17

Medium Access Control in Distributed Wireless Networks

Jun Peng
University of Texas - Pan American, Edinburg, Texas
United States of America

1. Introduction

Medium access control (MAC) is a fundamental and challenging problem in networking. This problem is at the data link layer which interfaces the physical layer and the upper layers. A solution to this problem in a particular network thus needs to factor in the characteristics of the physical layer and the upper layers, which makes the MAC problem both a challenging and evolving problem. Medium access control in distributed wireless networks is one of the most active research areas in networking because distributed wireless networks are diverse and evolving fast.

One of the most well-known problem in medium access control in distributed wireless networks is the hidden terminal problem. Hidden terminals are interesting but problematic phenomena in distributed wireless networks. Basically, even if two nodes in a wireless network cannot sense each other, they may still cause collisions at the receiver of each other (1). If the hidden terminal problem is not well addressed, a wireless network may have a significantly degraded performance in every aspect, since frequent packet collisions consume all types of network resources such as energy, bandwidth, and computing power but generate no useful output.

There are basically two existing approaches to the hidden terminal problem. One is the use of an out-of-band control channel for signaling a busy data channel when a packet is in the air (2; 3; 4; 5). This approach is effective in dealing with hidden terminals but requires an additional control channel. The more popular approach to the hidden terminal problem is the use of in-band control frames for reserving the medium before a packet is transmitted (6; 7; 8; 9; 10). The popular IEEE 802.11 standard (11) uses this approach in its distributed coordination function (DCF).

Basically, before an IEEE 802.11 node in the DCF mode transmits a packet to another node, it first sends out a Request to Send (RTS) frame after proper backoffs and deferrals. If the receiver successfully receives the RTS frame and the channel is clear, the receiver responds with a Clear to Send (CTS) frame, which includes a Duration field informing its neighbors to back off during the specified period. In an ideal case, the hidden terminals of the initiating sender will successfully receive the CTS frame and thus not initiate new transmissions when the packet is being transmitted.

However, control frames have limited effectiveness in dealing with hidden terminals because they may not be able to reach all the intended receivers due to signal attenuation, fading, or interference (12). In addition, control frames have considerably long airtimes

Source: Communications and Networking, Book edited by: Jun Peng,
ISBN 978-953-307-114-5, pp. 434, September 2010, Sciyo, Croatia, downloaded from SCIYO.COM

because they are recommended to be transmitted at the basic link rate in both narrow-band and broadband IEEE 802.11 systems. Moreover, they have relatively long physical layer preambles and headers. In-band control frames therefore introduce significant network overhead, even though they do not use an out-of-band control channel.

This article introduces a new approach of *bit-free* control frames to addressing the disadvantages of the traditional control frames. Basically, with the new approach, control information is carried by the *airtimes* instead of the *bits* of control frames. The airtime of a frame is robust against interference and channel effects. In addition, a bit-free control frame carries no meaningful bits so that no preamble or header is needed for it (Section 6 presents a fundamental view on bit-free control frames).

In investigating the performance of the new approach, we have first analyzed the potential performance gains of the IEEE 802.11 DCF if its traditional control frames are replaced by bit-free control frames. We have then modified the original protocol with the new approach of bit-free control frames and done extensive simulations. Our investigation has shown that the modified protocol improves the average throughput of a wireless network from fifteen percent to more than one hundred percent.

The rest of this article is organized as follows. Section 2 introduces our observations and analysis. Section 3 presents our modifications to the IEEE 802.11 DCF. We then show in Section 4 the comprehensive simulation results comparing the modified protocol to the original one. We introduce the related work in Section 5 and a fundamental view on the presented approach in Section 6. Finally, we give our conclusions in Section 7.

2. Observations and analysis

Our first observation is that the CTS frame of an IEEE 802.11 node may not be able to reach all the hidden terminals of the initiating sender, which was also studied in some related work such as (12). One source of the problem is that recovering the bits in a frame is a delicate process so that to corrupt a frame being received by a node is usually much easier than to correctly receive a frame from the same node. In general, if a node is receiving a frame at the power level L, then another node may corrupt the frame by generating a power of level l at the receiver in the channel that is several times lower than L. In particular, when $\frac{L}{l}$ is lower than the "capture" power ratio threshold, then the frame will be corrupted.

An example is shown in Fig. 1. We assume in the example that the network is a homogeneous network, which means that all the nodes are the same in terms of parameters such as transmission power and receive/carrier sense power thresholds. We also assume that the signal power deteriorates at a rate of $(\frac{1}{d})^4$ where d is the propagation distance (i.e., the receiver is beyond the crossover distance from the sender), the carrier sense range of a node is twice of its transmission range r, and the capture power ratio threshold is 10, as used as the default settings in ns-2 and in some other studies (12). Under these assumptions, node C shown in Fig. 1 is a hidden terminal to node A. Meanwhile, node C cannot correctly receive a frame from node B, since it is out of node B's transmission range. However, node C can still corrupt a frame at node B that is from node A. Therefore, node C is a hidden terminal of node A that cannot be addressed by the CTS control frame sent by node B. Actually, all nodes falling into the closed region enclosing node C are hidden terminals of node A that cannot be addressed by the CTS frames of node B.

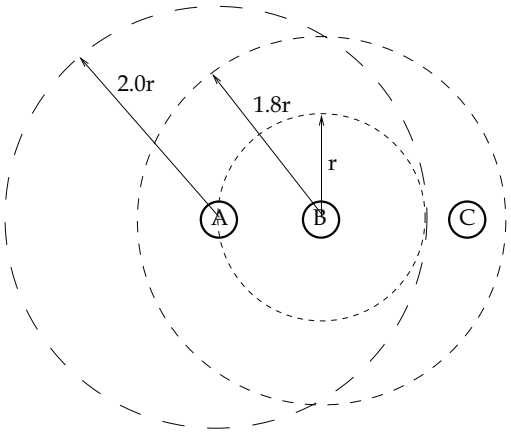


Fig. 1. A Case of a Failed CTS Frame for Reserving the Medium

Besides their limited effectiveness in dealing with hidden terminals, the control frames of IEEE 802.11 DCF also introduce significant overhead. There are two factors increasing the overhead. First, the control frames are recommended in both narrow-band and broadband IEEE 802.11 systems to be transmitted at the basic link rate for rate compatibility among competing nodes, which makes the bits in a control frame "flow" relatively slowly. Second, a bit-based frame, whatever the number of payload bits in it, needs a physical layer preamble and header for successful bit delivery.

As specified in IEEE 802.11, a DSSS (Direct Sequence Spread Spectrum) physical layer introduces 192-bit overhead (144-bit preamble plus 48-bit header) to each frame, while a FHSS (Frequency-Hopping Spread Spectrum) physical layer has an overhead of 128 bits (96-bit preamble plus 32-bit header). In the DSSS case, a RTS frame only uses 36% of its air time for delivering specific MAC information. It is even worse for a CTS frame, for which the percentage is 26%. The situation is relatively better in the FHSS case. The percentages are, however, still low at 44% and 33% for a RTS frame and a CTS frame, respectively.

