases by one for each idle slot time. When the backoff count becomes zero, the station transmits the frame. When the receiving station receives this frame successfully, it transmits an ACK frame back to the source station after a Short Interframe Space (SIFS) interval. When the source station receives the ACK frame, the transmission operation of that frame is finally completed.

The 802.11 MAC defines the exchange of RTS/CTS frames in order to protect the data and ACK frame exchanges by overcoming the hidden station problem. However, the RTS/CTS exchange is an expensive solution since it itself consumes the precious wireless bandwidth. The usage of the RTS/CTS exchange is controlled using RTS_Threshold; when the length of the pending MAC frame is larger than the threshold, an RTS/CTS exchange precedes the frame transmission. Accordingly, the RTS/CTS exchange can be enabled/disabled by adjusting the threshold value.

We also briefly overview how a frame is generated in IEEE 802.11a PHY based on Orthogonal Frequency Division Multiplexing (OFDM) [2]. It should be noted that the proposed hidden station detection scheme can be used for any 802.11 PHY. When a MAC frame is forwarded to the underlying PHY for its transmission, the PHY generates a PHY Protocol Data Unit (PPDU) as shown in Fig. 1, where the PHY Service Data Unit (PSDU) field is occupied by the MAC frame received from the MAC. Note that PPDU is the frame format, which is transmitted into the wireless medium.

The PLCP preamble is composed of a pre-determined symbols, and is used by a receiving station in order to detect the receiving frame. Two important subfields in the PLCP

header are RATE and LENGTH fields. As illustrated in Fig. 1, the SIGNAL field, which is the first part of the PLCP header, is composed of one OFDM symbol modulated with Binary Phase Shift Keying (BPSK) and coded by rate-1/2 convolutional code (i.e., transmitted at 6 Mbits/s.) The rest of the PPDU, marked as Data in the figure, is transmitted at the PHY rate specified in the RATE field, where 8 different rates from 6 to 54 Mbits/s are supported. The LENGTH field specifies the length of the MAC frame (i.e., PSDU) contained in the Data field.

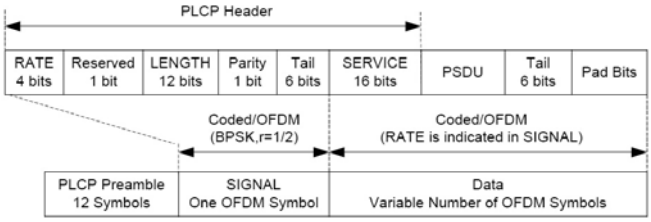

Fig. 1. Basic frame format of IEEE 802.11a.

In this letter, we consider two radio ranges, namely, data transmission range and carrier sense range. The data transmission range is defined as the range, in which stations can receive and decode a transmitted frame successfully. Apparently, this range depends on the employed transmission rate. The carrier sense range is defined as the range, in which stations can physically sense the medium busy during the data transmission. The mechanism to detect a frame transmission is referred to as Clear Channel Assessment (CCA), which can be performed by two methods: carrier detection, i.e., preamble detection, and energy detection. In the case of the 802.11a, both methods can be used, where the energy detection threshold (-62 dBm) is higher than the carrier sense threshold (-82 dBm). The receive sensitivity of 6 Mbits/s transmission is also -82 dBm.

III. Hidden Stations

A. Definition of Hidden Station

The basic rule of CSMA/CA is that a station needs to listen to the medium before a frame transmission. However, if the network is large, it is not possible to hear all the stations in the same network. A station might not know the existence of other stations, which are associated with the same AP. Such stations are called hidden stations. Here is a formal definition of a hidden station. A hidden station to a particular station (referred to as STA A) is a station that is not capable of making CCA busy at STA A[1], but, at the same time, is capable of making CCA busy at a communication party station, which is capable of making CCA busy at STA A.

