Exploiting Physical Layer Detection Techniques to Mitigate Starvation in CSMA/CA Wireless Networks

Alessandro Leonardi, and Sergio Palazzo
Dipartimento di Ingegneria Informatica e delle Telecomunicazioni
University of Catania, Italy

Abdul Kader Kabbani, and Edward W. Knightly
Department of Electrical and Computer Engineering
Rice University, Houston, TX 77005

Abstract— **Many proposed and implemented wireless MAC protocols are based on collision-avoidance handshakes between senders and receivers. Unfortunately, information asymmetry problems can potentially occur with such protocols and severely reduce the network capacity. In this paper, we introduce a receiver-initiated mechanism, called Carrier Sense Multiple Access with Collision Avoidance by Receiver Detection (CSMA/CARD), that makes use of collisions sensed at the physical layer of a receiver to mitigate the effect of such problems. More specifically, and depending on the exact nature of the handshake mechanism, collisions can be used by the receiver to predict whether some sender attempted to initiate a transmission towards this receiver. The receiver, in its turn, would initiate an action on its own to help expedite the handshake mechanism. Such a simple cooperation mechanism can be coupled with any appropriate MAC protocol to improve its performance. We evaluate the effectiveness of this approach with the 802.11 DCF MAC in particular, and we show that starvation and unfairness results can be highly mitigated.**

I. Introduction

Several studies have demonstrated that when all transmitters are within range of each other, CSMA protocols provide fair access opportunities to all flows. Unfortunately, in topologies where the different transmitters are essentially out of range, channel state information becomes incomplete. The lack of such information leads to poor performance even when further enhancements such as the RTS/CTS handshake mechanism are used [2]. In particular, starvation situations arise in which a few flows capture all the bandwidth while many other flows get very low or even zero throughput. We refer to this problem as *Information Asymmetry* [8].

In this paper we propose a novel solution to help alleviate this problem, called Carrier Sense Multiple Access with Collision Avoidance by Receiver Detection (CSMA/CARD). Our proposed solution is based on a novel receiver-initiated mechanism which exploits some information at the physical level. In particular, we illustrate via simple analysis and simulations that the detection of two or more overlapped signals at a potential receiver, when coupled with the appropriate mechanism, can be effective in providing extra channel state information for a protocol like IEEE 802.11 DCF. Note that our objective in this paper is not to come up with a MAC protocol that is optimal in any sense (be it throughput maximization, overhead minimization, fairness, or collision-free transmissions). Our objective in this paper is to rather illustrate the performance gain achieved by any existing contention-based protocol when it utilizes the cost-free collision information at the physical-layer. In other words, our PHY-aware mechanism can be introduced to operate jointly with any contention-based MAC protocol to improve its performance while keeping the changes minor and the design simple. Hence, the performance evaluation of our PHY-aware mechanism is done by comparing an appropriate existing contention-based protocol without the PHY-aware mechanism against the same protocol with the PHY-aware mechanism. We selected 802.11 in this paper due to its design simplicity and its uncomplicated analysis as well as the familiarity of the reader with its framework.

The remainder of this paper is organized as follows. In Section II we discuss the related work. In Section III the new protocol mechanism is described in details, and in Sections IV and V we illustrate the theory related to the collision detection and the model of the mechanism proposed, respectively. In Section VI we analyze the performance of the novel mechanism compared to a classical approach. Finally in Section VII some concluding remarks are drawn.

II. Related Work

Multiple Access Collision Avoidance (MACA)[10] has been proposed to counteract the hidden terminal problem in single-channel networks [12]. MACA suggests a bi-directional handshake mechanism between each sender and receiver to detect collisions. A sender initiates a Request-To-Send packet (RTS) to the receiver, and the receiver replies with a Clear-To-Send packet (CTS) if it receives the RTS correctly. Several other sender-initiated variations of the same handshake mechanism have been proposed as well [13], [15]. In particular, an RTS/CTS handshake mechanism has been standardized and adopted by the IEEE 802.11 committee [17]. Different solutions have been proposed in the literature to improve the performance of the IEEE 802.11 protocol while countering the hidden terminal problem. In particular, a major effort has been spent on the modification of the IEEE 802.11 MAC layer timers, handshake mechanism [2], and the Binary Exponential Backoff (BEB) mechanism [1], [6] with the purpose of achieving more fairness and spatial reuse. In addition, there have been also papers that aim at improving

