

CSMA/CCA: A Modified CSMA/CA Protocol Mitigating the Fairness Problem for IEEE 802.11 DCF

Xin Wang and Georgios B. Giannakis

Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN 55455, USA

Received 15 August 2005; Revised 23 November 2005; Accepted 22 December 2005

Carrier sense multiple access with collision avoidance (CSMA/CA) has been adopted by the IEEE 802.11 standards for wireless local area networks (WLANs). Using a distributed coordination function (DCF), the CSMA/CA protocol reduces collisions and improves the overall throughput. To mitigate fairness issues arising with CSMA/CA, we develop a modified version that we term CSMA with copying collision avoidance (CSMA/CCA). A station in CSMA/CCA contends for the shared wireless medium by employing a binary exponential backoff similar to CSMA/CA. Different from CSMA/CA, CSMA/CCA copies the contention window (CW) size piggybacked in the MAC header of an overheard data frame within its basic service set (BSS) and updates its backoff counter according to the new CW size. Simulations carried out in several WLAN configurations illustrate that CSMA/CCA improves fairness relative to CSMA/CA and offers considerable advantages for deployment in the 802.11-standard-based WLANs.

Copyright © 2006 X. Wang and G. B. Giannakis. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. INTRODUCTION

The medium access control (MAC) protocol is the main element determining how efficiently the limited communication bandwidth of the underlying wireless channel is shared in a wireless local area network (WLAN). It is crucial that the MAC protocol provides robustness and fairness among users. The IEEE 802.11 standards [5–7] are the first international standards for WLANs, providing general MAC layer and physical (PHY) layer specifications. At the MAC layer, IEEE 802.11 specifies a basic distributed coordination function (DCF) and an optional point coordination function (PCF). Our work in this paper pertains to the DCF, which is a contention-based *decentralized* protocol utilizing the so-called carrier sense multiple access with collision avoidance (CSMA/CA). The latter constitutes the basic access mechanism for supporting asynchronous data transfer. At a high-level description, the CSMA/CA for DCF consists of two parts: the CSMA scheme [2] and the CA scheme, relying on a binary exponential backoff (BEB) algorithm [2]. In the DCF, collisions of MAC frames are avoided and/or resolved by jointly utilizing the CSMA scheme and the BEB algorithm. The analytical and simulation results in [8, 9] confirm that CSMA/CA endows the IEEE 802.11 WLANs with fairly good saturation throughput. In the long term, the DCF basically provides the contending stations

equal opportunities to access the shared channel. However, with a nonfully connected wireless network topology, the IEEE 802.11 CSMA/CA protocol has to deal with the *fairness problem* whereby stations cannot gain access to the wireless medium equally during heavy traffic conditions [10]. Moreover, since contending stations do not always have a frame to transmit, they experience unfairness [12]. The fairness problem may seriously affect the *quality of service (QoS)* support for WLAN. The desirable QoS of some users may not be satisfied due to unfair access opportunities. Modifications to the existing IEEE 802.11 MAC protocols have been proposed [10–18], most aiming to modify the BEB algorithm.

It is well known that the fairness problem within the IEEE 802.11 WLANs comes behind the fact that each station must rely on its own direct experience in estimating congestion, which often leads to asymmetric views. All schemes in [10–15] are designed to counter the possibly wrong direct experience of congestion estimates. However, in the designs of [10–15], the *hidden-station problem* [2, Section 4.2.6], which is one of the main sources of erroneous direct experience estimates, was seldom investigated. Based on the multiple access with collision avoidance (MACA) protocol [3], Bharghavan et al. introduced the so-termed MACAW protocol [4], which accounts for the hidden-station problem. The idea in MACAW amounts to a simple yet efficient “backoff copying” from overheard packets, through which learning

about network congestion levels becomes a collective practice. Further congestion information exchange and backoff schemes improved the fairness of the original MACA protocol considerably.

The objective of this paper (in par with the goals of most prior works) is to develop a MAC protocol capable of mitigating the fairness problem at low cost and without having to make major modifications to existing hardware. By mitigating the fairness problem, CSMA/CCA facilitates QoS provisioning regardless of the underlying network topology. Inspired by the backoff copying in [4], our simple plan is to apply the contention window (CW) size copying among stations. We call the resulting protocol CSMA with *copying* collision avoidance (CSMA/CCA), since it is rooted in the original CSMA/CA protocol. Stations in CSMA/CCA contend for the channel similarly as in the CSMA/CA protocol. However, after winning the contention, a station piggybacks its CW size in its data frame. Deferring stations in the same basic service set copy the CW size in the overheard data frame. By this CW size copying, we expect that the stations can contend for the channel with similar CW sizes, thereby accessing the channel statistically equally. The main contribution of this paper is a practical MAC protocol, which is also different from the prior work in the following: (1) it is specifically tailored for IEEE 802.11 DCF; (2) unlike the continuous-value backoff copying, CW size copying incurs only 3 bits overhead which can be easily absorbed by the current standards; (3) while GDCF [13] implements the gentle CW decrease based on the individual station's contention history, our gentle CW size decrease algorithm takes into account the overall channel traffic; and (4) by the CW size reset function, we mitigate the *shadowed-receiver problem* which remains unresolved in MACAW [4].

The paper is organized as follows. In Section 2, the IEEE 802.11 DCF based on the CSMA/CA protocol is briefly outlined. Design of the proposed CSMA/CCA protocol is presented in Section 3. Then, in Section 4, computer simulations are carried out to evaluate the performance of CSMA/CCA. Section 5 gives the conclusions of this paper.

2. IEEE 802.11 DCF BASED ON THE CSMA/CA PROTOCOL

Figure 1 depicts an example configuration covered by IEEE 802.11 standards [5, 6], where a set of stations controlled by a single coordination function (such as a DCF) is defined as a basic service set (BSS). There are two kinds of BSSs: independent BSS (IBSS) and infrastructure BSS, the difference being that there is an access point (AP) in infrastructure BSS whereas no AP is available in IBSS. Both BSSs in Figure 1 are infrastructure ones. The members (stations or APs) of a BSS, for example, STA3 (hereafter, STA n denotes station n) and STA4 in BSS1, can directly communicate with each other, but two stations in different BSSs can only communicate through their APs and the distribution system (DS); for example, data from STA3 to STA5 has to go through STA3-AP1-AP2-STA5. Clearly, since there is no AP in IBSS, stations in one IBSS cannot communicate with stations in other BSSs. There is a

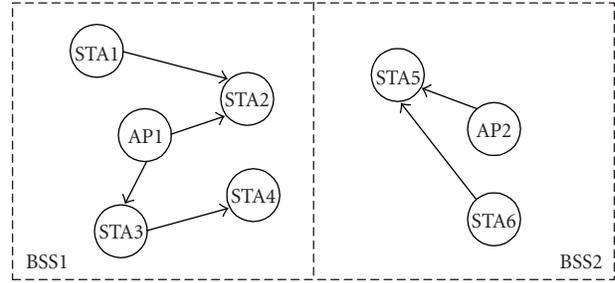


FIGURE 1: An example configuration of the IEEE 802.11 WLAN.

unique BSS identification (BSSID) which is the MAC address in use by the AP of the BSS. In the WLAN, a link is referred to as a directional data stream between two stations. The direction of the link is determined by the data frame transmission; for example, link STA3-STA4 in Figure 1 indicates that STA3 is the initial station and intends to transmit a data frame to STA4. It is the initial station of a link who contends for the link. In an infrastructure BSS, a normal station has one transmit buffer and can only initiate one link at a time. The AP may initiate more than one link. When the AP is the initial station of more than one link, it contends for these links separately. In this case, the AP is viewed as several different initial stations at the MAC layer by default; for example, AP1 in Figure 1 is viewed as two different initial stations by the MAC protocol when it contends for links AP1-STA2 and AP1-STA3 separately. Since all the members of a WLAN share the same wireless channel, a MAC protocol is needed to coordinate their access.