We may use some analysis to demonstrate how a protocol that overcomes the two disadvantages of the IEEE 802.11 DCF may decrease the control overhead and thus improve the throughput of a network. After proper deferrals and backoffs, an IEEE 802.11 sender in the DCF mode starts to transmit the RTS frame. With a probability of p_c, however, the RTS frame may encounter a contention collision because another contending sender may have drawn a similar backoff delay. Even if there is no contention collision, the RTS frame may still face a collision later because of the possible existence of hidden terminals. We may assume the probability of such a collision as p_h. Therefore, a RTS frame with a transmission time of t_{rts} consumes a medium time of

$$T_{rts} = \frac{1}{(1-p_c)\times(1-p_h)} \times (T_{bo} + t_{rts}) \quad (1)$$

before it is successfully received by the intended receiver, where T_{bo} is the average backoff time in a contention and the interframe space times are considered as negligible.

If the RTS frame is successfully received by the intended receiver, we may assume that the CTS frame will not have a collision at the initiating sender, considering that the RTS frame

has already reserved the medium around the initiating sender. However, there is still a probability of $f \times p_h$ (f is the hidden terminal residual factor of DCF and $f \leq 1$) that the data packet may encounter a collision because some hidden terminals of the initiating sender may have failed to receive the CTS frame, as explained earlier. When the data packet has a collision, the RTS/CTS/Data process needs to be repeated. If we denote the transmission time of a CTS frame and of an ACK frame by t_{cts} and t_{ack}, respectively, then the medium time consumed for delivering a data packet and all its retransmissions is as follows

$$T = \frac{1}{1 - f \times p_h} \times (T_{rts} + t_{cts} + t_{data}) + t_{ack}. \tag{2}$$

We also assume here that the ACK may not have a collision, as in the CTS frame case.

The average time for successfully sending a packet will be decreased if the 802.11 DCF is modified with the new approach of bit-free control frames. We may use $\frac{1}{r}$ ($r < 1$) to denote the improvement factor of the effectiveness of the control frames in reducing the probability of collisions caused by hidden terminals. We may also denote the length reduction factor for the control frames by v($v < 1$). Then, the medium time needed for successfully sending a RTS frame with the modified protocol is

$$T'_{rts} = \frac{1}{(1 - p_c) \times (1 - p_h)} \times (T_{bo} + v \times t_{rts}), \tag{3}$$

and the time for successfully sending a packet in such a case is

$$T' = \frac{1}{1 - r \times f \times p_h} \times (T'_{rts} + v \times t_{cts} + t_{data}) + v \times t_{ack}. \tag{4}$$

We now show by an example how the modified protocol with bit-free control frames may reduce the control overhead and thus increase the throughput of a network. For easy reference, we named the modified MAC protocol as CSMA/FP, which denotes Carrier Sense Multiple Access with Frame Pulses (bit-free frames may be regarded as a type of in-band pulses). In the example, the network has a DSSS physical layer, the control and data frames are transmitted at 1 Mb/s and 2 Mb/s, respectively, and each packet has a size of 512 bytes. In addition, p_h assumes a value of 0.2, which means that a frame without medium reservation has a probability of 0.2 to encounter a collision caused by hidden terminals. The hidden terminal residue factor f assumes a value of 0.2 for the IEEE 802.11 DCF in the example. T_{bo} takes the value of 2 *ms* for a high network load case, which is a typical value shown by our simulation results in Section 4. Finally, r and v assume values of 2 and 0.4, respectively, in the example.

Fig. 2 shows the average medium time consumed for successfully delivering a packet with the two protocols in our example as the probability of a contention collision on a frame increases (i.e., as the number of nodes and/or the traffic load increase in the network[1]). As shown in the figure, the performance gains of CSMA/FP over IEEE 802.11 DCF may be more than ten percent in our example.

[1] Although these factors may also affect p_h, we assign p_h a fixed value for the simplicity of demonstration.

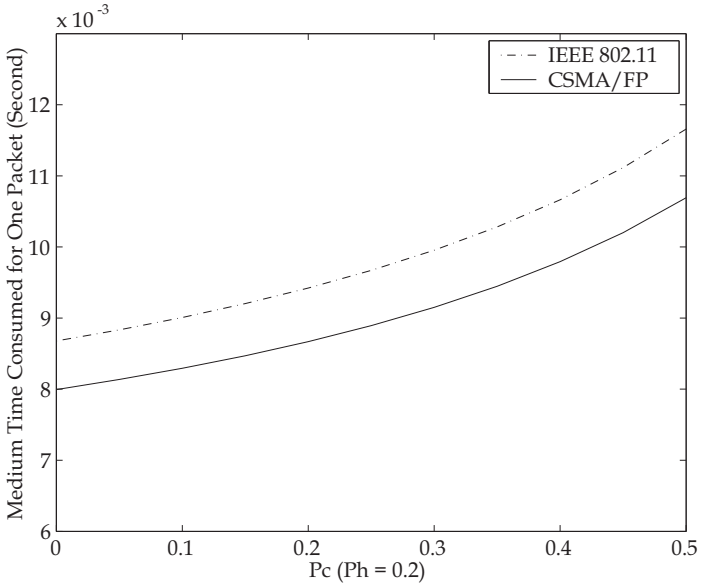


Fig. 2. Performance Analysis and Comparison

These numerical results in our example may not reflect what happens exactly in reality, since some heuristic assumptions have been made in the analysis. However, these results demonstrate the potential to considerably improve the performance of the IEEE 802.11 DCF by enhancing its capability of dealing with hidden terminals as well as shortening its control frames.

3. Applying the new approach

3.1 Basics

The challenge in applying the new approach to the IEEE 802.11 DCF is the limited capacity of the bit-free control frames in carrying control information. Particularly, only the airtime of a control frame can carry control information. To address this issue, we use two basic strategies. One is that the bit-free control frames only carry the *indispensable* information for medium access control, while the other is to use frame *pairs* for backoff duration control.

For sending bit-free control frames, we assume that the IEEE 802.11 hardware has some modification so that it can be commanded to transmit the carrier for a specified amount of time. We also assume that the airtime of a control frame can be recorded with a degree of accuracy depending on the hardware, bandwidth, and channel conditions. One protocol parameter, the minimum guard gap between the lengths of two control frames, may be adjusted based on the recording accuracy. In fact, with its carrier sense capability, the existing IEEE 802.11 hardware may record the airtime of an incoming frame.