1-4244-0860-1/07/25.00

the IEEE 802.11 MAC bandwidth efficiency by exploiting the physical layer capture [5], [14]. However, despite the numerous modifications suggested to improve their throughput performance, the IEEE 802.11 MAC protocol and its variants can suffer severe unfairness problems in multi-hop ad hoc networks due to location-dependent contention. In particular, one major shortcoming in the prevailing contention resolution mechanisms is that they are sender-initiated whereas the receiver has essentially better knowledge of the contention around itself than the sender. Different receiver-initiated MAC protocols have been proposed in literature [9], [16] to improve the performance of CSMA/CA protocols. Bharghavan et al. [2] suggested a Request-for-Request-To-Send (RRTS) packet initiated by the receiver to alleviate the unfairness problem. Receivers which could decode the RTS packet sent by their corresponding senders and could not reply with a CTS wait until their NAV expires. Once the NAV expires, the receiver sends the RRTS packet to its sender requesting the RTS packet to be sent back. Therefore, the RRTS packet can help reducing the extra backing off inefficiency and its unfairness consequence at the expense of introducing more overhead due to the RRTS packet itself. Despite their illustrated benefits, receiver-initiated schemes have not received wide acceptance in practice. This is partially because fully receiver-initiated schemes can sometimes initiate many unnecessary handshake packets that under-utilize the network bandwidth (although this is also true in the case of fully sender-initiated schemes). On the other hand, current receiver-initiated schemes require a per-receiver traffic estimator that should successfully adapt under dynamic topology and traffic environments. Another important reason why receiver-initiated protocols have not seen wide acceptance is that the state-of-the-art receiver-initiated protocols cannot interoperate with the current widely deployed IEEE 802.11 MAC devices. As opposed to other contention-based MAC protocols, our mechanism is particular for the approach it follows and for its ability to overcome the shortcomings of classical receiver-initiated MAC protocols. More specifically, the mechanism that we introduce is the first mechanism that attempts to utilize collisions on the physical layer even when no packets can be captured. In addition, our mechanism does not lead to a fully receiver-initiated protocol neither does it lead to a fully sender-initiated protocol. Hence, it avoids leading to a protocol that suffers from the overhead and under-utilization disadvantages of each of the two protocol classes as discussed earlier in this section. Our mechanism is also simpler than other fully receiver-initiated protocols in the sense that it does not require any traffic estimators [9], [16]. This allows easier implementation with minimal modifications on one hand, simple protocol designs, and inter-operability with legacy devices that implement the 802.11 standards.

III. CSMA/CARD Protocol Design

Conceptually, and as purely sender-initiated protocols are not successful, our approach suggests that the receiver should participate in the contention mechanism in order to mitigate information asymmetry problems [7]. The main challenge with such hybrid sender-and-receiver-initiated techniques is that a potential receiver should be able to predict the existence of a potential sender in a timely manner while minimizing the probability of false predictions and maximizing that of true ones. Our approach for counteracting such a challenge is by making use of the events occurring at the physical layer. In particular, detection of significant received signal power variations can be probabilistically interpreted as handshake messages initiated by a potential sender based on historical observations. The receiver then, in the case of anticipating a sender-initiated handshake attempt, reacts accordingly by participating itself in a handshake sequence.

We now illustrate the mechanism and demonstrate its efficiency within the CSMA/CA framework. We call our approach CSMA/CARD. We make use of collision events at a potential receiver to help it make an educated guess of whether an RTS packet has been specifically destined to it or not, even if the RTS packet cannot be completely decoded. We describe the CSMA/CARD mechanism by which any node can detect whether two or more packets collided at it. Whenever a collision is detected at a node (two packets are transmitted simultaneously within the range of this node), the node will assume with a certain probability that the collision took place with an RTS packet which was intended for it and will broadcast a Request-for-Request-to-Send (RRTS) packet accordingly. Bharghavan et al. had a similar receiver cooperation approach as ours in the context of CSMA/CA protocols which does not rely on physical layer events, but, as we illustrate in this paper, making use of physical layer events can help further improve the performance of CSMA/CA by increasing the number of true predictions of sender initiated RTS packets. Note that CSMA/CARD is based on IEEE 802.11 DCF mechanism and we will use in the following the same terminology and most of the parameters already used in 802.11.

We start by describing a non-adaptive probabilistic model which is easy to adopt in an analytical model (as shown in Section V) after which we present the adaptive probabilistic model.

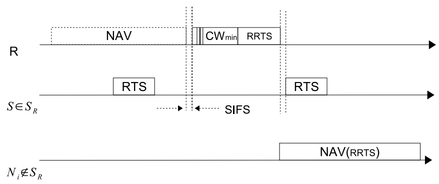
A. Non-adaptive CSMA/CARD

Denote a potential receiver by R and the set of all its potential sending neighbors by S_R. Upon an RTS transmission by a node $S \in S_R$, R will send back a CTS if R is in the idle state[1]). Otherwise, if R is not in the idle state, we distinguish two different cases depending on whether R is able to decode the RTS or not.

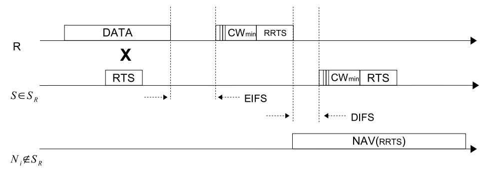
- *Decodable RTS.*
  If R is able to decode the RTS packet of S, R will send an RRTS packet back to S at the minimum contention window, CW_{min}, for once only (i.e., no RRTS packets are retransmitted) right after R's NAV expires. When the RRTS packet is received by S, S defers for a SIFS period

[1] R will not defer sending the CTS packet due to physical or virtual carrier sensing.

and sends back an RTS packet to R. Any node $N_i \notin S_R$ which receives the RRTS packet will set its NAV to NAV(RRTS) = RTS+SIFS+CTS+SIFS. This mechanism is shown in Figure 1(a) and be applied to the situation shown in Figure 2(a) where the two receivers B and C are in the range of each other. Note that it has been already illustrated in [2] that such an approach mitigates the short-term unfairness in different scenarios.