At the MAC layer, the IEEE 802.11 specifies a basic DCF based on the CSMA/CA protocol. For DCF operations, IEEE 802.11 defines certain interframe space (IFS) intervals between successive transmissions of MAC frames. The two relevant intervals are short IFS (SIFS) and DCF-IFS (DIFS). The SIFS is smaller and used for high-priority frames such as ACK (acknowledgment) frames and CTS frames; whereas the DIFS is larger and used for normal data frames in DCF operation.

In the CSMA/CA protocol, an initial station with a MAC frame to transmit has to sense the channel. If the channel is idle for a DIFS period, the station can proceed with its transmission. Otherwise, the station defers and continues monitoring the channel until an idle DIFS is detected. Then a random backoff counter is generated by the station before sending. The backoff counter runs down as long as the channel remains idle; it pauses when the channel becomes busy; and it resumes as the channel is idle for a DIFS period again. The station is permitted to transmit when its backoff counter reaches zero. For implementation efficiency purposes, the backoff counter employed by DCF is discrete-time scaled. The time immediately following an idle DIFS is slotted and the random backoff counter counts down one after a slot.

The CSMA/CA protocol relies on the BEB algorithm to control the CW size of each initial station and thereby resolve collisions. In a WLAN, each initial station has a CW

size w which has minimum value CW_{\min} and maximum value CW_{\max} . Before each transmission, the initial value of the backoff counter is uniformly chosen by the initial station in the range $[0, w - 1]$. At the first attempt of a data frame, w is set to CW_{\min} . After each failed transmission, it doubles w until the latter reaches CW_{\max} . After each successful data frame transmission, w is reset to CW_{\min} since it begins the first attempt of another data frame.

With the CSMA/CA protocol in use, the DCF provides both a DATA-ACK two-way handshaking basic access mechanism and an RTS-CTS-DATA-ACK four-way handshaking access mechanism (called RTS/CTS access mechanism hereinafter). In the basic access mechanism, the CSMA/CA protocol is applied to the DATA/ACK exchange. A good illustration for the implementation of the basic access mechanism of DCF can be found in [1, Chapter 11]. The difference between the RTS/CTS access mechanism and the basic access mechanism is the addition of the RTS/CTS exchange for reservation purposes before DATA/ACK transmissions. The CSMA/CA protocol is applied to the short RTS/CTS exchange and DATA/ACK transmissions are carried out contention-free. This mechanism is effective for system performance when the average length of data frames is large compared to that of the RTS and CTS frames. Besides reservation, the purpose of RTS and CTS frames is to carry the duration of the following DATA/ACK exchange. Based on this information, all other stations in the WLAN are then able to update their network allocation vectors (NAVs), which indicate how long the channel will remain busy. For the RTS/CTS access mechanism, IEEE 802.11 standards define virtual carrier sensing based on the NAV signal. An initial station is able to proceed with its transmission only if the channel is sensed idle both physically and virtually. Virtual carrier sensing is designed to combat the hidden-station problem for radio channels.

3. DESIGN OF THE CSMA/CCA PROTOCOL

The proposed CSMA/CCA protocol operates under two assumptions: (1) RTS/CTS access mechanism is active (even though the proposed CSMA/CCA can be applied also to the basic access mechanism, RTS/CTS access mechanism is incorporated for better addressing the fairness issue related to the hidden-station problem); and (2) all the links in the WLAN have identical priorities. Although the newly proposed IEEE 802.11e standard [7] defines a MAC enhancement for QoS traffic and some recent efforts were made to provide fairness in QoS [19, 20], we do not deal with QoS-enabled MAC architectures, where links could have different priorities.

Based on the fact that the CW size represents the contending priority and the stations could contend fairly with similar CW sizes, our CSMA/CCA protocol aims to mitigate the fairness problem. The main difference between the proposed CSMA/CCA and the existing CSMA/CA protocol is the addition of the CW size copying, which we invoke to handle the inherent fairness problem. In our novel CCA scheme, we define CW size copying routines and propose a

gentle BEB equipped with reset (GBEBwR) algorithm modified from the BEB algorithm to control the CW size of each initial station. The detailed design of the CW size copying routines and the GBEBwR algorithm are presented next.

3.1. CW size copying routines

The CW size copying routines include a piggyback routine, a copy routine, and an update routine. In our CSMA/CCA protocol, initial stations contend for the channel with a backoff-before-transmit process, as in the CSMA/CA protocol. However, after winning the contention, that is, after a successful RTS/CTS exchange, a station executes a piggyback routine to piggyback its CW size in its data frame. Then the deferring stations copy the CW size in the overheard data frame with a copy routine. After CW size copying, the deferring stations also execute a routine to update their current backoff counters according to the new CW size.

Piggyback routine

In IEEE 802.11 standards [5–7], the CW size w can only take the values of $2^l CW_{\min}$, $l = 0, 1, \dots, L - 1$, in the range $[CW_{\min}, CW_{\max}]$, where CW_{\min} , CW_{\max} , and the number of CW size levels L are PHY-specific. To carry the CW size copying, we only need to piggyback the corresponding CW size level in a frame. For various IEEE 802.11 PHY layer specifications, it turns out that at most 7 levels of CW size, carried by 3 bits, are required. Since the CW size information is used for MAC operation, we piggyback it in the MAC header of certain frames. The general IEEE 802.11 MAC frame format comprises a set of fields in a fixed order in all frames, as depicted in Figure 2. Each MAC frame consists of a MAC header, a frame body, and a frame check sequence (FCS). Note that CW size copying is effective only when there exists a successful transmission. For the RTS/CTS access mechanism, a data frame is always transmitted under the contention-free situation with high probability of success. For this reason, we plug the CW size level in the MAC header of a data frame. For instance in IEEE 802.11a, b, as shown in Figure 2, the frame control field in the MAC header consists of a number of subfields, among which the type and subtype fields together identify the function of the frame. The type value of a data frame is defined as 10 and the subtype values 1000–1111 for the data frame are reserved in IEEE 802.11. These reserved subtype values can provide the required 3 bits to carry the CW size level. In a nutshell, our piggyback routine proceeds as follows: after winning the contention, a station piggybacks its CW size level in the data frame MAC header with the subtypes 1000–1111, where the first bit indicates the piggyback in a normal data frame, and the remaining three bits specify the CW size level. Note that some reserved subtype values 1000–1111 are already used in 802.11e for QoS support [7]. However, the new 802.11e MAC frame format adds to the MAC header two bytes of QoS control field, where some reserved bits can be used for the piggyback routine as well.

