Enhanced Protection Mechanism for Wireless LAN to Reduce Protocol Overhead

1 Dr. S. Bhargavi
Professor, Dept.of ECE
SJCIT, Chickballapur
E-mail: bhargavisunil@gmail.com

2 Chandra Naik G
Asst. Professor, Dept.CS & E
AIT Chickmagalur
chandru2468@gmail.com

Abstract—The Wireless LANs (WLAN) have become more popular and commonly used these days. WLAN links many devices using some wireless methods like OFDM, Spread Spectrum etc. There are several IEEE Standards exists for Wireless LAN, among them IEEE 802.11b and IEEE 802.11g are most popular types of IEEE 802.11. These two standards are “Wi-Fi” certified and operate at 2.4GHz band. The 802.11g supports higher data rate i.e. up to 54Mbps when compared to 11Mbps of 802.11b. In this work, we mainly focused on analysis of 802.11 Standards and implementing the enhanced protection mechanism for improving Co-existence of IEEE 802.11b and IEEE 802.11g Wireless LANs. The enhanced protection mechanism grants higher priority to 802.11g devices by enlisting duration field of CTS-to-self frame and reducing number of extra generated CTS-to-self frames. Our simulation results shows that proposed scheme improves the performance by reducing the number of extra frames used for channel reservation while utilizing both IEEE 802.11b and 802.11g devices in the mixed environment. The effectiveness of our proposed solution to improve system performance in the mixed 802.11b and 802.11g WLAN is verified by simulation.

Keywords: WLAN, OFDM, IEEE 802.11, enhanced protection

I. INTRODUCTION

The wireless WLANs (WLANs) are being deployed widely across the enterprise, home, and public environments to facilitate VoIP and other various data services. The widespread deployments of WLANs are underpinned by two most popular variants of IEEE 802.11 standards, 802.11b and 802.11g. IEEE has specified a set of standards as the 802.11 family for WLANs. The IEEE 802.11 specifications define a single medium access control (MAC) layer [1] [2] along with multiple physical layers [1] [3] [4]. Distributed Coordination Function (DCF) is the fundamental MAC technique that employs a CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) distributed algorithm and an optional virtual carrier sense using RTS (Request To Send) and CTS (Clear To Send) control frames. The original IEEE 802.11 standard [1] specifies data rates of 1 Mb/s and 2 Mb/s, and defines direct sequence spread spectrum (DSSS)-based physical layer that operates at the 2.4 GHz ISM band. The original 802.11 was rapidly supplemented by IEEE 802.11b [3], which is specified to support higher data rates up to 11 Mb/s at 2.4 GHz using DSSS with complementary code keying (CCK) modulation. IEEE 802.11g further extends 802.11b to support the data rates up to 54Mb/s at 2.4GHz [4]. The higher data rate in 802.11g is enabled by using OFDM (Orthogonal Frequency Division Multiplexing) modulation as specified in the so-called extended rate physicals (ERPs) physical layers. Along with the gradual deployment of WLANs, the involved WLAN products are delivered under different versions of 802.11 standards. Thus, IEEE 802.11b and IEEE 802.11g devices unavoidably co-exist in certain coverage area. In this mixed networking environment, the legacy 802.11b devices cannot detect the ERP-OFDM signals sent from 802.11g devices; consequently they cannot cause the CCA (Clear Channel Assessment) function within physical layer to indicate the channel busy and refrain from channel access as specified in CSMA/CA. This inability of legacy 802.11b devices leads to frame collisions in the channel access between 802.11b and 802.11g devices. To deal with this issue, the 802.11g defines a protection mechanism based on the channel reservation for the ERP-OFDM transmissions. To ensure that the reserved channel status is understandable by the mixed devices, extra frames are introduced in the protection mechanism. Those frames have to be sent with NonERP modulation at a low rate (typically 2 Mb/s) for them to be understood by all stations. One option of extra frames is the RTS/CTS frames which are originally designed to reduce frame collisions caused by hidden terminals. Any device (other than sender and intended receiver) receiving the RTS or CTS frames should refrain from sending data by setting its network allocation vector (NAV) for a given time period indicated in the Duration field of RTS and CTS frames. The other option of extra frames is CTS-to- self frames whose source address and destination address are identical. The 802.11g sender...
transmits a CTS-to-self frame to inform all the neighboring 802.11g and 802.11b devices to update NAV according to the Duration field of the CTS-to-self frame. Obviously, extra frames (RTS, CTS, and CTS-to-self) used for ensuring interoperability are viewed as overhead for system performance because they reduce the available medium resource for data delivery.