(a) Decodable RTS Case



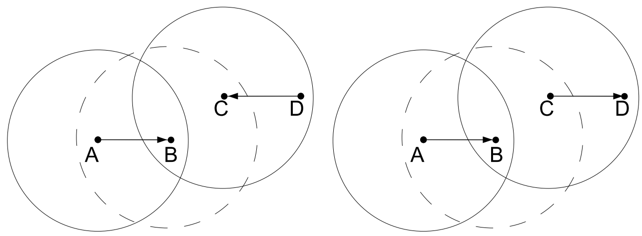
(b) Non-decodable RTS Case

Fig. 1. CSMA/CARD Time-line

- *Non-decodable RTS.*
  This case is when R detects a collision for the duration of an RTS packet (as discussed in Section IV) while R is not already in the process of another transmission procedure (i.e., R has not just sent or received a CTS or a DATA packet). In such a case, R broadcasts an RRTS packet for once only with a fixed probability p_S and at the minimum contention window after R's NAV expires by an Extended-IFS (EIFS) period. When a node $S \in S_R$ receives R's RRTS, an interested sender S will contend for sending an RTS to R at the minimum contention window size. As it is possible ther is more than one potential sender to R, sending such an RTS takes places by contention where a node S would start contending after deferring for a DIFS period. Consequently, upon the reception of the RTS, all other nodes in $N_i \notin S_R$ will set their NAV for a period of time equal to NAV(RRTS)=DIFS+CW_{min}+RTS+SIFS+CTS+SIFS. Figure 1(b) illustrates the time-line of the proposed mechanism and can be applied to the situation shown in Figure 2(b).

B. Adaptive CSMA/CARD

As opposed to the non-adaptive protocol discussed in the previous section, the adaptive protocol adjusts the probability value for sending an RRTS at each potential receiver, p_S based on the events experienced by the receiver itself. This is to reduce the probability of having a potential receiver send out unnecessary RRTS packets as is the case in the non-adaptive CSMA/CARD protocol. For example, one choice is to design p_S to be the fraction of the last RRTS packets which were responded to by an RTS packet. Other design choices include optionally piggy-backing on the broadcast RRTS packet the number of collisions that a receiver senses since the last RRTS packet it sent out.



(a) Symmetric Flows (b) Asymmetric Flows

Fig. 2. Example topologies.

IV. Collision Detection

Unlike CSMA/CD protocol where the transmitter simultaneously listens for collisions from other senders, in wireless networks, monitoring for collisions while sending is not possible without a second radio. Moreover, the collision occurs at the receiver, making a sender-side collision irrelevant. The novelty of CSMA/CARD design approach is in the use of the actually received signal to detect a collision. At its simplest form, we consider collision happens when there are two signals superimposed at the receiver. We show now how to use the known methods in the detection theory to define and solve our collision detection problem.

In standard problems of detection theory, there exists a set of data $\{x_i\}_1^n$ known as data set, samples, or observation, and a set of decisions $\{\mathcal{H}_i\}_1^K$, known as the set of hypotheses and we are interested to decide one of the choices $\mathcal{H}_i$ for the given set of observations. To arrive a decision we form a function of data set, $T(x^n)$ and make a decision based on its value. For the case of collision of two transmissions, the collision detection problem is simply a binary hypothesis testing problem. Our objective is to make the correct decision of whether there is a collision (null hypothesis denoted by $\mathcal{H}_0$), which is the reception of two or more superimposed signals, or not (alternative hypothesis denoted by $\mathcal{H}_1$). Such a problem of arriving to one decision out of two is termed binary hypothesis testing in the detection theory. In testing $\mathcal{H}_0$ versus $\mathcal{H}_1$, there are two types of errors that can be made: $\mathcal{H}_0$ can be falsely accepted or $\mathcal{H}_0$ can be falsely rejected. The first of these two error types is called a false alarm where the consequence is introducing extra overhead caused by activating the RRTS mechanism when it is not really needed. The second error type is called a miss, and the consequence is keeping the starved flow in its disadvantaged state. The correct acceptance of $\mathcal{H}_0$ is called a detection. Obviously, for any given decision problem, there is more than one possible decision strategy or rule that can be applied. We next consider the Neyman-Pearson criterion as the appropriate optimization formulation for our detection problem. The Neyman-Pearson optimality criterion is simply to maximize the detection probability (hence, minimize the *missing* probability) for some fixed false alarm probability P_{FA}.