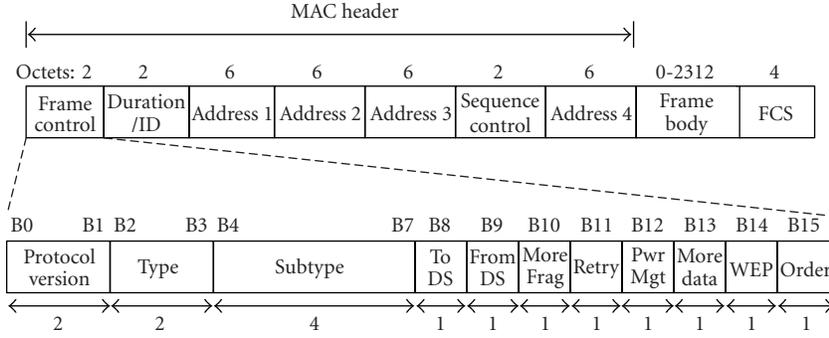


FIGURE 2: MAC frame format.

TABLE 1: Address field contents.

ToDS	FromDS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Copy routine

In the MACAW protocol [4], it is suggested that the backoff copying should be allowed only among the pads in the same cell. In the proposed CSMA/CCA protocol with stations and BSS playing the roles of pads and cell, we follow similar steps and copy the CW size without leakage across the BSSs by utilizing the BSSIDs. The frame format for a data frame is shown in Figure 2. The content of the address fields depends on the values of the ToDS and FromDS bits (which indicate if the frame goes to or comes from another BSS, with a “1” indicating “true”) in frame control field, as defined in Table 1. If the content is shown as N/A, the field is omitted. The DA and SA denote the destination and sender addresses, respectively. The RA and TA are only used in a data frame transmission between two APs (in the situation that both ToDS and FromDS are equal to 1), and denote the addresses of receiving and transmitting AP, respectively. Note that RA and TA are two BSSIDs for the BSSs to which the two APs belong. To prevent leakage across the BSSs, we design a copy routine as follows: upon hearing a data frame, a deferring station copies the CW size only if the overheard data frame carries a BSSID, RA or TA matches the station’s BSSID, and the piggybacked CW size level is different from the station’s CW size.

Update routine

Along with CW size copying, the deferring stations also need to update their backoff counter values. Through the update, the backoff counter of a deferring station pretends to be generated according to the new CW size. To this end, we design an update routine as follows: let w_n , w_o denote the new and old CW sizes of a deferring station before and after CW size copying, respectively; and define a CW size changing factor

$f_c = w_n/w_o$. Then a deferring station updates the new backoff counter value c_n from the old value c_o using

$$c_n = \begin{cases} c_o f_c + \lfloor f_c x_{\text{rnd}} \rfloor & \text{if } f_c > 1, \\ \lfloor c_o f_c \rfloor & \text{if } f_c < 1, \end{cases} \quad (1)$$

where x_{rnd} denotes a random real number uniformly distributed in $[0, 1)$, and $\lfloor a \rfloor$ denotes the integer part of a positive real number a . Note that f_c is an integer when it is greater than 1. When the CW size increases by a factor f_c , we add $\lfloor f_c x_{\text{rnd}} \rfloor$ to $c_o f_c$ so that the future collision probability is reduced; and thus stations with the same c_o may no longer collide in the future. Accordingly, when the CW size decreases, we simply use $\lfloor c_o f_c \rfloor$ as the new counter value. In this way, the backoff counter update (1) saves the contention histories of the deferring stations, as in the CSMA/CA protocol.

3.2. GBEBwR algorithm

The GBEBwR algorithm is used to control the CW size of an initial station in the proposed CSMA/CCA protocol. In the GBEBwR, a station does not reset its CW size to the minimum after only one successful transmission as in the BEB algorithm. Instead, we use a gentle CW size decrease algorithm, where a station halves its CW size after hearing no less than c consecutive successful transmissions in its BSS. Although independently designed, this gentle CW size decrease is very similar to the GDCE scheme in [13]. In GBEBwR, when a station’s access attempt fails, the station doubles its CW size until reaching a maximum value as in the BEB algorithm. However, to cope with the *shadowed-receiver problem*, we design a CW size reset function where a station resets its CW size to the minimum value, instead of doubling it as in GDCE, when it experiences r consecutive failed access attempts.

Gentle CW size decrease algorithm

In the CSMA/CA protocol, the CW size w of the initial station is reset to CW_{min} upon a success. If we adopt this rapid decrease scheme in the proposed CSMA/CCA and let it affect the CW size copying, after every successful transmission we return to the case where all initial stations within a certain

range have a minimal CW size. Then we repeat a period of contention to increase the CW size until a successful access attempt happens. To avoid this wild oscillation, a multiplicative increase and linear decrease (MILD) algorithm is used in the MACAW protocol [4] to control the adjustment of backoff intervals. With the MILD algorithm, the backoff interval of a station is increased upon a collision by a multiplicative factor (1.5) and is decreased by 1 upon success. Clearly, the MILD algorithm cannot be applied to our CW size adjustment since the CW size can only take limited values. To facilitate our CW size copying, we design a gentle CW size decrease algorithm, which is similar to the GDCF scheme in [13] but is based on the overall channel traffic instead of individual station's contention history. We let each initial station have an integer success counter n_s with initial value 0. The counter n_s is updated in several ways. Whenever an initial station finishes a successful RTS/CTS exchange, it increases its n_s by 1, that is, $n_s = n_s + 1$; and whenever it has a failed RTS/CTS exchange, it resets its n_s to 0. Whenever an initial station hears a data frame with a matched BSSID, if the overheard frame carries the same CW size as its current one, it sets its $n_s = n_s + 1$; otherwise it sets its $n_s = 1$. Before sending its data frame after winning the contention, the station compares its n_s with a prescribed decrease threshold d , which is a design parameter. If $n_s \geq d$, as resetting $n_s = 0$, the station halves its current CW size and piggybacks the new CW size level in the data frame MAC header. Otherwise, the station does not adjust its CW size and piggybacks its current CW size level. This way, the gentle CW size decrease algorithm disallows simultaneous fast decrease of all the initial stations' CW sizes.

CW size reset function

Normally, the double-upon-collision size of the CW used in the BEB algorithm is still adopted by the GBEBwR algorithm. Together with the gentle CW size decrease algorithm, from a single station's point of view, the CW size adjustment becomes a fast-increase-slow-decrease process. This may induce the shadowed-receiver problem, which is illustrated by Figure 3, copied from [8, Figure 7]. In this two-BSS configuration, both STA1 and STA2 are in range of each other but can only hear their respective APs. Consider that links AP1-STA1 and STA2-AP2 are active. In this scenario, the two initial stations AP1 and STA2 may have very different contention experiences. Whenever AP1 is sending a data frame, STA2 would know the duration of the data transmission from the preceding CTS frame sent by STA1. Therefore, it defers and resumes to contend the channel until the AP1-STA1 transmission ends. However, when STA2 is sending, AP1 still senses an idle channel physically and virtually, thereby may access the channel. As AP1 accesses the channel during the STA2-AP2 transmission, STA1 becomes a shadowedreceiver. STA1 may not receive the RTS frame from AP1 and is not allowed to respond since it is in the range of STA2. As a result, the CW size in AP1 could rapidly reach CW_{\max} during the STA2-AP2 transmission. For a fast-increase-slow-decrease algorithm, the situation in Figure 3 always ends up