Specifically, when voice traffic is provisioned over homo- geneous 802.11 WLANs (802.11b only WLAN or 802.11g only WLAN), exchange of RTS and CTS frames is typically turned off because a VoIP packet size (200 bytes in G.711) is usually less than a pre-defined triggering threshold (maximum is 2347). In the mixed 802.11b and 802.11g WLAN, either exchange of RTS/CTS frames or sending CTS-to-self frames needs to be initiated for performing the protection mecha- nism. CTS-to-self protection mechanism is more efficient than RTS/CTS protection mechanism in clear channel conditions (no hidden terminals). Usually, there are few hidden termi- nals in the indoor voice over WLAN (VoWLAN) services; hence CTS-to-self protection mechanism is typically utilized. Nevertheless, the voice performance degrades significantly in the mixed 802.11b and 802.11g WLAN with either protection mechanism. Compared to the 802.11g only WLAN, it is reported in [6] that the voice capacity in the mixed WLAN drops more than 70% and 50% with RTS/CTS protection mechanism and CTS-to-self protection mechanism, respec- tively. Therefore, our work in this paper focuses on improving voice performance in the mixed 802.11b and 802.11g WLAN by reducing the overhead frames used for channel reservation. We propose an enhanced protection mechanism to reduce the number of transmitted CTS-to-self frames and achieve improved voice performance in terms of capacity and packet loss rate.

The remainder of the paper is organized as follows. Section II describes the related work about the overhead reduction for coexistence of 802.11b and 802.11g WLAN. In Section III, we present the enhanced protection mechanism. The effectiveness of our proposed solution is shown in Section IV by simulation. Finally, conclusions are given in Section V.

II. RELATED WORK

It has been pointed out in [7] that using NonERP RTS/CTS exchange is a costly solution to protect the ERP-OFDM transmissions, and a solution called 802.11g CP is proposed to avoid NonERP RTS/CTS exchange. [7] Reviews that an 802.11 superframe is composed of a contention-free period (CFP) for PCF (point coordination function) and a contention period (CP) for DCF. During CFP, the stations do not contend for the channel as their NAV is set to a pre-defined value, CF Max Duration. A CFP ends when the AP (Access Point) transmits a CF-End frame, which should be transmitted at NonERP rate for it to be understood by all the stations in the mixed 802.11b and 802.11g network.[7] realizes that reception of CF-End frame is supported by all 802.11 stations (STAs) though PCF is optional. The proposal in [7] is to transmit the CF-End frame modulated with an ERP modulation so that only 802.11g stations can understand this ERP CF-End. In this situation, only 802.11g stations reset NAV and start contention after receiving ERP CF-end while 802.11b stations wait until the original NAV expires at the end of the CF Max Duration. Therefore, the period of 802.11g CP is from the end of the ERP CF-End frame to the expiration of the original NAV in 802.11b stations, and it is only used for contention by the 802.11g stations. During the 802.11g CP, the 802.11g stations do not need to use NonERP RTS/CTS exchange since they are safe from the 802.11b stations’ contention. Thus the overhead caused by the protection mechanism is reduced so that the throughput of WLAN increases.