In addition, a bit-free control frame cannot be mistaken as a bit-based frame, since a bit-free frame does not include a physical layer preamble and thus the synchronization on the frame cannot be done. A bit-based frame, however, may be mistaken as a bit-free frame if the synchronization on the frame fails. This kind of interference is usually filtered out due to the typically long airtime of a bit-based frame and the short airtime of a bit-free control frame.

3.2 Bit-free control frames

The frame type needs to be specified for each frame so that the receiver knows how to interpret the bits in the bit-based frame case or the frame airtime in the bit-free frame case. Bit-free frames carry no meaningful bits so that the frame type information can only be delivered by their airtimes. Particularly, if the airtime of a bit-free frame falls into a specified range or ranges, then the frame belongs to the type of frame denoted by the range or ranges.

Besides the frame type information, the other indispensable information in a RTS frame is the address of the receiver. The length of a bit-free RTS frame needs to fall into the designated range or ranges. We therefore may not be able to encode the address information of each single receiver into the airtime of a bit-free RTS frame. To address this problem, we apply a "Mod-n" calculation on each receiver address before it is encoded. Basically, we first divide the address by n and then encode the remainder into the frame airtime. Particularly,

$$\text{If } r = Mod(RA,n), \text{ then } F_L = RTS(r)$$

where RA is the receiver address, n is an integer, r is the remainder, F_L is the airtime of the bit-free RTS frame to send, and $RTS(r)$ is an r-indexed element in the set of RTS lengths in *microseconds*.

The Duration field in a bit-based RTS frame is also important because it specifies the period during which a receiver of the frame should back off. A bit-free RTS frame does not have the capacity for the duration information. Instead, a receiver of a bit-free RTS frame starts to back off upon receiving the frame and ends the backoff only after the medium has been sensed idle for a specified amount of time (more details later).

In our proposed design with bit-free frames, all CTS frames have the same fixed length that distinguishes them from other bit-free frames. In addition, we use control frame pairs to communicate the backoff duration information of a traditional CTS frame, which will be introduced later. Similarly, all bit-free ACK frames in our design have the same fixed length that distinguishes them from other types of bit-free frames (the address issue of these frames is discussed in Section 3.5).

In addition to the RTS, CTS, and ACK bit-free frames, we add another type of bit-free control frame named CTS-Fail frame in our design. A CTS-Fail frame has a fixed length and is sent by a CTS frame sender in two cases to notify other nodes to end their backoff. The first case is that a CTS frame sender does not receive any packet after sending the CTS frame. The second case is that a CTS frame sender receives a packet after sending the CTS frame but finds that either the packet is not intended for it or the packet has errors.

3.3 Frames working together

To explain how the four types of bit-free control frames work together in the modified IEEE 802.11 DCF, we describe how a node contends for the medium when it has a packet to transmit. The IEEE 802.11 DCF is basically a CSMA/CA protocol, and our modifications to the protocol are only on the CA part.

When a node has a packet to transmit, it starts to listen to the channel. If the channel has been found idle for a period of time longer than the DCF Interframe Space (DIFS), the node starts a random backoff timer whose value is uniformly drawn from the node's contention window (CW). If the node detects no carrier before its backoff timer expires, it proceeds to transmit the bit-free RTS frame upon the expiration of its backoff timer. Otherwise, the node backs off.

As soon as the backoff timer of the node expires, the node starts to transmit the bit-free RTS frame. As explained earlier, the airtime of the bit-free frame is determined by the address of the intended receiver. After finishing the transmission, the node waits for a bit-free CTS frame, whose airtime is fixed and known.

After a neighbor of the initiating sender receives the bit-free RTS frame, it does the "Modn" calculation on its own address and compares the remainder to the length of the received frame in microseconds. If the remainder matches the length, the neighbor sends out a bit-free CTS frame and then waits for a packet. If the CTS frame sender does not receive any packet after a period of SIFS (Short Interframe Space) plus propagation delays, it sends out a CTS-Fail frame. On the other hand, if the remainder does not match the length of the received RTS frame, the neighbor will enter backoff and remain in backoff until the medium has been sensed idle for a period of time that is SIFS plus either the CTS frame length or the ACK frame length, whichever is longer.

After the initiating sender obtains the bit-free CTS frame, it waits for SIFS and then starts to transmit the packet. If for any reason the RTS frame sender fails to obtain the expected CTS frame, the sender starts over to contend for the medium. In such a case, the sender doubles its CW. On the other hand, if a node receives an unexpected bit-free CTS frame (i.e., the node is not a RTS frame sender), the node increases its CTS frame counter Num_{cts} by one, starts a backoff monitor timer, and then enters backoff. Such a node exits backoff in two cases. One is that its CTS frame counter Num_{cts} reaches zero when the node decrements the counter by one after receiving an ACK or CTS-Fail frame (the backoff monitor timer is canceled in such a case), while the other is that its backoff monitor timer expires (more details later).

After the initiating sender succeeds in contending for the medium, receives the expected CTS frame, and fully transmits the packet, it expects a bit-free ACK frame from the receiver. If the sender does not obtain the expected acknowledgment, it doubles its CW and starts to monitor the channel again for a retransmission.

On the other hand, after a node receives the data packet, it checks if the packet is intended for it and free of error. If so, the node sends back a bit-free ACK frame. If the packet is not intended for it or the packet has errors, the node checks whether it has sent a CTS frame for the packet. If so, the node sends out a CTS-Fail frame to notify its neighbors to exit backoff.

The whole process repeats until the initiating sender obtains an acknowledgment for the packet or the retry limit is reached. The node discards the packet in the latter case and resets its CW to the minimum size in both cases.

3.4 Some design considerations

The first design consideration on the modified MAC protocol is the choices of receive power thresholds for its bit-free control frames. Unlike bit-based frames, bit-free control frames can be correctly received as long as they can be sensed. The receive power threshold for a bit-free control frame may thus be adjusted for controlling the transmission range of the frame. As introduced earlier, a bit-based CTS frame may not successfully reach all the hidden terminals of the initiating sender (12). A node with the modified protocol, therefore, needs a lower receive power threshold for bit-free control frames.