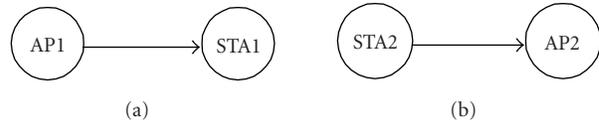


FIGURE 3: A two-BSS configuration where both stations are only in range of their respective APs and also in range of each other: (a) AP1 is sending data to STA1, and (b) STA2 is sending data to AP2. Each link is generating data at 32 frames per second.

with AP1 having a maximum CW size and STA2 having a minimum CW size. Note that this shadowed-receiver problem can also occur within one BSS; for example, replacing AP1 and AP2 with STA3 and STA4 and assuming that all the stations are in the same BSS but STA3 and STA4 cannot hear each other, the same problem arises. The MACAW protocol [4] fails in this shadowed-receiver scenario, since with link STA2-AP2 fully seizing the channel, link AP1-STA1 is prohibited. Without a CW size reset function, our CSMA/CCA protocol does not fail thanks to the good backoff scheme inherited from the CSMA/CA protocol. But STA2 probably seizes the channel much more often than AP1, causing the shadowed-receiver problem because the initial station cannot distinguish between access failure due to collision and access failure due to the shadowed-receiver. Based on the observation that the initial station could probably have consecutive failed accesses in a shadowed-receiver scenario, we design a CW size reset function as follows. We let each initial station have an integer failure counter n_f with initial value 0. Whenever an initial station senses a busy channel due to other stations, or, it finishes a successful RTS/CTS exchange by itself, it resets its n_f to 0. Only after a failed RTS/CTS exchange by itself, it increases its n_f by 1, that is, $n_f = n_f + 1$. Then it compares its n_f with a prescribed reset threshold r , which is another design parameter. If $n_f < r$, it doubles its CW size as normal; otherwise, with $n_f = 0$, the station resets its CW size back to CW_{\min} .

3.3. Operation of CSMA/CCA protocol

Here we summarize the operation of our CSMA/CCA protocol. In CSMA/CCA, each initial station has a CW size w , a backoff counter, a success counter n_s along with a prescribed decrease threshold d , and a failure counter n_f along with a prescribed reset threshold r at the MAC layer. The values of the thresholds d and r will be heuristically determined through simulations.¹ For clarity, consider the finite-state machine of Figure 4 describing the behavior of an initial station. In the proposed CSMA/CCA protocol, an initial station can be in one of six states.

- (1) Waiting: the station has an empty transmit queue and is waiting for the data arrival.

¹ Analytical determination of the optimal d and r , which may be functions of the number of links, goes beyond the scope of this paper and is left for future research.

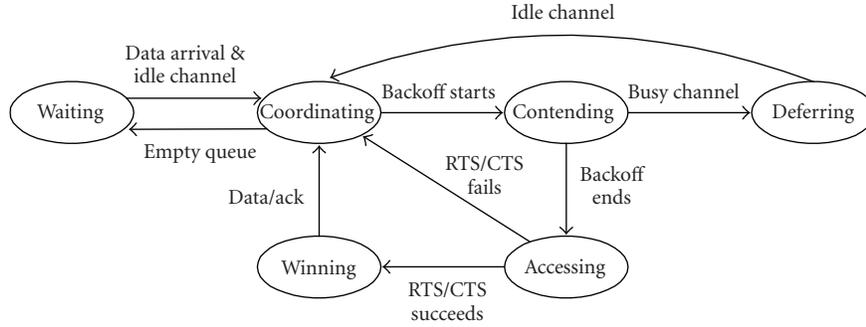


FIGURE 4: A finite-state machine for the behavior of an initial station in the proposed CSMA/CCA protocol.

- (2) Coordinating: the station is coordinating its CW size and backoff counter according to the proposed CCA mechanism.
- (3) Contending: the station is contending the channel by running down its backoff counter.
- (4) Deferring: the station is deferring its contention due to the busy channel.
- (5) Accessing: the station is performing RTS/CTS exchange.
- (6) Winning: the station is performing DATA/ACK exchange.

The coordinating state is in the core of the operation. In this state, the proposed CCA scheme, which is our major contribution, is active to resolve the collision and achieve fairness. An initial station transits between different states and behaves at the MAC layer as follows.

(1) Waiting-coordinating: after data frames arrive and the channel is sensed idle (by the CSMA scheme) for a DIFS period, the station transits from the waiting state to the coordinating state, in which a random integer is uniformly selected from $[0, w - 1]$ as the backoff counter value.

(2) Coordinating-contending: if the transmit queue is non-empty, after the backoff counter value is determined, the station starts or resumes its backoff counter and then transits from the coordinating state to the contending state, in which the backoff counter keeps running down as long as the channel is idle.

(3) Contending-deferring: if the channel is sensed busy before the backoff counter reaching zero, the station transits from contending to deferring, in which it freezes its backoff counter and resets its failure counter $n_f = 0$.

(4) Deferring-coordinating: after the channel is sensed idle for a DIFS period, the station transits from deferring to coordinating. If a data frame is heard successfully while deferring, the station executes the copy routine in the coordinating state to determine if it needs to copy the CW size in the overheard frame. If the overheard data frame has a matched BSSID and carries the same CW size as the station's, the station does not copy and increments its success counter $n_s = n_s + 1$. However, if the overheard data frame with a matched BSSID carries a different CW size, the station copies the CW size and executes the update routine to refresh its current backoff counter value as in (1), while setting

its $n_s = 1$. Corrupted and overheard data frames without a matched BSSID are ignored.

(5) Contending-accessing: upon its backoff counter reaching zero, the station transits from contending to accessing, in which an RTS/CTS exchange is carried out.

(6) Accessing-coordinating: if the RTS/CTS exchange fails, the station transits from accessing to coordinating. In the coordinating state, the station resets its success counter to $n_s = 0$ and sets its failure counter to $n_f = n_f + 1$. Then the station compares its n_f with the reset threshold r . If $n_f < r$, it doubles its CW size w until reaching CW_{max} ; otherwise, as resetting $n_f = 0$, the station resets its CW size $w = CW_{min}$. A random integer is generated according to the new CW size w as the backoff counter value.

(7) Accessing-winning: if the RTS/CTS exchange succeeds, the station transits from accessing to winning. In the winning state, the station resets its failure counter to $n_f = 0$ and sets its success counter to $n_s = n_s + 1$. Then the station compares its n_s with the decrease threshold d . If $n_s \geq d$, as resetting $n_s = 0$, the station halves its CW size w ; otherwise, it keeps w unchanged. Finally, it executes the piggyback routine to piggyback w in the MAC header of the data frame and performs DATA/ACK exchange.

(8) Winning-coordinating: after the DATA/ACK exchange, the station transits from the winning state to the coordinating state. If the DATA/ACK succeeds, the transmitted data frame is removed from the transmit buffer; otherwise, it is still kept for retransmissions. Then if the transmit queue is nonempty, the station generates a random integer as its backoff counter value according to its CW size w .

(9) Coordinating-waiting: if the transmit queue is empty, the station transits from the coordinating state to the waiting state.

4. PERFORMANCE EVALUATION

We use computer simulations to evaluate the performance of the proposed CSMA/CCA protocol and compare it with that of the CSMA/CA protocol in the IEEE 802.11 DCF. In the simulations, we assume a "near-field" radio technology in use in the investigated IEEE 802.11 WLANs, where both capture and interference are rare due to sharp decays in signal strength [4]. All the stations contend for a single wireless

TABLE 2: FHSS system parameters and additional parameters used in the simulations.