Another approach for overhead reduction in WLAN is frame- bursting supported by 802.11e [2] [8]. It enhances the ability of a station to upload data at faster speeds by using SIFS (Short Interframe Space) to “burst” a sequence of up to three frames before waiting the required period, longer DIFS (Distributed Interframe Space). This allows more data to be sent and less waiting to occur.

The proposal of 802.11g CP in [7] only works for infrastruc- ture BSS (Basic Service Set), where an AP is used to announce the ERP CF-end in the beacon. Frame- bursting only allows a single station to seize the channel and send a sequence of frames. Therefore, it is not suitable for VoWLAN where VoIP frames arrive in a fixed long interval (20ms in G.711). In this paper, we propose a solution that can work for multiple stations in both infrastructure BSS and independent (ad hoc) BSS.

III. ENHANCED PROTECTION MECHANISM

The purpose of our solution is to improve system performance by reducing the number of CTS-to-self frames generated by the 802.11g devices. In our solution, the enhance- ments are introduced into the 802.11g devices only, while the 802.11b keeps unchanged. We first present the two principles for the enhancements, then we describe the processes to implement the principles in 802.11g devices. We further clarify our solution by giving an illustration. Moreover, we describe how to extent our solution to RTS/CTS protection mechanism, and to IEEE
A. **Principles for enhancements**

The first principle is that channel is reserved for 802.11g devices to transmit multiple VoIP frames aided by just one CTS-to-self frame. This principle is achieved by set-ting the **Duration** field of CTS-to-self frame to **protection duration**, which is larger than **ori_duration**. Here **ori_duration** denotes the original duration for a single voice frame transmission (including exchange of data and ACK frame) at faster ERP rate. Once an 802.11b STA receives a CTS-to-self frame, it sets its NAV as **protection duration**. On the other hand, an 802.11g STA knows this principle and does not update its NAV when receiving such a CTS-to-self frame. Hence, only 802.11b STAs are prohibited to medium access during the period of **protection duration**.

One option scheme to set the value of **protection duration** can be given by

\[
\text{protection duration} = N_g \times (\text{ori_duration} + \text{ave backoff}) \tag{1}
\]

where \( N_g \) is the number of 802.11g STAs with the voice traffic, and \( \text{ave backoff} \) is the average backoff duration of 802.11g STAs, which is expressed as:

\[
\text{ave backoff} = CW_{\text{min}} + CW_{\text{max}} / 2 \times \text{Slot} \tag{2}
\]

where \( CW_{\text{min}} \) and \( CW_{\text{max}} \) are the minimum and maximum contention window, respectively; \( \text{Slot} \) is the slot time in WLAN. The value of \( N_g \) can be obtained by AP and then indicated to the 802.11g devices via beacon indication; \( N_g \) can also be obtained directly by an 802.11g device itself via overhearing the voice frames from other 802.11g devices. It is noticeable that **protection duration** in (1) can be adjusted dynamically depending on the number of 802.11g VoIP STAs in the mixed WLAN. Therefore, with the setting of **protection duration** using (1), each STA of \( N_g \) 802.11g STAs can transmit one VoIP frame; the 802.11b STAs defer medium access until protection duration expires.

The second principle is that an 802.11g device does not send a CTS-to-self frame again during the period of channel reserva-tion. This principle is achieved by maintaining a dedicated counter in each 802.11g device to count down the value of **Duration** field of a CTS-to-self frame. The counter is called **CDC** (CTS-to-self Duration Counter) to prevent the 802.11g devices unnecessarily transmitting the CTS-to-self frames during the period of **protection duration**.

After an 802.11g STA transmits a CTS-to-self frame, it activates **CDC** with an initial value **ini_counter** as

\[
\text{ini}\_\text{counter} = \text{protection duration} \tag{2}
\]

Once other 802.11g STAs overhear the CTS-to-self frame with the NonERP modulation, the value of **CDC** is updated as

\[
\text{new}\_\text{counter} = \text{max}(\text{overheard duration, cur}\_\text{counter}) \tag{3}
\]

Where new counter is the updated value of **CDC**, **over-heard duration** is the value of **Duration** field in the overheard CTS-to-self frame, and cur counter is the current value of **CDC**. With these two principles, multiple 802.11g STAs can seize the channel and send a sequence of VoIP frames one by one. Hence, our solution can be viewed as a “distributed frame bursting” technique.