The lowest power threshold that a node may use for receiving a bit-free control frame is the carrier sense power threshold. In such a case, a node decodes a bit-free frame if the frame can be sensed. The implementation in our simulations uses this conservative choice to

ensure the coverage of bit-free control frames. However, there is an exception. When a node receives a bit-free RTS frame matching its address, the node responds with a CTS frame only if the received power of the RTS frame is above the receive power threshold for data frames, since the node should not respond if it cannot correctly receive a packet from the other node.
Another design consideration on bit-free control frames is the set of lengths in terms of airtimes that the frames should use. The basic rule is that control frames should be easy to detect and distinguish from one another. The shortest control frame in our simulations is $20\mu_s$ and the minimum guard gap between two lengths in the set is $5\mu_s$, which corresponds to 5-bit airtime at the transmission rate of 1Mb/s (even in broadband systems such as 802.11g, the control frames are recommended to be transmitted at the basic link rate). In reality, the minimum guard gap should be set based on the length detection accuracy of bit-free frames, which may be affected by the hardware, bandwidth, and channel conditions.
When choosing the length for a specific control frame that has a fixed length, we need to consider another factor. In particular, when multiple bit-free frames arrive at the same node in the same time segment, they may forma "merged" bit-free frame that has a length denoting another defined bit-free control frame. This kind of false control frame may appear when the merged frame has a longer airtime than any individual merging frame, as demonstrated by Case 3 in Fig. 3.
The possible adverse effects of the phenomenon of merged frames are alleviated by the discrete lengths of the defined control frames and the strict timelines for receiving CTS and ACK control frames. Particularly, only when a merged frame matches a defined bit-free control frame, would it possibly cause some harm. Moreover, for such control frames as CTS and ACK, a false frame may be harmful only if it emerges in the right timeline and at the right node.
However, we may still further address the merged frame phenomenon by carefully choosing the lengths for the fixed-length control frames. We have three types of fixed-length control frames, which are CTS, ACK, and CTS-Fail. Among them, a false CTS frame would arguably generate the worst scenario, in which the nodes receiving the false frame enter backoff and wait for a non-existing ACK or CTS-Fail frame for exiting backoff. Therefore, to avoid false CTS frames generated by merging frames, we need to assign a CTS frame the shortest length in the chosen length set for control frames.

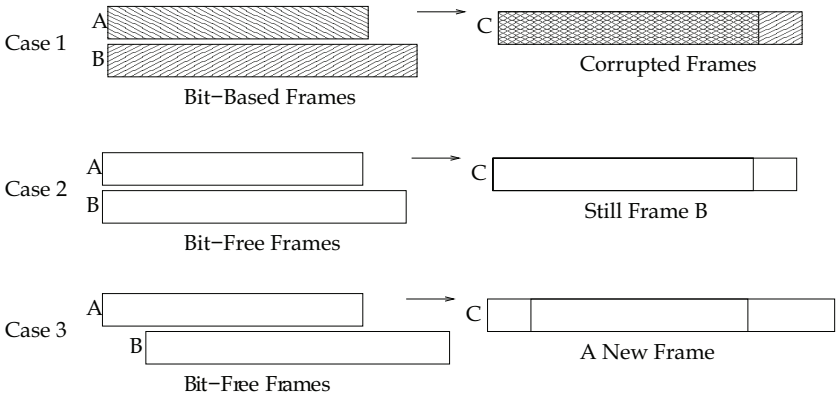


Fig. 3. Merging of Control Frames.

What happens if a false CTS frame emerges anyway due to such a reason as environmental noise? A backoff monitor timer is used to address this problem. When a node receives a CTS frame, it starts a backoff monitor timer before it enters backoff. The backoff monitor timer is set to a value T_m that is the transmission time of the largest allowable frame in the network. The node exits backoff anyway when its back off monitor timer expires. Additionally, a backoff monitor timer also solves the problem of lost ACK or CTS-Fail frames due to interference or failed nodes.

In addition, it needs some extra caution to receive a CTS frame. A RTS frame may be interpreted by two or more nodes as being intended for them due to the "Mod-n" calculation design and thus two or more bit-free CTS frames may be generated for a single RTS frame. The consequence in such a case is that the received CTS frame may be slightly longer than usual because of the various propagation delays between the RTS frame sender and its receivers (besides, the medium may be reserved in a larger space than necessary for the transmitter in such a case). A degree of tolerance on length variation is therefore needed for decoding a CTS frame. Particularly, if we denote the transmission distance of a node by d_{tx} and the signal propagation speed by c, then the decoding tolerance δ on the length of a CTS frame should be

$$\delta = 2 \times \frac{d_{tx}}{c}. \tag{5}$$

Finally, a bit-free ACK frame needs to have a longer length than a bit-free CTS-Fail frame. This is because a data frame may have one or more CTS-Fail responses besides the ACK response. In such a case, a sender still needs to recognize the ACK frame even if it is accompanied by CTS-Fail frames.

3.5 More design issues on bit-free control frames

As explained earlier, bit-free control frames have two advantages over bit-based control frames. One is that bit-free control frames are robust against interference and channel effects, and the other is that they can be very short. However, bit-free control frames have disadvantages too. One is that two or more bit-free control frames may merge at a node and form a new, false control frame. The second disadvantage of bit-free control frames is that they carry no specific address information so that they may be interpreted by any receiver as legitimate. One basic observation is that when an initiating sender is expecting a CTS or ACK frame, it has already notified its neighbors except the intended receiver to backoff. Therefore, an initiating sender may only receive a CTS or ACK frame from the intended receiver in a general case. Moreover, an initiating sender sets a strict timeline for receiving a CTS or ACK frame. For these two reasons, an initiating sender can hardly receive a false and harmful CTS or ACK frame, which makes the lack of address information in the CTS and ACK frames almost harmless. This is the reason why we choose bit-free ACK frames instead of the traditional, bit-based ACK frames in our design.

There is a special case to consider, which is that two senders may start to transmit their RTS frames almost at the same time. If the two nodes can hear each other, there is usually no harm. This is because in such a case the sender with a shorter RTS frame will finishes its RTS frame transmission earlier and thus detect the other sender. If the two senders cannot hear each other, there may exist a harmful situation in which one sender overhears the CTS frame intended for the other sender and mistakenly starts to transmit its packet. This kind of

harmful situation occurs, however, with low probabilities because two senders with different RTS frames have different timelines for receiving their CTS frames.
RTS and CTS-Fail frames are more sensitive to false frames because they have no strict receive timelines. However, several factors greatly lower the possibility of harmful false RTS and CTS-Fail frames. First, neighboring nodes cannot generate false frames. Two neighboring nodes may transmit in the same time segment only if they start to transmit at almost the same time so that none of them hears the other. In such a case, the longer frame will "hide" the shorter one, as illustrated by Case 2 in Fig. 3. Second, control frames have designated lengths so that a false frame is harmful only if it has a matching length. Thirdly, not all false control frames can cause significant harm. For example, if a false RTS frame does not form at a node having a matching address, there is no harm.
In summary, the disadvantages of bit-free control frames are greatly alleviated by the following factors. First, false control frames may be few in the network because of the discrete lengths of the defined control frames. Secondly, only if false control frames form at the right node and possibly at the right time, do they cause harm. Finally, when a sender is expecting a CTS or ACK frame, its neighbors except the intended receiver have already been in backoff in general.