B. Impact of Hidden Station

Manipulating hidden stations in WLAN is important since the hidden stations can severely degrade the system performance [5]. Fig. 2 shows the impact of hidden stations via NS-2 simulation [6] for both basic access (i.e., without RTS/CTS) and RTS/CTS access cases of the 802.11 DCF. We assume the 802.11a PHY, and the best transmission rate, achieving the maximum throughput performance, for a given transmission is employed. In this simulation, a single AP is located at the center of the network and eight stations are uniformly located at the edge of a cell. All stations transmit 1500-byte frames to the AP in a greedy manner. The throughput performance is measured when the cell radius varies from 11 m to 45 m. The throughput performance drastically decreases after the cell radius exceeds 21 m. If the cell radius is larger than 21 m, the stations cannot hear the frame transmission from the station located at the opposite side. If RTS/CTS exchange is used before the frame transmission, the hidden stations do not affect the system throughput. However, the overhead of RTS/CTS exchange is clearly observed when the cell radius is small.

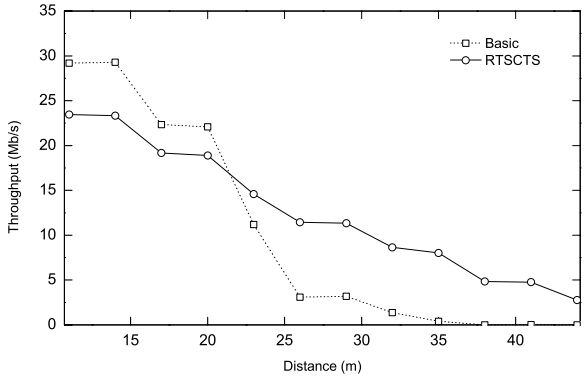

Fig. 2. Impact of the hidden stations.

C. Hidden Station Detection

Fig. 3 shows various ranges and a frame reception status diagram when a transmitting station (TX STA) sends a data frame and a receiving station (RX STA) responds with an ACK frame after a SIFS interval. At the left side of the figure, TX STA sends a data frame to RX STA at a selected rate. The data transmission range is indicated by a small dotted circle. The large dotted circle represents the carrier sense range for that data frame. The right side of the figure shows the frame reception status for the stations in the area numbered at the left side of the figure. That is, only correctly-received parts of the transmitted frame are shown in the figure. A light rectangle represents the PPDU and a dark rectangle inside the light rectangle represents the corresponding PSDU. The stations in the carrier sense area detect the frame transmission, but cannot decode the PSDU part of the frame correctly.

The stations in area 1 are not hidden from TX STA since they can decode the PLCP header of the frame while they fail to decode the data frame correctly. The stations in areas 2 and 3 are not hidden from TX STA because they hear both data and ACK frames. The stations in areas 4 and 5 are clearly hidden form TX STA. Those stations hear only the ACK frame from RX STA. Therefore, it is possible to say that a station knows the existence of the hidden station when it hears only an ACK frame without detecting the preceding data frame transmission, i.e., after over SIFS idle interval.

[1]The statement that “STA B can (cannot) make CCA busy at STA A” is equivalent to the statement that “STA A assesses that the medium is busy (idle) when STA B is transmitting a frame.”

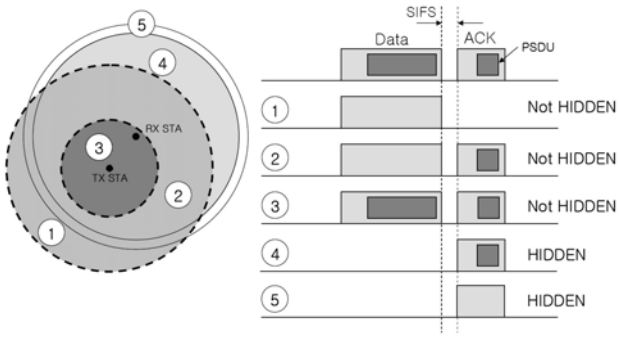

Fig. 3. Various ranges when TX STA sends a data frame to RX STA.

When the station hears the ACK frame, it may or may not decode the PSDU part of the ACK frame. When the PSDU part is not decoded correctly, i.e., Frame Check Sequence (FCS) failure, RX STA cannot tell that the received frame is an ACK frame. Instead, the length field in the PLCP header can be used since only ACK and CTS frames have the unique length field value of 14 (octets) [1]. Therefore, a station can detect the existence of a hidden station using one of the following conditions.