B. **Implementation Processes**

To implement the designed principles, the process of frame sending and the process of frame receiving at an 802.11g device are given in Fig. 1 and Fig. 2, respectively. As shown in Fig. 1, when an 802.11g device has data to be transmitted, it first checks the current value of **CDC**, **cur_counter**, to see whether it is larger than the duration required for a data frame transmission (denoted as required duration). If cur counter is greater than required duration, the data frame can be transmitted directly without initiating the protection by sending a CTS-to-self frame. Otherwise, the 802.11g device has to send a CTS-to-self frame whose **Duration** field is set to be **protection duration**, and the 802.11g device activates **CDC** with an initial value as **protection duration**.

As shown in Fig. 2, once overhearing a frame, the 802.11g device checks whether it is a CTS-to-self frame or not. If the received frame is a data frame (not a CTS-to-self frame), the 802.11g device sets its NAV to be the value specified in the **Duration** field of the received frame. If the received frame is a CTS-to-self frame, the 802.11g device updates its **CDC** using (3), but it omits updating its NAV.

C. **Illustration**

To further clarify the proposed solution, an illustration is given in Fig. 3. In this figure, the STA A and STA B are 802.11g devices, while STA C is an 802.11b device.
from protection mechanism can be significantly reduced, the throughput of 802.11b devices is likely to increase as well since more medium resource is released for data delivery. The value of protection duration plays a tradeoff for channel access between 802.11g and 802.11b devices. For instance, smaller value of protection duration can be used to allocate less airtime for 802.11g devices by using \( n (n < N_g) \) instead of \( N_g \) in (1).

E. Extension to RTS/CTS protection mechanism

The principles to enhance CTS-to-self protection mechanism can also be utilized in the RTS/CTS protection mechanism. When the 802.11g devices want to transmit data frames, they perform the process as given in Fig. 1 to determine whether to send an NonERP RTS frame. The 802.11g devices can find that the protection mechanism is initiated when they receive the NonERP RTS frame, and then they send back an NonERP CTS frame whose Duration field is set using (1). Similarly, the 802.11g devices perform the same process as given in Fig. 2 when they overhear the NonERP CTS frame.

F. Extension to 802.11n

The 802.11n WLAN [5] is under specification to support 300 Mb/s or higher data rate. Our solution can be extended to improve the performance of 802.11n WLAN when legacy devices such as 802.11b and 802.11g devices co-exist. The 802.11n devices can still use the CTS-to-self protection mechanism to allow the legacy devices to correctly determine whether to perform medium access. The CTS-to-self frame must be transmitted using one of the legacy data rates that a legacy device can receive and decode. Thus, the overhead of sending CTS-to-self frames by 802.11n devices also lowers the effective throughput in the mixed networking environments. Our solution can be utilized to reduce the overhead caused by the CTS-to-self protection mechanism in 802.11n after making simple modification. The 802.11n devices utilize two adjacent 20MHz channels to build a 40MHz bonded channel for data delivery. We can just perform the proposed solution separately over each 20MHz channel. Once an 802.11n device determine that the protection mechanism needs to be invoked at any of the 20MHz channels (i.e., logic OR operation), the device sends the CTS-to-self frame first and activates CDC before transmitting the data frames.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the proposed solution by simulation in the mixed 802.11b and 802.11g WLAN. The simulation scenario is shown in Fig. 4.
In the simulation scenario, the 802.11g STAs are used only for VoIP service and the 802.11b STAs are used only for non-real-time data traffic delivery. Normally, most of the 802.11b STAs work as the data terminals such as laptop and PDA, while the current voice terminals operate mainly in 802.11g for the benefit of higher capacity. Therefore, the simulation scenario considered here is a typical realistic system and the corresponding simulation results can reflect the effectiveness of our solution in the practical environment.