4. Scheme evaluations

We have done extensive simulations with ns-2 (13) to investigate the performance of the modified IEEE 802.11 DCF (named as CSMA/FP for easy reference) and compare it to the original protocol. As mentioned earlier, we have only modified the collision avoidance (CA) part of the original protocol by applying the proposed bit-free control frame approach, while other parts of the original protocol have been kept unchanged.

4.1 Configuration details

We have first evaluated CSMA/FP in a wireless LAN with saturation traffic and compared it to the original protocol. We have then used a more general scenario of a multihop ad hoc network to investigate its performance. Particularly, we evaluated the protocols from the perspective of an individual user in the ad hoc network.
From an individual user's perspective, a network is better if the user can have statistically higher flow throughput. Although a contention-based MAC protocol may not be always fair to contending nodes in terms of one-hop, short-term throughput, the statistical rate of a random flow in the network truthfully reflects the throughput of the network, particularly when the transport layer does not apply rate control over the flows in the network, as configured in our simulations.
The ad hoc network has 100 nodes in an area of 1000 by 1000 square meters. Each node uses a transmission power of 0.2 watts, which means a carrier sense range of about 500 meters with the default power threshold settings of ns-2. The link rate of each node is 1Mb/s (a higher rate means that more bits may be transmitted in the times saved by CSMA/FP for using more effective and efficient control frames). In addition, there is a maximum of 25 Constant Bit Rate (CBR) background flows that are randomly initialized. The routing protocol used in the simulations is the Dynamic Source Routing protocol (DSR) (14).
In modifying the IEEE 802.11 DCF with the bit-free control frame approach, we have used an n of 20 in the "Mod-n" calculation over the receiver's address for obtaining the length of

a RTS frame. Twenty is the average number of nodes that fall into the transmission range of a node in the ad hoc network (however, we have also investigated the impact of a halved n). The elements in the length set designated for RTS frames fall into two ranges for balancing the average length of a RTS frame with the average length of other control frames. One of the ranges is from 40 to 90μs, while the other is from 120 to 170μs (with a guard gap of 5μs). In addition, a CTS frame, a CTS-Fail frame, and an ACK frame have fixed lengths of 20, 100, and 110μs, respectively.

Actually, these parameters for bit-free control frames are chosen conservatively. The accuracy of detecting the length of a frame is affected by the hardware, bandwidth, and channel conditions. If we assume a basic link rate of 1 Mb/s (control frames are recommended to be transmitted at the basic link rate in narrow-band as well as broadband 802.11 systems), then each bit of a control frame has an average transmission time of 1μs. The chosen parameters for the bit-free control frames are at least multiple times of this unit and are therefore safe in reality, assuming that the bits of a conventional frame can be recovered in the channel.

For other parameters, the modified protocol shares the default ns-2 configurations with the original protocol. For example, the minimum and maximum sizes of the contention window of a node are 32 and 1024 timeslots, respectively, while a timeslot is 20μs. In addition, the retransmission limits are 7 and 4 for a RTS frame and a longer data packet, respectively.

4.2 Wireless LANs

Fig. 4 shows the throughput of a wireless LAN versus the number of nodes in the LAN. In the simulations, every node always has packets to send (i.e., a saturation traffic scenario) and the destination of each packet is randomly selected. In addition, each packet is 512-byte long. As shown in Fig. 4, the modified protocol has a relative throughput gain of about 15% (an absolute gain of about 100 kb/s) when there are 5 nodes in the network. As the number of nodes in the network increases, the throughput gain of the modified protocol increases too. When the number of nodes in the network reaches 25, the relative gain increases to 25% (an absolute gain of 150 kb/s).

The average medium access delay for a packet in the network is shown in Fig. 5. As shown in the figure, a packet experiences less delay when the modified MAC protocol replaces the original one in the network. These results conform to the throughput results shown above. For conciseness, we only show throughput results for ad hoc networks in the following sections.

4.3 Ad Hoc networks

The multihop ad hoc network introduced earlier provides us a more general scenario to investigate the performance of the modified protocol. The nodes in the network have random waypoint movement and have a minimum and a maximum speed of 1.0 and 5.0 m/s, respectively (the average pause time is 0.5 second). In such an ad hoc network, we have examined what percentage of the packets in a test flow in the network were successfully received by the flow receiver as the network load varied.

In particular, the two protocols were tested in a series of simulations in which the rate of the background flows varied from 0.5*512 bytes/second (B/s) to 8*512 B/s with an increase factor of 100%. The test flow, however, kept its rate *constant* at 4*512 B/s to monitor the actual throughput that it could obtain in various cases of network load.