Theorem 1 (Neyman-Pearson): To maximize probability of detection, P_D, for a given probability of false alarm $P_{FA} = \alpha$, decide $\mathcal{H}_0$ if

$$L(x) = \frac{p(x|\mathcal{H}_0)}{p(x|\mathcal{H}_1)} > \gamma, \tag{1}$$

where the threshold γ is found from

$$P_{FA} = \int_{\{x:L(x)>\gamma\}} p(x|\mathcal{H}_1)dx = \alpha. \tag{2}$$

The Neyman-Pearson rule described in this section is based on the assumption that the distributions $pr(x|\mathcal{H}_0)$ and $pr(x|\mathcal{H}_1)$ are known a priori[2]. For example, if we assume that (i) collisions happen when two signals are superimposed at the receiver (with additive white gaussian noise) and (ii) 1's and 0's are sent with the same probability using BPSK modulation over gaussian fading channels, then the detection algorithm can assume both $pr(x|\mathcal{H}_0)$ and $pr(x|\mathcal{H}_1)$ to have zero-mean gaussian distributions each with the appropriate variance value. Observing N samples $x_1, x_2, \ldots, x_N$ of the received signal at the receiver, it can be calculated [11] that the decision $\mathcal{H}_1$ should be made when

$$\frac{1}{N}\sum_{n=1}^{N} x_n^2 > \frac{\frac{2}{N}\ln\gamma + \ln\frac{\sigma_1^2}{\sigma_0^2}}{\frac{1}{\sigma_0^2} - \frac{1}{\sigma_1^2}}. \tag{3}$$

Figure 3 illustrates the distribution of each hypothesis and shows the decision regions and corresponding thresholds found using Neyman-Pearson theorem. The implementation of collision detection in today's hardware requires only small modifications. There exist already some receivers such as [4] which are very similar to IEEE 802.11 PHY except that they continue to monitor the received signal strength after the PHY transits from receiver training state to data reception state. These kind of receivers can be used to detect collisions.

V. Analysis

In this section we compute the per-flow throughput that can be achieved using CSMA/CARD in the Information Asymmetry scenario depicted in Figure 2(b). The model we follow in this section borrows from that derived in [8]. In particular, we build a model representing the channel state as seen by the individual channel sources. According to this model, the behavior of an arbitrary station employing a CSMA protocol such as 802.11 DCF can be identified by four different states: *(i)* idle, *(ii)* occupied by a successful transmission of the station, *(iii)* occupied by a collision, and *(iv)* busy due to the activity of other nodes. The time intervals during which the station remains in each of the four states above are denoted by σ, T_s, T_c and T_b respectively.

[2]Direct extension of the presented likelihood ratio test for the case of unknown a priori distributions is known as Generalized Likelihood Ratio Test (GLRT). For brevity we do not include the discussion of GLRT and its performance in this paper.

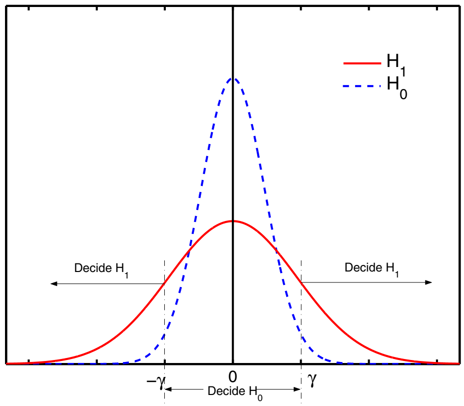


Fig. 3. Illustration of hypotheses regions and decision thresholds for signal with two different variances.

The final expression for the throughput of a station is given by:

$$T_P = \frac{\tau(1-p)}{\tau(1-p)T_s + \tau p T_c + (1-\tau)(1-b)\sigma + (1-\tau)bT_b} \tag{4}$$

where τ is the probability that the station sends out a packet after an idle slot (under the assumption that it is always backlogged), p is the probability that a transmission of the station is not successful (also called conditional packet loss probability), and b is the probability that the channel becomes busy after an idle slot due to the activity of other nodes.

In the following analysis we always consider a system managed by RTS/CTS handshake mechanism. In this case the values of T_s and T_c are given by

$$\begin{aligned} T_s &= RTS + SIFS + \delta + CTS + SIFS + \delta \\ &+ E\{P\} + SIFS + \delta + ACK + DIFS + \delta, \end{aligned}$$

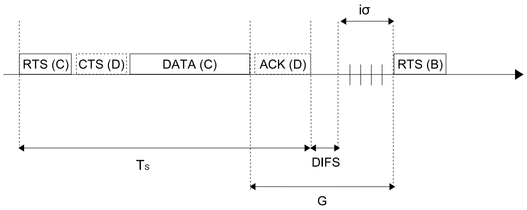
$$T_c = RTS + DIFS + \delta \tag{5}$$

where $E\{P\}$ represents the average length of the packet and δ is the propagation delay.

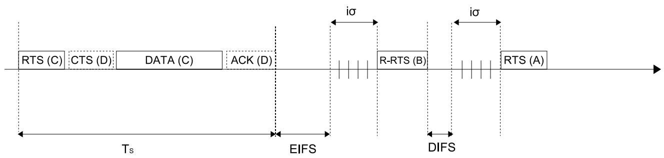
The probability τ has been computed in [3] as follows:

$$\tau = \frac{2(1-2p)}{(1-2p)(W+1) + pW(1-(2p)^m)} \tag{6}$$

where $W = CW_{min}$ and m is the maximum backoff stage such that $CW_{max} = 2^m W$. The throughput expression, eq. (4), and the expression of the probability τ, eq. (6), remain the same in the case of the CSMA/CARD mechanism. Note that sender A does not detect any of C's and D's transmissions, as a consequence, its transmission attempts are not coordinated with those of sender B and occur at random points of time according to its backoff process. In Figure 4, we show the channel state as perceived by node B, in two different cases. Case (a) refers to the channel state while sender A attempts to initiate a new RTS transmission, while case (b) refers to the channel state after a RTS transmission made by node A which occurs during C's transmission. In the classical 802.11 DCF



(a)



(b)

Fig. 4. Channel state perceived by node B while sender A attempts to transmit an RTS (a). Channel state perceived by node B after sender A has transmitted an RTS (b).

approach, in order to have a successful transmission, node A has to send the RTS during the gap when node C is in the backoff phase. Only during this gap, the receiver B knows that an RTS packets has been sent to it. We call this gap G as illustrated in Figure 4(a). As for CSMA/CARD, when A's transmission occurs during the time interval outside G, a collision occurs and is therefore followed by the transmission of an RRTS from node B towards node A[3].