The simulation parameters about the network configuration and traffic model are given in Table I. The voice session is assumed to be bi-directional and the best-effort data traffic is uni-direction. A VoIP packet is dropped when it exceeds the delay bound (200ms) or reaches the maximum retry count. PLR (Packet Loss Rate) for the VoIP service is the criterion to evaluate the voice capacity (maximum allowable number of VoIP STAs). In our simulation, the maximum acceptable PLR is 3% for VoIP services.

### TABLE I

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data rate</td>
<td>802.11g: 54Mbps, 802.11b: 11Mbps</td>
</tr>
<tr>
<td>Control data rate</td>
<td>2Mbps</td>
</tr>
<tr>
<td>Slot time</td>
<td>24μs</td>
</tr>
<tr>
<td>SIFS</td>
<td>11μs</td>
</tr>
<tr>
<td>Frame length</td>
<td>802.11g: 20μs, 802.11b: 192μs</td>
</tr>
<tr>
<td>Retry Count</td>
<td>4</td>
</tr>
<tr>
<td>CW size</td>
<td>Voice Traffic: CW_{min} = 7, CW_{max} = 83, Data Traffic: CW_{min} = 31, CW_{max} = 1023</td>
</tr>
</tbody>
</table>

The PLRs of downlink and uplink with different number of 802.11g VoIP STAs are illustrated in Fig. 5 and Fig. 6, respectively. It is observed that PLR increases sharply with the increasing number of VoIP STAs in the WLAN when using traditional 802.11g standard. With the proposed solution, PLR does not increase very much even if there are many co-existing 802.11b data STAs. Specifically, the proposed mechanism reduces PLR over downlink and uplink by 80% and 37%, respectively as there are $N_g = 29$ 802.11g VoIP STAs co-existing with $N_b = 12$ 802.11b data STAs in the network, where $N_b$ and $N_g$ denote the number of 802.11b and 802.11g STAs, respectively. Under the requirement that the PLR should be less than 3%, voice capacity in WLAN can be determined accordingly. It can be observed that the proposed solution can result in more obvious improvement in terms of voice capacity. Actually, voice capacity improves almost 100% (from 15 to 29).

On the other hand, the data throughput of 802.11b STAs is shown in Fig. 7. It is found that the throughput achieved with the proposed solution is higher than that of 802.11 standards by 300% in the case that $N_g = 12$ and $N_b = 13$. With increase of $N_g$, the throughput of 802.11b devices decrease since 802.11b STAs is deferred more on account of the increase of protection duration introduced by more 802.11g devices.
V. CONCLUSION

This paper presents an enhanced protection mechanism to reduce the protocol overhead in the mixed 802.11b and 802.11g WLAN environment. The enhanced mechanism grants higher priority to the 802.11g devices by enlarging the duration field of CTS-to-self frame and reducing the number of generated CTS-to-self frames. The proposed mechanism can improve system performance of VoWLAN significantly in terms of packet loss rate and voice capacity. The proposed solution only requires modifications on the 802.11g devices. Therefore, it is believed that the mechanism presented in the paper has backward compatibility with legacy 802.11b devices. Finally, the proposed solution can also be employed for improving co-existence between 802.11n with other 802.11 variants.

REFERENCES


AUTHORS PROFILE

Dr. S. Bhargavi is presently working as a Professor in the department of Electronics and Communication engineering, SICIT, Chikballapur, Karnataka, India. She is having 13 years of teaching experience. Her areas of interest are Communication systems, Network security, Robotics, Embedded Systems, Low Power VLSI, Wireless communication, ASIC and Cryptography.

Chandra Naik G is presently working as an Assistant Professor in the department of CS&E, AIT, Chickmagalur, Karnataka, India. He is having 2 years of teaching experience. His areas of interest are Digital Communication, Cryptography, Network security, Networking.