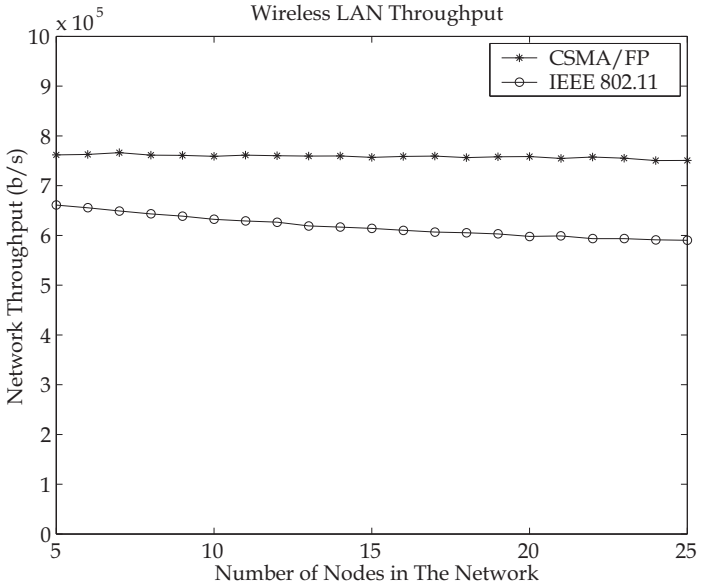


Fig. 4. Network Throughput vs. Number of Nodes

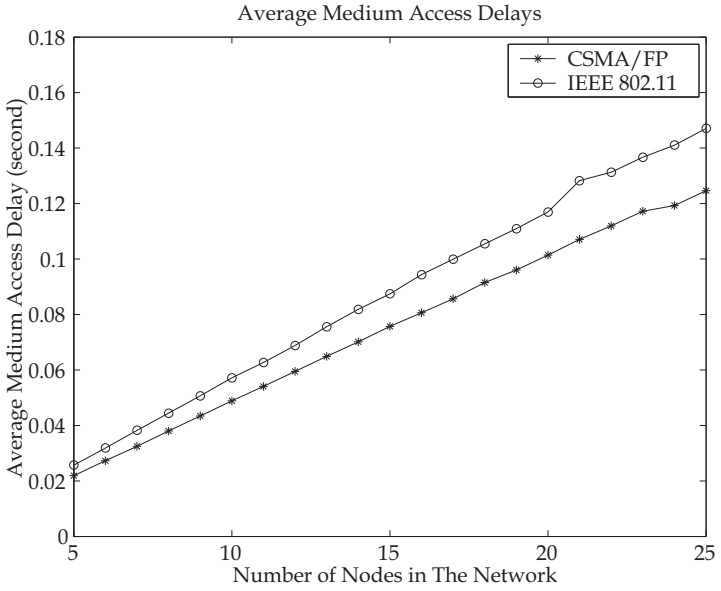


Fig. 5. Average Medium Access Delay vs. Number of Nodes

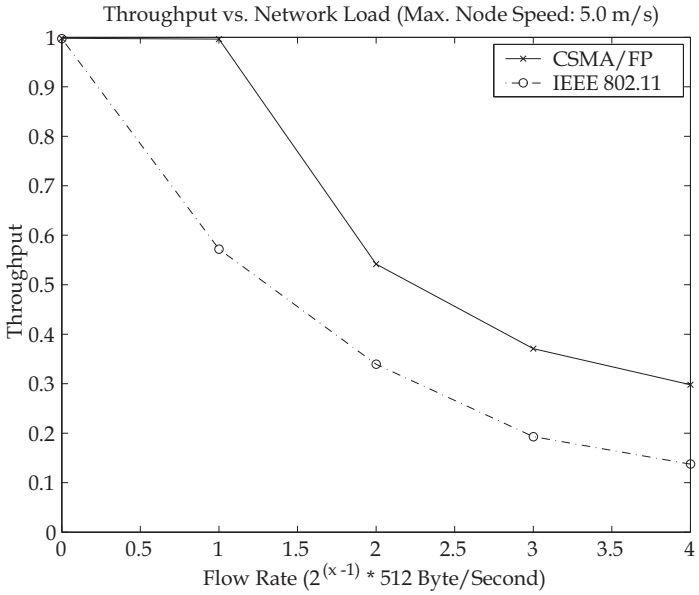


Fig. 6. Flow Throughput, Max Node Speed 5.0 m/s

Fig. 6 shows the throughput of the test flow versus the flow rate in the network, which determines the network load in our simulations. As shown in the figure, when the rate of the background flows is 0.5*512 B/s, almost all packets of the test flow are successfully delivered by the network with either MAC protocol. However, as the network load increases, more packets of the test flow are delivered by the network with the modified MAC protocol.

Particularly, when the rate of the background flows is 1*512 or 2*512 B/s, the throughput of the test flow increases by at least 50% as the modified MAC protocol replaces the original one. When the rate of the background flows is further increased above 4*512 B/s, the relative performance gains of CSMA/FP reach more than 100%. In summary, the modified protocol shows higher relative performance gains when the network load is higher.

In addition, as shown by the comparison of Fig. 6 to Fig. 4, the modified protocol shows higher performance gains in multihop ad hoc networks than in wireless LANs. These results are expected because there are hidden terminals in the multihop ad hoc network and the modified protocol is more effective in dealing with hidden terminals than the original protocol.

4.4 More hidden terminals

This section shows how the modified protocol performs when there is a higher probability of hidden terminals for a transmitter in the network. To increase the probability of hidden terminals, we increased the carrier sense (CS) power threshold of a node from less than one twentieth to half of its packet receive power threshold. The increase of the CS power threshold shrinks the carrier sense range of a node in the network.

Fig. 7 shows the throughput of the test flow when the CS power threshold has been increased in the network. As shown in Fig. 7, the relative performance gain of the modified protocol is, on average, more than 100% in the case of a higher probability of hidden

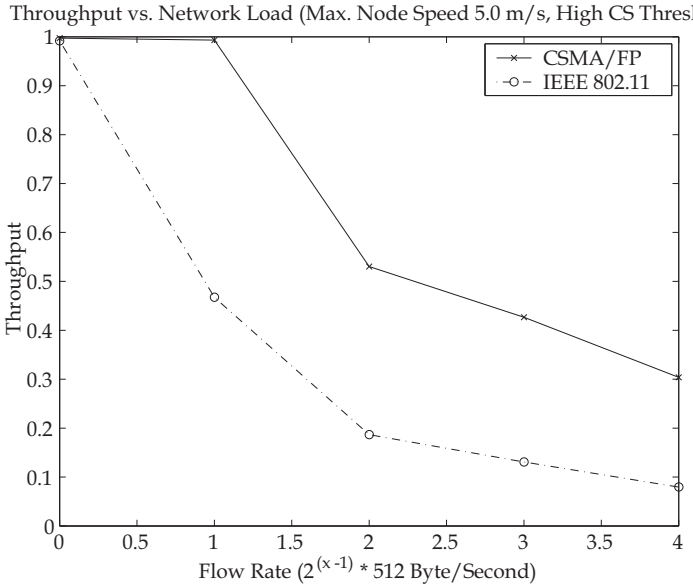


Fig. 7. Higher CS Power Threshold Case

terminals. By comparing Fig. 7 to Fig. 6, we find that the modified protocol has higher performance gains as the probability of hidden terminals is increased in the network. These results further show that the modified protocol is better in dealing with hidden terminals than the original protocol.

4.5 Rayleigh fading channel

By default, the two-ray ground channel model is used in ns-2. We have also investigated the impact of a Rayleigh fading channel on the performance of the modified protocol. The bit-free control frames of the modified protocol are robust against channel effects because of their low receive power threshold. However, a traditional, bit-based control frame may be easily lost in a fading channel.

Fig. 8 shows the results for the case of a Rayleigh fading channel. As shown by the comparison of Fig. 8 to Fig. 6, a fading channel increases the relative performance gains of the modified protocol over the original protocol. These results are expected because traditional control frames are sensitive to fading while any loss of a control frame makes all preceding related transmissions wasted.

4.6 Environmental noise

Besides the impact of channel effects, we have also investigated the impact of environmental noise on the modified protocol. On one hand, the bit-free control frames are robust against environmental noise in the sense that a noise signal may not change the length of a bit-free control frame but may corrupt a bit-based control frame. On the other hand, environmental noise may be falsely interpreted as control frames by a node with the modified MAC protocol. As explained in Section 3, a noise signal must have the right length, arrive at the right node, and possibly arrive at the right time for it to be harmful.