Using the model introduced in [8], we can also calculate the conditional packet loss probability of flow f_{AB} as:

$$p(A) = 1 - \frac{\tau \cdot \overline{\Delta}}{\overline{T}} \tag{7}$$

where $\overline{\Delta}$ is the average time during which node A can send a packet to node B, while $\overline{T}$ represents the total summation of the average duration of each channel state. More specifically, each cycle $\overline{T}$ is composed of a successful data transfer, T_s, a variable number of slots corresponding to the backoff phase, $i\sigma$, and three constant time interval: EIFS, DIFS, and the duration of an RRTS. The average time interval, $\overline{\Delta}$, can be computed as follows:

$$\overline{\Delta} = \frac{1}{W} \cdot \sum_{i=0}^{W-1} [T_s + i\sigma - RTS - SIFS] \tag{8}$$

Substituting eq. (8) and the value of $\overline{T}$ in eq. (7), we obtain the final expression of the conditional packet loss probability

[3]In order to simplify our analysis, we assume that all collisions can be perfectly detected and are always followed by an RRTS packet.

σ (slot time)	$20\mu s$
SIFS	$10\mu s$
DIFS	$50\mu s$
RTS	288 bit
CTS	240 bit
ACK	240 bit
RRTS	288 bit
CW_{min}	31
CW_{max}	1023
E (packet payload)	8224 bit
δ (propagation delay)	$2\mu s$
Channel bit rate	2 Mbit/s

TABLE I

PHY AND MAC LAYER PARAMETERS.

as:

$$p(A) = 1 - \frac{\tau \cdot \left[\Delta' + \frac{\sigma(W-1)}{2}\right]}{\tau T_s + (1-\tau)\sigma + (EIFS + DIFS + RRTS)} \tag{9}$$

where $\Delta' = T_s - RTS - SIFS$.

The value of τ in eq. (9) is calculated from eq. (6) when $p = 0$ or $m = 0$, i.e., no exponential backoff is considered. $p(A)$ can now be calculated because all the parameters are known. Substituting eq. (9) in eq. (6), we obtain $\tau(A)$, and then substituting $\tau(A)$ and $p(A)$ in eq. (4) we obtain the throughput, $T_P(A)$, of flow f_{AB}. Remember that we assume $b(A) = 0$ as the sender A cannot detect C's transmissions. In order to compute the throughput of flow f_{CD} we observe that node C will receive a RRTS packet from node B after the expiration of EIFS followed by the backoff phase. C will then set its NAV timer and suspends its activity allowing A's transmission to complete successfully. The duration of this phase, T_b, is equal to:

$$T_b = T_s - RTS - RRTS \tag{10}$$

The probability, $b(C)$, that node C detects the channel busy can be computed taking into account that $T_P(A)$, can also be expressed as [8]:

$$T_P(A) = \frac{[1-\tau(B)]\, b}{\tau(B)T_s + (1-\tau(B))\,(1-b)\,\sigma + (1-\tau(B))\, bT_b} \tag{11}$$

Solving eq. (11) in the variable b and then using this value and T_b obtained in eq. (4), we can achieve the throughput of flow f_{CD}. Table 1 summarizes the values of the parameters used to obtain our numerical results in the analytical model as well as in the simulations.

A parameter which plays an important role in the analytical model described above is the length of EIFS. In our approach we use EIFS not only as defined in the 802.11 DCF standard, but also such as a period of time the receiver, B, has to wait before to send the RRTS after a collision of an RTS has been detected such as illustrated in Section III. The value of EIFS can be cause of starvation, for this reason we have chosen a value of EIFS in order to obtain a value of throughput equal for both connections, which we call *fair* value of throughput. Figure 5 shows a plot of throughput achieved by flows f_{AB}

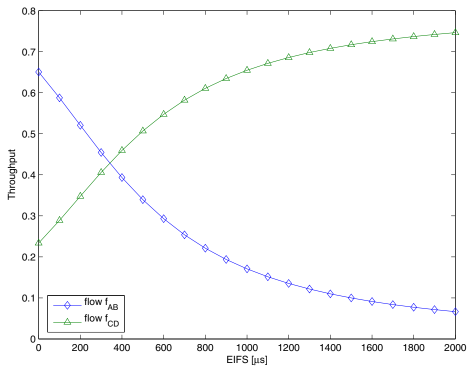


Fig. 5. Throughput of flows f_{AB} and f_{CD} vs. length of EIFS.