Frame payload	8184 bits
MAC header	272 bits
PHY header	128 bits
ACK	112 bits + PHY header
RTS	160 bits + PHY header
CTS	112 bits + PHY header
Channel bit rate	1 M bits/s
Propagation delay	1 μ s
Slot duration	50 μ s
SIFS	28 μ s
DIFS	128 μ s
CW_{\min}	16
CW_{\max}	1024
Retry limit for RTS/CTS access	7
CW size decrease threshold d	10 (default)
CW size reset threshold r	4 (default)

channel. When a receiver is in the range of more than one transmitting station, a collision occurs and all transmitted frames cannot be recovered. A frame can also be corrupted by the noise even when there is no collision. The simulations are carried out at the frame level. The effect of the noise is simulated by a given bit error rate (BER) P_b for all the links. The success probability P_s of a frame in a link is then given by $P_s = (1 - P_b)^t$, where t is the duration of the frame in bits. Infinite transmit buffering is assumed for each link.

The values of the system parameters for the IEEE 802.11 DCF simulator are summarized in Table 2. As in [8], these parameter values closely follow those specified for the frequency hopping spread spectrum (FHSS) PHY layer in IEEE 802.11b standard [5]. Note that for each data frame, there is a retry limit. Whenever the number of retransmissions of a data frame reaches this limit, it has to be removed from the transmit buffer no matter if its last transmission succeeds or not. The channel bit rate is assumed 1M bits/s. Frame and header sizes are exactly as those defined by IEEE 802.11 MAC and FHSS PHY layer specifications. Unless otherwise specified, the data frame body payload size is constant (8,184 bits), which is about a fourth of the maximum MAC protocol data unit (MPDU) size (4095 octets) specified for the FHSS PHY layer [5, Section 14.9]. Unless otherwise specified, we assume that the BER $P_b = 10^{-5}$, thereby resulting in a 0.9177 data frame success probability. The error detection of transmitted frames by their FCS is assumed to be perfect at the receiver. Each simulation result (in the sequel) is obtained by averaging 10 independent runs, where in each run the simulated system is typically run for a time period between 100 and 500 seconds.

4.1. Performance measures

To evaluate the network performance, we use five performance measures: throughput, average data frame delay, data frame loss rate, and two fairness indices: STD (standard deviation) and LFI (link fairness index).

We define the throughput R as the average number of successful data frames per second, and the average data frame delay D as the average delay in seconds for a data frame from being generated to being successfully received. We define the data frame loss ratio ρ as

$$\rho := \frac{\text{number of discarded data frames}}{\text{total number of transmitted data frames}}. \quad (2)$$

Since infinite transmit buffering is assumed, the data frame loss is only caused by the prescribed retry limit. When calculating the total number of transmitted data frames in (2), we do not count retransmissions of the same data frames. The STD is defined as the standard deviation of the individual link throughput. If N denotes the number of links, R the total throughput, and R_n the throughput for link n , $n = 1, 2, \dots, N$, then the STD is given by

$$\text{STD} := \sqrt{\frac{1}{N-1} \sum_{n=1}^N \left(R_n - \frac{R}{N} \right)^2}. \quad (3)$$

As in [10], we define the LFI as

$$\text{LFI} := \frac{\max \{R_n\}}{\min \{R_n\}}, \quad n = 1, \dots, N. \quad (4)$$

4.2. Fully loaded IBSS

As in [8, 10], we first investigate a fully loaded IBSS (without AP and communication with other BSSs), in which we assume a fixed number of links per IBSS, each always having a data frame ready to send. The throughput obtained in this fully loaded case is the maximum one which the IBSS can afford. In this case, we do not consider the delay measure since the queueing delay for a data frame could become arbitrarily large. In the IBSS considered, all stations are within the radio range of each other. There does not exist hidden-station problem, let alone the shadowed-receiver problem. Hence, the reset threshold r does not affect the performance of CSMA/CCA. We take a default value $r = 4$. As described in Section 3, for the operation of the proposed CSMA/CCA, we need to assign a decrease threshold d . The performance evaluation of CSMA/CCA with different d s and that of the CSMA/CA protocol are compared in Figure 5. As shown in Figures 5(a) and 5(b), the CSMA/CCA protocols have much smaller fairness indices (STDs and LFIs) than the CSMA/CA protocol. This fact meets the design expectation and demonstrates that the CW size copying can mitigate the fairness problem. In Figure 5(c), the CSMA/CCA protocols with $d = 10, 12$ have a steady throughput whereas the CSMA/CCA protocols with $d = 6, 8$ and the CSMA/CA protocol have large throughput drops as the network traffic load (number of links) goes up. Note that when the traffic load is not heavy and collision occurs rarely, rapid decrease of CW size is preferred since it increases transmission probabilities of the stations. This accounts for the slightly higher throughput of