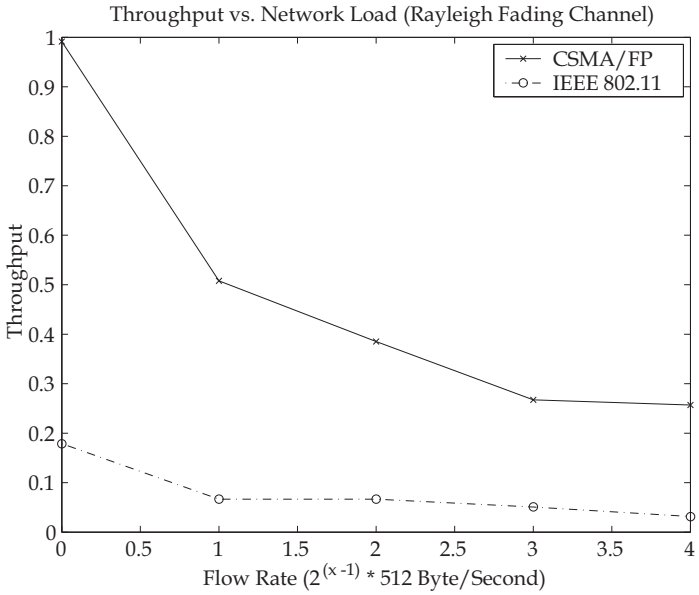


Fig. 8. Rayleigh Fading Channel Case

To test the impact of environmental noise,we placed a noise source at the center of the network and let it generate random-length noise signals at an average rate of 100 signals per second. Moreover, we restricted the noise signal lengths to the range from 1μs to 200μs, which were the range designated for the bit-free control frames. The simulation results for this scenario are shown in Fig. 9. As shown by the comparison of Fig. 9 to Fig. 6, the modified protocol is not more sensitive to noise than the original one. In fact, after the noise source is introduced in the network, the modified protocol shows higher *relative* performance gains over the original one.

4.7 Protocol resilience

The above subsections are about how external factors may impact the performance of the modified protocol. This subsection shows how the parameters of the protocol affect its performance. We have investigated the three most important parameters of the protocol, which are the receive power thresholds for control frames, the length set for control frames, and the base n of the Mod-n calculations for obtaining RTS frame lengths.

Fig. 10 shows how the modified protocol performs when all its control frames use the same receive power threshold as data frames, which deprives the modified protocol of its advantage of better hidden terminal handling. As shown in the figure, the protocol still maintains significant gains over the original protocol.

Fig. 11 shows the performance of the modified protocol as the average length of its control frames becomes similar to the average length of the bit-based control frames of the original protocol. As shown in this figure, the performance of the modified protocol degrades gracefully in this case.

Fig. 12 shows how the modified protocol performs as the base n of the Mod-n calculation is halved. Halving the n is similar to doubling the node density of the network in terms of