	802.11	CSMA/CARD
$p(A)$	0.9364	0.5602
$T_P(A)$	0.0093	0.4170
$T_P(C)$	0.7961	0.4385

TABLE II

COLLISION PROBABILITY AND THROUGHPUT ACHIEVED IN INFORMATION ASYMMETRY SCENARIO.

and f_{CD} when our approach of RRTS with collision detection is applied. The value of throughput has been calculated using the analytical framework discussed before. Varying the length of EIFS in the range $[0, 2000]\mu s$, we observe that, as expected, for low values of EIFS duraton, f_{AB} achieves an higher throughput if compared to f_{CD}, this is due to the fact that both flows are backlogged and if EIFS is short, flow f_{AB} captures the channel every time it sends an RTS and starves flow f_{CD}. Instead, for high values of EIFS, the asymmetry between the flows increases, resulting in the same starvation obtained using the 802.11 approach in this scenario. We have observed from Figure 5 that in the scenario considered, an optimal value of EIFS is 342 μs.

Now, we can compare the value of the parameters calculated using the CSMA/CARD mechanism and those obtained considering a previous analytical model of the classical 802.11 DCF approach [8]. The model considered has been developed according to the same rules we followed in this paragraph. Remember that, using 802.11 DCF, node A, for each cycle, can transmit only during the short gap G showed in Figure 4(a), when node C is idle, and this results in a very low probability to access the channel. In Table 2 we have reported the value of the conditional collision probability $p(A)$, and the throughput of node A and C, respectively $T_P(A)$ and $T_P(C)$ in both cases examined. The analytical results show that the collision probability evaluated for node A using the 802.11 DCF protocol is almost 1, it means that the flow f_{AB} is starved while, using the CSMA/CARD approach, this value of collision probability drops down to about 50% and the value of throughput calculated for flow f_{AB} is almost the same of that evaluated for f_{CD}. We can say that using CSMA/CARD

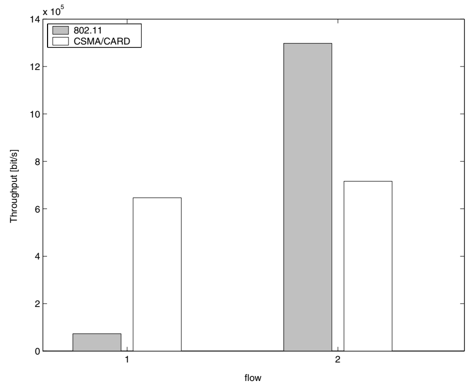


Fig. 6. Throughput of flow f_{AB} and flow f_{CD} in the Asymmetric Flows scenario.

we can mitigate starvation due to information asymmetry in a simple configuration such as the Figure 2(b).

In the next section we will show some simulation results obtained applying our approach in more general cases.

VI. SIMULATION RESULTS

We consider only the non-adaptive version of the CSMA/CARD in our experiments, and we simulate using the ns-2 platform. Each simulation was run for 200 seconds after a 10-second warm-up period where backlogged traffic conditions were assumed. We start by validating our model in Section V on the information asymmetry scenario after which we evaluate our protocol in random topologies. In all the simulations we suppose both *sensing range* and *transmission range* equal to 250 m and there are no power capture effects. Similar results can be obtained when sensing range is greater that transmission range and the capture effect is taken into account.

A. Information Asymmetry Scenario

We describe here the results obtained in the scenario depicted in Figure 2(b). Figure 6 shows the throughput measured for both flows where flow 1 indicates flow f_{AB} and flow 2 corresponds to flow f_{CD}. As expected and already shown in previous works, flow f_{AB} is almost starved when the 802.11 DCF protocol has been used. Our simulation results also validate the results obtained through the analytical model described in Section V where the throughput value for both flows are almost the same with CSMA/CARD. Note that we have used in the simulations the value of EIFS calculated in Section V.

B. Random Scenario

In this paragraph we consider two different topologies where the nodes are deployed in a random way while the node density is varied. In each simulation, half the nodes are transmitters and the other half are receivers. Each node chooses a node within its transmission range and attempts to transmit to this node during all the simulation runs. Plotted results are obtained after averaging the results obtained in 10 different runs for the same topology. In order to reduce the number of collisions that can be caused by the RRTS mechanism, we show the results obtained considering a probabilistic approach when sending the RRTS packets. In particular, a potential receiver sends the RRTS packet with a fixed probability p_S after it detects a collision.

1) Topology 1: we consider a sparse topology where 50 nodes are randomly distributed inside an area of 2000 m x 2000 m. Figure 7 shows the node distribution in the area considered. Note that all nodes have at least one neighbor and that channel contention, hidden terminals, information asymmetry effects are present. In order to show how the proposed approach outperforms the classical 802.11, we have considered a performance measure already used in [8], called "flow preference graph". As shown in Figure 8 we report the difference in throughput achieved with CSMA/CARD and 802.11 for each individual flow. In Figure 8 these differences are plotted for different values of RRTS sending probability, p_S, and sorted in descending order. This measure shows the number of flows that reach a largest throughput with respect to the other. This parameter is a good measure of how well CSMA/CARD performs and shows when the proposed protocol outperforms 802.11. We observe that, when p_S is equal to 10% and 20%, all the values of difference in throughput remain in the positive region of the graph, meaning that all the flows achieve higher throughput with CSMA/CARD. However, when p_S is equal to 50% and 100%, some flows reach lower throughput as opposed to 802.11. This behavior indicates that when p_S is high enough, there can be potentially situations where the performance is rendered worse, even if the number of flows with higher throughput is more. Another parameter we have considered is the value of minimum throughput vs. the sending probability, shown in Figure 9. For all the values of p_S considered, the minimum throughput with CSMA/CARD reaches high values if compared to 802.11. This shows that CSMA/CARD is successful in alleviating the starvation problem as well.