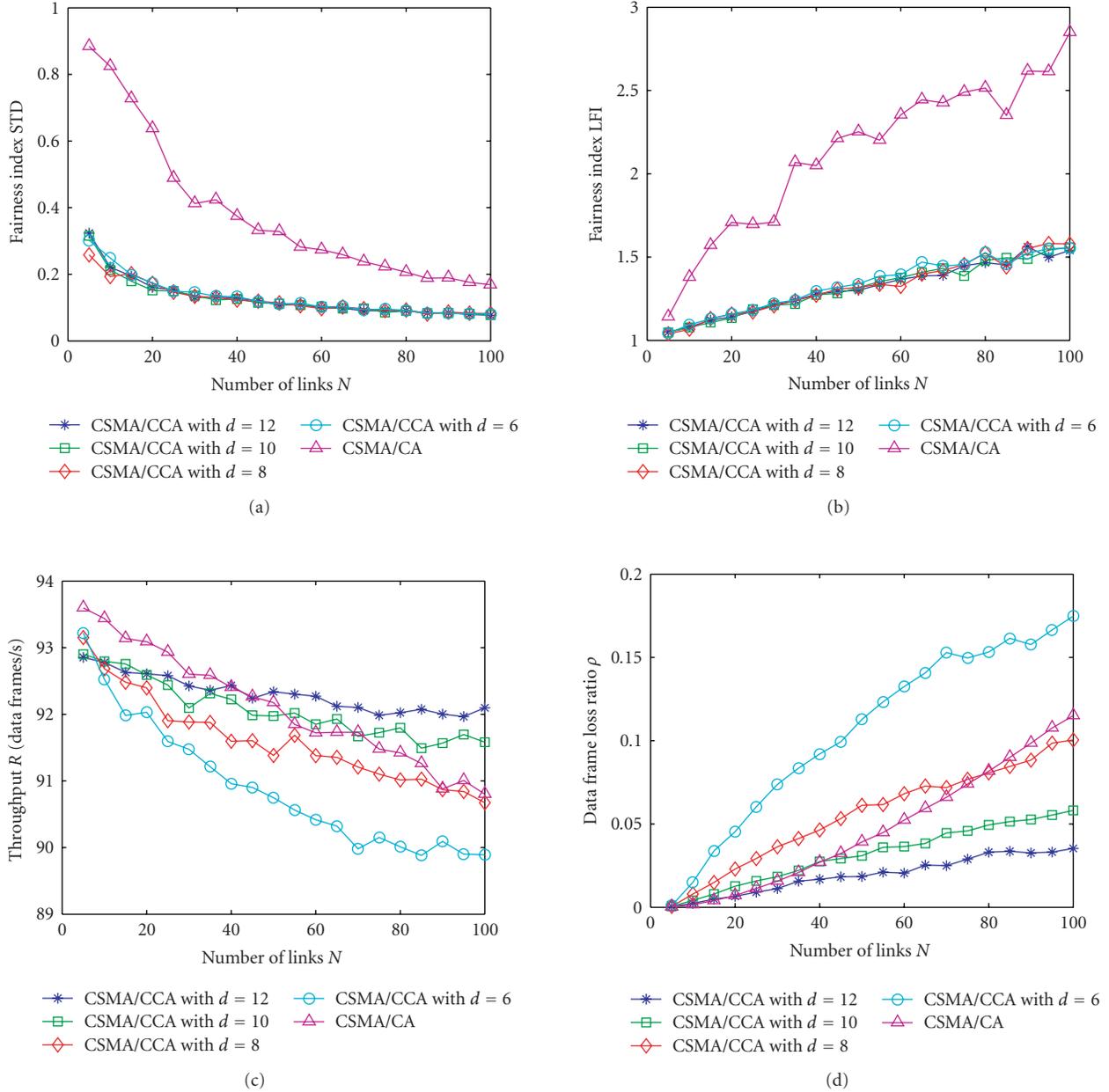


FIGURE 5: Comparison of (a) fairness index STD, (b) fairness index LFI, (c) throughput, and (d) data frame loss ratio for the CSMA/CCA protocol and CSMA/CA protocol in a fully loaded IBSS.

CSMA/CA relative to CSMA/CCA when $N < 40$. As shown in Figure 5(d), the CSMA/CCA protocols with $d = 10, 12$ have smaller data frame loss ratios than the CSMA/CA protocol, whereas the CSMA/CCA protocol with $d = 6, 8$ exhibits larger data frame loss ratio than the CSMA/CA protocol. The worse throughput and data frame loss ratio performance of the CSMA/CCA protocols with small d s comes from the oscillation phenomenon stated in [4]. It coincides with the analysis in [13] and suggests that a moderate decrease threshold d should be chosen to avoid possible performance drops in throughput and data frame loss ratio.

4.3. Infrastructure BSSs with Poisson arrivals

To evaluate CSMA/CCA in more realistic scenarios, we revisit certain network configurations from [4]. In those configurations, we consider infrastructure BSSs with Poisson arrivals. There exist an AP and several associated stations in each BSS and each link is fed with data frames following a Poisson distribution with the same intensity $\lambda = 32$ data frames/s. Unless otherwise specified, the stations can only hear their associated AP and vice versa. By default, we assign the decrease threshold $d = 10$ for the CSMA/CCA protocols in this section.

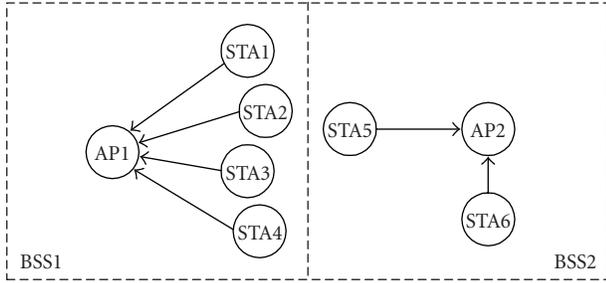


FIGURE 6: A two-BSS configuration where all the stations in BSS1 and STA5 in BSS 2 are in range of each other. The stations are sending data to their respective APs. Each link is generating data at 32 frames per second.

In the following network configurations, we compare CSMA/CCA against the existing CSMA/CA protocol. In order to investigate the effects of the designed CW size reset function and the CW size copying leakage, we also test two modified versions of the CSMA/CCA protocols: CSMA/CCA protocol without reset and CSMA/CCA protocol allowing for leakage. In the CSMA/CCA without reset, we simply set the reset threshold to a large number $r = 100$, so that the CW size reset function seldom works; whereas, unless otherwise specified, we let the reset threshold $r = 4$ in CSMA/CCA. In the CSMA/CCA allowing for leakage, we let a deferring station copy the CW size level in the overheard data frame without checking the BSSID.

A two-BSS configuration

First, we consider a two-BSS configuration copied from [8, Figure 8], as depicted in Figure 6, where all stations (STA1–STA4) in BSS1 and STA5 in BSS2 are in range of each other. The stations are sending data to their respective APs. Since all the stations (STA1–STA4) in BSS1 and STA5 in BSS 2 are in range of each other, the leakage of the CW size copying may happen in the tested CSMA/CCA protocol allowing for leakage. As shown by the simulation results in Table 3, all the CSMA/CCA protocols have smaller fairness indices (STDs and LFIs) than the CSMA/CA protocol, at the price of a little worse throughput and average delay performance. Actually, in all four protocols the links $STAn-AP1$, $n = 1, \dots, 4$, in BSS1 have very fair throughput shares; whereas in BSS2, link $STA5-AP2$ has much smaller throughput than that of link $STA6-AP2$. This is largely due to the inherently unfair fact that when a station in BSS1 transmits, the link $STA5-AP2$ has to defer; whereas the link $STA6-AP2$ can succeed in parallel. Our CSMA/CCA protocol does not intend to solve this kind of unfairness since it may largely degrade the system throughput. In this example, the CSMA/CCA allowing for leakage yields worse fairness performance than the other two CSMA/CCA protocols. The reason is that in the CSMA/CCA with leakage, after a successful data frame transmission in BSS1, the CW size is leaked to STA5 whereas STA6 is unaffected. Since congestion around the area where STA6 stays is much lighter than that in the BSS1-BSS2 border, the leaked

CW size is expected to be larger than that of STA6. Therefore, the leakage usually makes STA5's CW size larger than that of STA6, which reduces the STA5's access opportunities further. As shown in Table 3, both CSMA/CCA as well as the CSMA/CCA protocol without reset yield very similar fairness performance. The designed CW size reset function has little impact on the protocol performance, since there does not exist shadowed-receiver problem in this configuration.