- An ACK reception when the medium has been idle over SIFS interval.
- A reception of a frame with the PLCP header including Length = 14 (i.e., either ACK or CTS) octets while the FCS failure occurs from the frame reception and the medium has been idle over SIFS interval.

In both cases, the station is able to detect the existence of the hidden station. For the first condition, the station obtains the MAC address of the hidden station from the receiver address of the ACK frame. For the second condition, the station cannot obtain the MAC address of the hidden station. The station acquires only the existence of the hidden station, which is enough to switch the RTS/CTS exchange. It should be noted that the content of the length field in PLCP header varies depending on the underlying PHY. The length field of the PLCP header in IEEE 802.11a and the mandatory mode of IEEE 802.11g PHY [4] contains the length information in byte as shown in Fig. 1 while that of IEEE 802.11b PHY [3] contains the frame transmission time duration in milliseconds. However, the duration can be easily converted to the length since the transmission rate information is also available from the PLCP header. The process of the hidden station detection algorithm is shown in Fig. 4.

IV. Performance Evaluation and Conclusion

In order to demonstrate the effectiveness of the hidden terminal detection, the simulation environment used for Fig. 2 is considered again. Stations use the proposed hidden station detection scheme in order to detect the existence of the hidden stations, thus adaptively employing the RTS/CTS exchange. Fig. 5 shows that the proposed scheme basically achieves the best of basic and RTS/CTS access performances for a given distance between the AP and stations.

In this letter, a hidden station detection mechanism is proposed. The proposed scheme allows a fast hidden station detection without changing the current specification. The hidden station detection can be used in order to decide whether to use the RTS/CTS exchange adaptively in order to maximize the system performance.

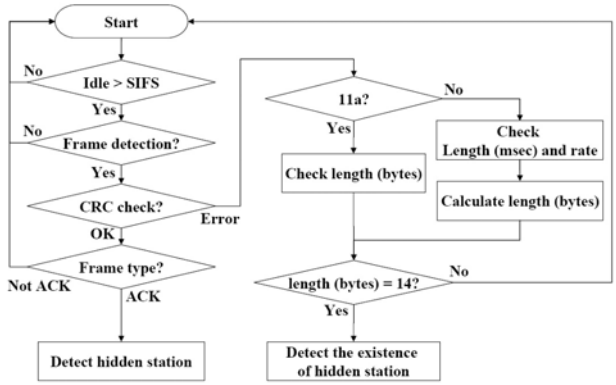

Fig. 4. Hidden station detection process.

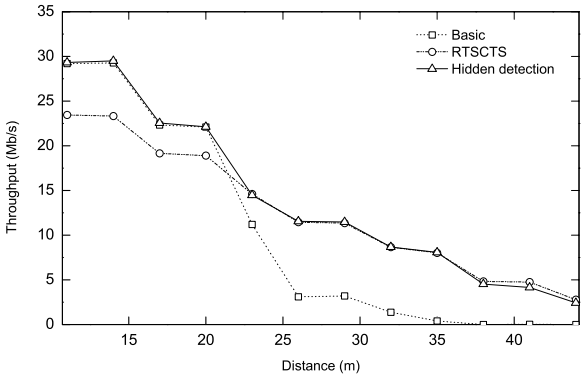

Fig. 5. Performance of the hidden station detection scheme.

References

[1] IEEE Std 802.11, *International Standard [for] Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, IEEE 802.11-1999, 1999.

[2] IEEE Std 802.11a, *Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band*, IEEE Std. 802.11a-1999, 1999.

[3] IEEE Std 802.11b, *Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer Extension in the 2.4 GHz Band*, IEEE Std. 802.11b-1999, 1999

[4] IEEE Std 802.11g, *Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher Data Rate Extension in the 2.4 GHz Band*, IEEE Std. 802.11g-2003, 2003

[5] S. Khurana, A. Kahol, and A. P. Jayasumana, "Effect of hidden terminals on the performance of IEEE 802.11 MAC protocol," in *Proc. IEEE Conference on Local Computer Networks (LCN'98)*, October 11–14, 1998.

[6] The Network Simulator ns-2, http://www.isi.edu/nsnam/ns/, online link.