2) Topology 2: We now evaluate the performance of CSMA/CARD in the dense topology shown in Figure 10. The same number of nodes as in topology 1 is used, but the area is reduced to 1000 m x 1000 m. As illustrated in Figure 11, CSMA/CARD does not always provide better results than 802.11. In particular, for high p_S values, the number of flows which throughput is reduced can be very high due to the collisions introduced by the RRTS packets. On the other hand, when p_S is equal to 10% and 20%, CSMA/CARD outperforms 802.11 in terms of the number of flows with higher throughput. Similar results, when using the minimum throughput as the performance metric, are shown in Figure 12.

VII. Conclusion

In this paper a new mechanism, called CSMA/CARD has been introduced. This solution is based on a novel receiver-initiated mechanism which exploits some information at the physical level. More specifically, collision sensed by the receiver can be used to predict whether some sender attempted to initiate a transmission towards this receiver. Using this information, the receiver can initiate an action to help expedite the handshake mechanism and to avoid the starvation of some flows. A simple analytical model of the proposed protocol has been developed, and we have shown that CSMA/CARD can almost achieve perfect fairness in the known information asymmetry scenario. The mechanism has been evaluated jointly with IEEE 802.11 DCF protocol through ns-2 simulations in the information asymmetry scenario and other experiments have been carried out in more general topologies. The results obtained show that the mechanism proposed, highly alleviates the problem of starvation in all the scenarios considered. Moreover, we have observed that tuning the number of RRTS sent is a key factor in order to obtain better performance.

Acknowledgment

The authors would like to thank Ahmad Khoshnevis for his precious help in this work.

References

[1] B. Bensaou, Y. Wang, and C. C. Ko, "Fair Medium Access in 802.11 Based Wireless Ad-Hoc Networks." *Proc. of IEEE/ACM International Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc '00)*, Boston, MA, August 2000.

[2] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang. "MACAW: a Media Access Protocol for Wireless LAN's." *Proc. of SIGCOMM '94*, London, UK, September 1994.

[3] G. Bianchi. "Performance Analysis of the IEEE 802.11 Distributed Coordination Function." *IEEE Journal on Selected Areas in Communications*, 18(3):535-547, March 2000.

[4] J. Boer et al. "Wireless LAN with Enhanced Capture Provision" U.S. Patent 5987033. Technical Report, 1999.

[5] M. Cesana, D. Maniezzo, P. Bergamo, M. Gerla, "Interference Aware (IA) MAC: an Enhancement to IEEE802.11b DCF." *Proc. of IEEE Vehicular Technology Conference (VTC '03)*, Orlando, Florida, USA, October 2003.

[6] K. Christensen, "Performance Evaluation of the Binary Logarithmic Arbitration Method (BLAM)," *Proc. of 21st Conference on Local Computer Networks (LCN '96)*, Minneapolis, MN, October 1996.

[7] M. Garetto, T. Salonidis, and E. Knightly. "Modeling Per-flow Throughput And Capturing Starvation in CSMA Multi-hop Wireless Networks." *Proc. of IEEE INFOCOM 2006*, Barcelona, Spain, April 2006.

[8] M. Garetto, J. Shi, and E. Knightly. "Modeling Media Access in Embedded Two-Flow Topologies of Multi-hop Wireless Networks." *Proc. of ACM MobiCom*, Cologne, Germany, August 2005.

[9] J. J. Garcia-Luna-Aceves and A. Tzamaloukas, "Receiver-initiated Collision Avoidance in Wireless Networks." *ACM Wireless Networks,* vol. 8, pp. 249-263, 2002.

[10] P. Karn, "MACA - A New Channel Access Method for Packet Radio." *ARRL/CRRL Amateur Radio 9th Computer Networking Conference,* pp. 134-40, ARRL, 1990.

[11] Steven M. Kay, "Fundamentals of Statistical Signal Processing - Detection Theory." *Prentice-Hall*, 1998.

[12] L. Kleinrock and F. A. Tobagi, "Packet Switching in Radio Channels." *IEEE Transactions on Communication.* vol. 23, issue no. 12, pp. 1400-1416, 1975.

[13] W. F. Lo and H. T. Mouftah, "Carrier Sense Multiple Access with Collision Detection for Radio Channels." *Proc. of IEEE 13th International Communication and Energy Conference*, pp. 244-47, IEEE, 1984.

[14] J.P. Monks, V. Bharghavan, W.-M.W. Hwu, "A Power Controlled Multiple Access Protocol for Wireless Packet Networks," *Proc. of INFOCOM'01*, Anchorage, Alaska, April 2001.