A three-BSS configuration

Here we consider a three-BSS configuration copied from [8, Figure 10], as depicted in Figure 7. Besides the APs, BSS1 contains four stations (STA1–STA4) and BSS2 contains only one station (STA5), all STA1–STA5 near the BSS1-BSS2 border. There is one station (STA6) which straddles the BSS2-BSS3 border and is in range of both AP2 and AP3. The stations near the BSS1-BSS2 border are within range of each other; however, they can only hear their own APs. Each of STA1–STA5 has data frames to and from the AP of its BSS. Recall that AP1 is viewed as a number of different initial stations when it contends for different links separately. STA6 is sending data frames to AP3. The data frame generation rate in each link is 32 frames per second. Table 4 shows the simulation results for the four tested protocols. Since BSS3 only contains one link, the BSS3 fairness indices are omitted. It can be verified from Table 4 that the individual link throughput in BSS1 is unfair for the CSMA/CA protocol, with links $STAn-AP1$ having much higher throughput than links $AP1-STAn$, $n = 1, \dots, 4$. This unfairness comes from the shadowed-receiver problem occurring at AP1 when STA5 is transmitting. Compared to the CSMA/CA protocol, the three versions of CSMA/CCA protocol largely mitigate the fairness problem in BSS1. Specifically, in each BSS, the CSMA/CCA protocol without reset exhibits very good fairness characteristics with small BSS STDs and LFIs. However, this good fairness is actually achieved by almost prohibiting the data transmissions in BSS2. Because either link ($AP2-STA5$ or $STA5-AP2$) in BSS2 encounters the shadowed-receiver problem when any link in BSS1 and BSS3 is on, without the CW size reset function, both links would easily have their CW sizes staying at CW_{max} and seldom transmit. Besides maintaining good fairness in each BSS, the other two CSMA/CCA protocols achieve better balance among the BSSs than the CSMA/CCA protocol without reset. With the help of the CW size reset function, the links in BSS2 could have their CW sizes escape from CW_{max} and hence gain more chances to access the channel. From Table 4, we can see that the CW size leakage across the BSSs actually helps to further balance the BSS throughput in this example, by sacrificing some fairness in the single BSS, because the CW size leakage from BSS1 to BSS2 can mitigate the heavy shadowed-receiver problem in BSS2. In the MACAW protocol [4], the shadowed-receiver problem is partly solved by using a self-defined RRTS (request-for-RTS) frame. With the addition of the RRTS scheme, the MACAW protocol achieves near-perfect throughput balance in each BSS as well as among BSSs for this three-BSS configuration. Since the RRTS frame

TABLE 3: Simulation results for the two-BSS configuration in Figure 6: throughput is in data frames/s, and average delay is in seconds.

	CSMA/CCA	CSMA/CCA without reset	CSMA/CCA allowing for leakage	CSMA/CA
STA1-AP1 throughput	18.8198	8.9500	19.9860	20.4957
STA2-AP1 throughput	18.9746	18.8951	20.0013	20.2652
STA3-AP1 throughput	18.8679	18.9073	19.9051	19.9821
STA4-AP1 throughput	18.9251	18.9197	19.9912	20.2681
STA5-AP2 throughput	16.4971	16.3774	12.3084	11.5260
STA6-AP2 throughput	32.3277	32.4309	32.2214	31.7331
Overall throughput	124.4112	124.4803	124.4133	124.2708
Overall average delay	28.7690	30.0479	27.5486	28.9493
Overall data frame loss ratio	0.00016	0.00013	0.00024	0.00022
BSS1 fairness index STD	0.0583	0.0240	0.0384	0.1821
BSS2 fairness index STD	7.9153	8.0267	9.9565	10.1036
Overall fairness index STD	5.2580	5.3071	5.8493	5.8712
BSS1 fairness index LFI	1.0082	1.0029	1.0048	1.0257
BSS2 fairness index LFI	1.9596	1.9802	2.6178	2.7532
Overall fairness index LFI	1.9596	1.9802	2.6178	2.7532

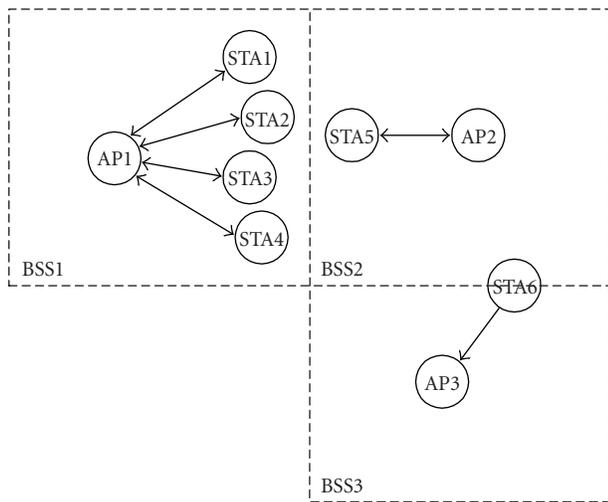


FIGURE 7: A three-BSS configuration with varying levels of congestion.

is out of the definitions of the IEEE 802.11 standards, we do not investigate this RRTS scheme. Also note that the RRTS scheme cannot completely solve the shadowed-receiver problem; for example, it fails in the shadowed-receiver configuration in Figure 3.

A worst case

Finally, let us revisit the two-BSS configuration in Figure 3 with two links (AP1-STA1 and STA2-AP2). Since there is only one link in each BSS in this configuration, the desired benefit of the CW size copying diminishes. Moreover, there exists high unbalance between the two links, where link STA2-AP2 experiences a severe shadowed-receiver problem whereas link AP1-STA1 does not. As described in Section 3,

the designed gentle CW size decrease algorithm is nonrobust to the shadowed-receiver problem. This imbalance may largely degrade fairness performance of the CSMA/CCA protocol. Therefore, the configuration in Figure 3 is one of the worst cases for the proposed CSMA/CCA protocol. As verified by simulation results in Table 5, the CW size reset function does mitigate the shadowed-receiver problem, for example, the CSMA/CCA protocol without reset yields the worst performance, and the CW size leakage does not help in this example, for example, the CSMA/CCA allowing leakage has worse performance than our CSMA/CCA protocol. Compared to the CSMA/CA, the proposed CSMA/CCA protocol has a little worse fairness performance. But the biggest disadvantage of our CSMA/CCA protocol is its severe degradation in average delay performance compared to that of CSMA/CA in this worst case.

As demonstrated by our simulations, the proposed CSMA/CCA protocol meets the design objective and mitigates the fairness problem in most cases. But we hasten to note that there are many remaining design issues, including the amelioration of the shadowed-receiver problem in Figure 3.

5. CONCLUSIONS

In this paper, we designed a CSMA/CCA MAC protocol for the IEEE 802.11 DCF. The main concept behind this new protocol is that by CW size copying, all stations in a BSS can contend fairly with similar CW sizes, thereby mitigating the fairness problem. To facilitate CW size copying, we modified the CA scheme in CSMA/CA protocol to obtain our novel CCA scheme. Simulations confirmed that our CSMA/CCA protocol provides promising results showing improved fairness compared to the CSMA/CA protocol, especially in network configurations with multiple links and heavy congestion. A major advantage of the proposed CSMA/CA protocol is the fact that it is designed based on the structure of the

TABLE 4: Simulation results for three-BSS configuration in Figure 7: throughput is in data frames/s, and average delay is in seconds.

	CSMA/CCA	CSMA/CCA without reset	CSMA/CCA allowing for leakage	CSMA/CA
STA1-AP1 throughput	10.9465	11.4992	10.2350	15.2702
STA2-AP1 throughput	11.1360	11.5067	10.0668	15.1787
STA3-AP1 throughput	10.8232	11.2967	10.2854	16.1105
STA4-AP1 throughput	10.9170	11.3074	10.1881	15.8502
AP1-STA1 throughput	10.7715	11.3690	8.9339	5.7771
AP1-STA2 throughput	10.6091	11.2821	8.5661	5.9530
AP1-STA3 throughput	10.4814	11.3093	8.9035	6.0410
AP1-STA4 throughput	10.5912	11.2590	8.6512	6.2679
STA5-AP2 throughput	2.0741	0.3808	6.1743	3.5362
AP2-STA5 throughput	1.9264	0.4811	5.3879	1.8705
STA6-AP3 throughput	32.1408	32.0342	32.0012	32.4216
Overall throughput	122.4172	123.7255	119.3935	124.2770
Overall average delay	32.8033	37.1690	23.9973	24.9502
Overall data frame loss ratio	0.0283	0.0081	0.0786	0.0523
BSS1 fairness index STD	0.2028	0.0910	0.7260	4.8059
BSS2 fairness index STD	0.0739	0.0502	0.3932	0.8328
Overall fairness index STD	7.4434	7.7825	6.8645	8.4317
BSS1 fairness index LFI	1.0625	1.0220	1.2007	2.7887
BSS2 fairness index LFI	1.0767	1.2634	1.1460	1.8905
Overall fairness index LFI	16.6844	84.1234	5.9395	17.3331

TABLE 5: Simulation results for shadowed-receiver configuration in Figure 3: throughput is in data frames/s, and average delay is in seconds.

	CSMA/CCA	CSMA/CCA without reset	CSMA/CCA allowing for leakage	CSMA/CA
AP1-STA1 throughput	26.2337	18.3634	22.1149	28.5990
STA2-AP2 throughput	32.8342	32.9669	30.1760	27.0833
Total throughput	59.0671	51.3303	52.2909	55.6823
Average delay	11.7957	32.9497	30.0828	0.0054
Data frame loss ratio	0.0016	0.00078	0.0077	0.0011
Fairness index STD	3.3003	7.3018	4.0305	0.7578
Fairness index LFI	1.2516	1.7953	1.3645	1.0560

IEEE 802.11 DCF. Therefore, it can be readily deployed in the existing IEEE 802.11 WLANs.

6. DISCLAIMER

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the US Government.

ACKNOWLEDGMENTS

This work was prepared through collaborative participation in the Communications and Networks Consortium sponsored by the US Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative

Agreement DAAD19-01-2-0011. The US Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

REFERENCES

- [1] K. Pahlavan and P. Krishnamurthy, *Principles of Wireless Networks: A Unified Approach*, Prentice-Hall, Upper Saddle River, NJ, USA, 2002.
- [2] L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels: part I—carrier sense multiple-access modes and their throughput-delay characteristics," *IEEE Transactions on Communications*, vol. 23, pp. 1400–1416, 1975.
- [3] P. Karn, "MACA—a new channel access method for packet radio," in *Proceedings of the 9th ARRL/CRRL Amateur Radio*

- Computer Networking Conference*, pp. 134–140, Ontario, Canada, September 1990.
- [4] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, “MACAW: a media access protocol for wireless LAN’s,” in *Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM ’94)*, pp. 212–225, London, UK, August–September 1994.
- [5] IEEE 802.11 WG, *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: higher speed physical layer (PHY) extension in the 2.4GHz band*, IEEE Std. 802.11b/D5.0, April 1999.
- [6] IEEE 802.11 WG, *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: higher speed physical layer (PHY) extension in the 5GHz band*, IEEE Std. 802.11a/D5.0, April 1999.
- [7] IEEE 802.11 WG, Draft supplement to *Part 11: wireless medium access control (MAC) and physical layer (PHY) specifications: medium access control (MAC) enhancements for quality of service (QoS)*, IEEE 802.11e/D3.3.2, November 2002.
- [8] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535–547, 2000.
- [9] F. Cali, M. Conti, and E. Gregori, “IEEE 802.11 wireless LAN: capacity analysis and protocol enhancement,” in *Proceedings of IEEE 17th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM ’98)*, vol. 1, pp. 142–149, San Francisco, Calif, USA, March–April 1998.
- [10] T. Ozugur, “Optimal MAC-layer fairness in 802.11 networks,” in *Proceedings of IEEE International Conference on Communications (ICC ’02)*, vol. 2, pp. 675–681, New York, NY, USA, April–May 2002.
- [11] T. Ozugur, M. Naghshineh, P. Kermani, C. M. Olsen, B. Rezvani, and J. A. Copeland, “Balanced media access methods for wireless networks,” in *Proceedings of 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom ’98)*, pp. 21–32, Dallas, Tex, USA, October 1998.
- [12] I. Tinnirello and S. Choi, “Temporal fairness provisioning in multi-rate contention-based 802.11e WLANs,” in *Proceedings of 6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM ’05)*, pp. 220–230, Taormina, Italy, June 2005.
- [13] C. Wang, B. Li, and L. Li, “A new collision resolution mechanism to enhance the performance of IEEE 802.11 DCF,” *IEEE Transactions on Vehicular Technology*, vol. 53, no. 4, pp. 1235–1246, 2004.
- [14] E. M. Cheung, G. W. Wong, and R. W. Donaldson, “Probabilistic contention window control in 802.11 WLANs,” in *Proceedings of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM ’03)*, vol. 2, pp. 654–658, Victoria, BC, Canada, August 2003.
- [15] Y. Kwon, Y. Fang, and H. Latchman, “Design of MAC protocols with fast collision resolution for wireless local area networks,” *IEEE Transactions on Wireless Communications*, vol. 3, no. 3, pp. 793–807, 2004.
- [16] S. J. Golestani, “A self-clocked fair queueing scheme for broadband applications,” in *Proceedings of IEEE 13th Networking for Global Communications (INFOCOM ’94)*, vol. 2, pp. 636–646, Toronto, Ontario, Canada, June 1994.
- [17] C. E. Koksall, H. Kassab, and H. Balakrishnan, “An analysis of short-term fairness in wireless media access protocols,” in *Proceedings of International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS ’00)*, pp. 118–119, Santa Clara, Calif, USA, June 2000.
- [18] Z. Fang, B. Bensaou, and Y. Wang, “Performance evaluation of a fair backoff algorithm for IEEE 802.11 DFWMAC,” in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc ’02)*, pp. 48–57, Lausanne, Switzerland, June 2002.
- [19] S. Mangold, S. Choi, P. May, and G. Hiertz, “IEEE 802.11e—fair resource sharing between overlapping basic service sets,” in *Proceedings of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC ’02)*, vol. 1, pp. 166–171, Lisboa, Portugal, September 2002.
- [20] Y. Xiao and H. Li, “Voice and video transmissions with global data parameter control for the IEEE 802.11e enhance distributed channel access,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 15, no. 11, pp. 1041–1053, 2004.

Xin Wang received his B.S. degree in 1997 and M.S. degree in 2000 from Fudan University, Shanghai, China, and his Ph.D. degree in 2004, from Auburn University, all in electrical engineering. He is currently a Research Associate at the University of Minnesota. His research interests include medium access control, cross-layer design, energy-efficient resource allocation, and signal processing for communication networks.



Georgios B. Giannakis received his B.S. in 1981 from the National Technical University of Athens, Greece and his M.S. and Ph.D. degrees in electrical engineering in 1983 and 1986 from the University of Southern California. Since 1999 he has been a Professor with the Department of Electrical and Computer Engineering at the University of Minnesota, where he now holds an ADC Chair in Wireless Telecommunications. His general interests span the areas of communications and signal processing, estimation and detection theory—subjects on which he has published more than 250 journal papers, 450 conference papers, and four books. Current research focuses on complex-field and space-time coding, multicarrier, ultra-wideband radios, cross-layer designs, and wireless sensor networks. He is the (co-) recipient of six best paper awards from the IEEE Signal Processing (SP) and Communications Societies and also received the SP Society’s and EURASIP’s Technical Achievement Awards in 2000 and 2005.