[15] R. Rom, "Collision Detection in Radio Channels, in Local Area and Multiple Access Networks." *Computer Science Press*, pp. 235-49, 1986.

[16] F. Talucci and M. Gerla, "MACA-BI (MACA by Invitation): A Receiver Oriented Access Protocol for Wireless Multihop Networks." *Proc. of PIMRC'97*, Oulu, Finland, September 1997.

[17] P802.11 - Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications, IEEE, January 1996.

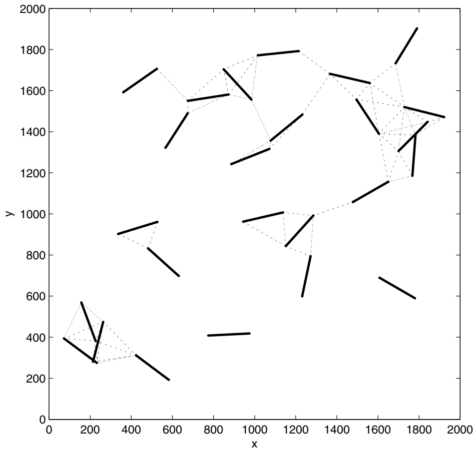


Fig. 7. Topology 1: 50 nodes in 2000 m x 2000 m scenario.

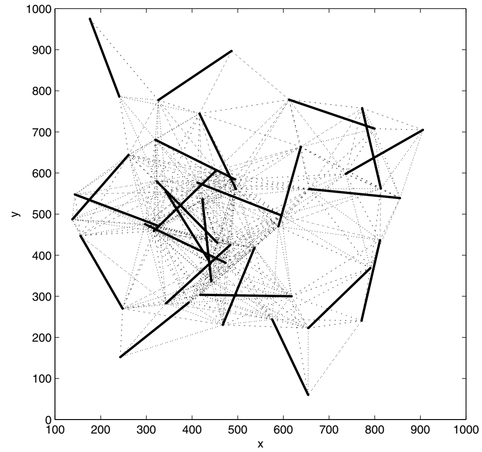


Fig. 10. Topology 2: 50 nodes in 1000 m x 1000 m scenario.

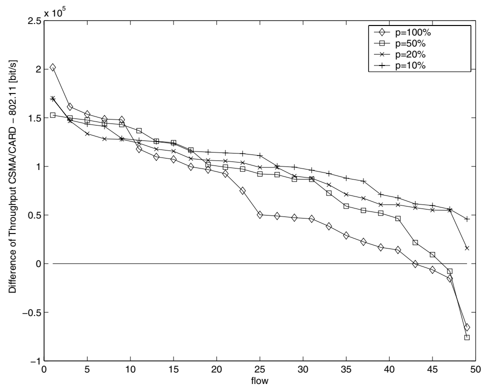


Fig. 8. Throughput difference for different values of RRTS sending probability, p_S, in topology 1.

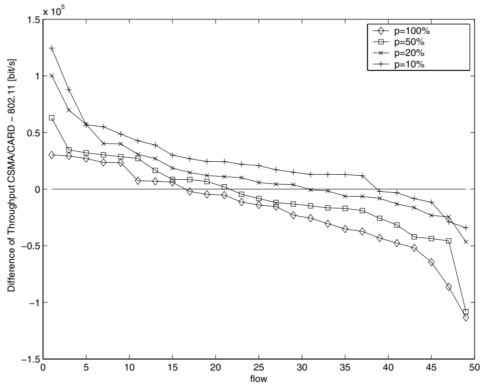


Fig. 11. Throughput difference for different values of RRTS sending probability, p_S, in topology 2.

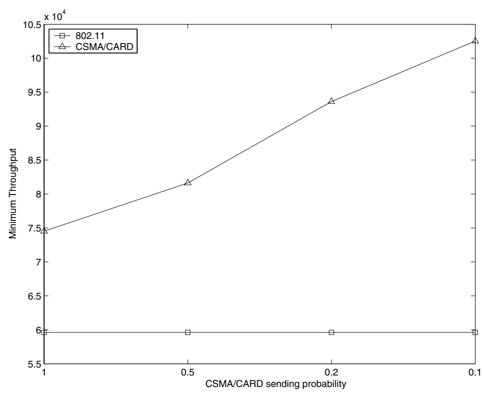


Fig. 9. Minimum throughput vs. RRTS sending probability, p_S, for CSMA/CARD and 802.11 in topology 1.

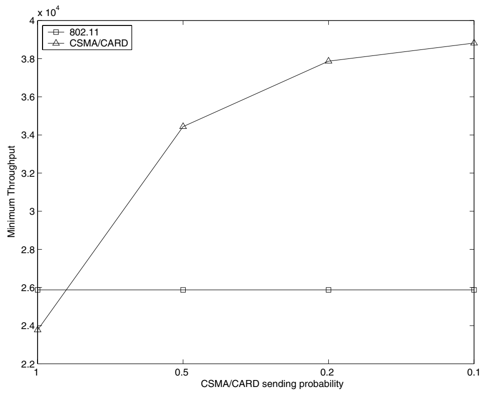


Fig. 12. Minimum throughput vs. RRTS sending probability, p_S, for CSMA/CARD and 802.11 in topology 2.