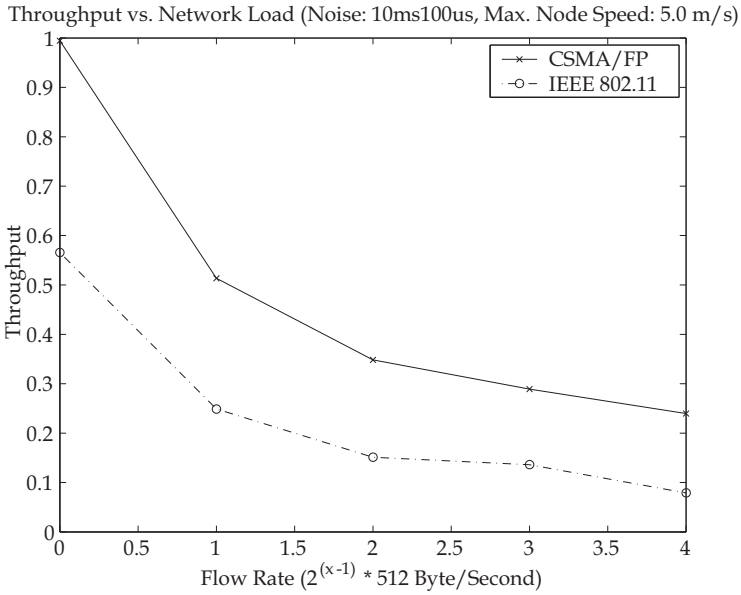


Fig. 9. Environmental Noise Case

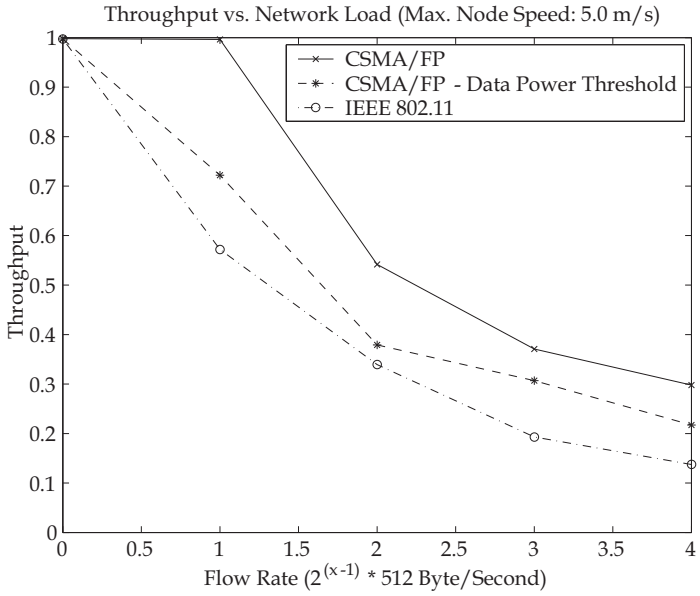


Fig. 10. Data Receive Power Threshold Case

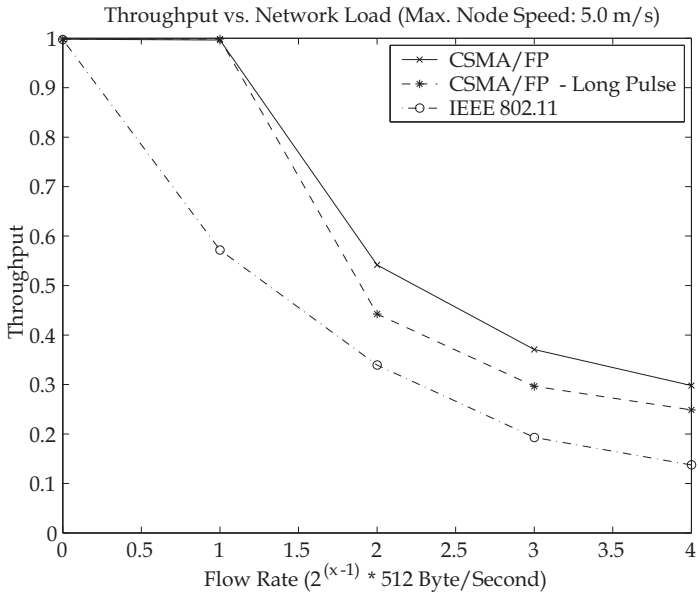


Fig. 11. Long Bit-Free Control Frames Case

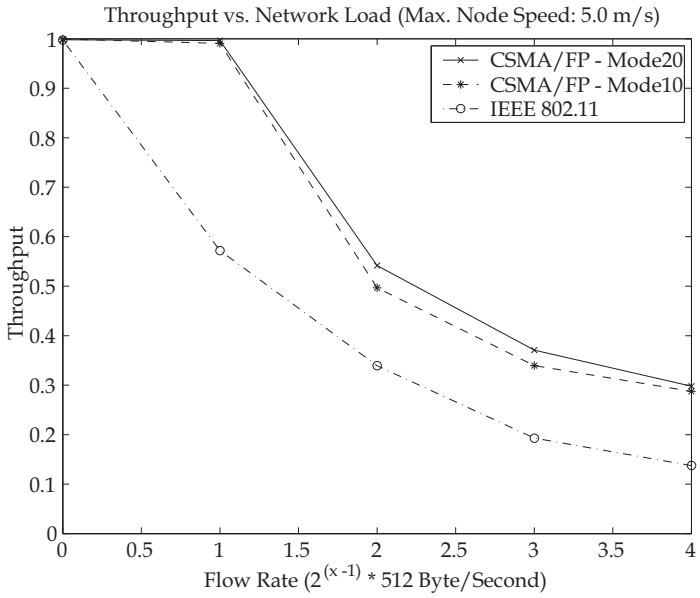


Fig. 12. Mod-n: n Changes from 20 to 10

investigating how the redundant CTS frames for a RTS frame may affect the performance of the protocol. As shown in Fig. 12, the performance of the modified protocol has a graceful degradation when the n is halved.

5. Related work

We introduce in this section some recent efforts on improving the IEEE 802.11 DCF in the community. Many efforts have been made to modify the backoff algorithm of the DCF. Cali et al. proposed an algorithm that enables each node to tune its backoff algorithm at run-time (15). Bianchi et al. proposed the use of a Kalman filter to estimate the number of active nodes in the network for dynamically adjusting the CW (16). Kwon et al. proposed a new CW adjustment algorithm that is to double the CW of any node that either experiences a collision or loses a contention (17). On the other hand, Ma et al. proposed a centralized way to dynamically adjust the backoff algorithm (18). From a theoretical perspective, Yang et al. investigated the design of backoff algorithms (19).

Another interesting scheme on backoff algorithms, named *Idle Sense*, was proposed by Heusse et al (20). With Idle Sense, a node monitors the number of idle timeslots between transmission attempts and then adjusts its contention window accordingly. This method uses interference-free feedback signals and the authors showed its fairness and flexibility among other features. Instead of modifying the backoff algorithm, some other works proposed diverse ways to improve the performance of the IEEE 802.11 DCF. Peng et al. proposed the use of out-of-band pulses for collision detection in distributed wireless networks (5). Sadeghi et al. proposed a multirate scheme that exploits the durations of high-quality channel conditions (21). Cesana et al. proposed the embedding of received power and interference level information in control frames for better spatial reuse of spectrum (22). Sarkar et al. proposed the combination of short packets in a flow to form large frames for reducing control and transmission overhead (23). Additionally, Zhu et al. proposed a multirate scheme that uses relay nodes in the MAC sub-layer (24).

Different from the work mentioned above, the work in this article is to improve the effectiveness and the efficiency of the collision avoidance (CA) part of the IEEE 802.11 DCF. The proposed method may work with other schemes that improve the backoff algorithm of the DCF protocol (i.e., the CSMA part of the protocol).

6. A fundamental view

Finally, we provide a fundamental view on bit-free control frames from the perspectives of information theory and digital communications. The basic goals of bit-free control frames are to increase the range, reliability, and efficiency of control information delivery for medium access control.

Information theory states that the capacity of a channel decreases as the signal to noise ratio decreases. For example, the capacity of a band-limited Gaussian channel is

$$C = W \log(1 + \frac{P}{N_0 W}) \tag{6}$$

where the noise spectral density is $N_0/2$. This equation basically states that when the received power P is lower, then the channel capacity is smaller. Therefore, if the control

information for medium access control needs to be delivered in a larger range without sacrificing reliability, then the transmission power may need to be increased (the bandwidth W is usually fixed).

There are, however, two issues with the approach of higher power for control frames. One is that the transmission power for control frames has to be increased by at least multiple times because signals deteriorate fast in wireless channels. For example, if the transmission range of a control frame needs to be doubled, then the transmission power may have to be increased by more than ten times even in free space. The other issue is that when the transmission range of a control frame is increased, then its carrier sense range is also increased at the same ratio, which causes unnecessary backoff for some nodes.

Instead, the capacity of the channel may be traded, as shown by Equation 6. The first step in this direction is to trim the control information for medium access control, which is to only deliver indispensable control information. The second step is to find away to realize the tradeoff by using new physical layer mechanisms. With bit-free control frames, the medium access control information is not translated into *bits* and then goes through the *bit* delivery process. Instead, the control information is directly modulated by the airtimes of control frames. From this perspective, the bit-free control frame approach is a cross-layer approach with which control information is delivered with a simple modulation method that trades capacity for transmission range and information reliability.

7. Conclusions

We have presented in this article a new approach of *bit-free* control frames to collision avoidance in distributed wireless packet networks. With the new approach, medium access control information is not delivered through bit flows. Instead, the information is encoded into the airtimes of bit-free control frames. Bit-free control frames are robust against channel effects and interference. Furthermore, bit-free control frames can be short because they do not include headers or preambles. We have investigated the new approach by analysis and extensive simulations. We have shown how hidden terminals, a fading channel, and environmental noise may impact the performance of the new approach. Additionally, we have examined the impact of the average length, the receive power thresholds, and the length set size of control frames on the performance of the new approach. Our conclusion is that the new bit-free control frame approach improves the throughput of a wireless LAN or ad hoc network from fifteen percent to more than one hundred percent.

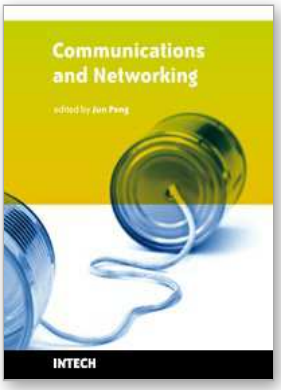
8. References

[1] F. A. Tobagi and L. Kleinrock, "Packet switching in radio channels: Part II - the hidden terminal problem in carrier sense multiple access and the busy tone solution," *IEEE Transactions on Communications*, vol. 23, pp. 1417–1433, 1975.

[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] C. Wu and V. O. K. Li, "Receiver-initiated busy-tone multiple access in packet radio networks," in *Proc. of the ACM SIGCOMM*, Stowe, Vermont, August 1987.

[4] Z. J. Haas and J. Deng, "Dual Busy Tone Multiple Access (DBTMA) - a multiple access control scheme for ad hoc networks," *IEEE Transactions on Communications*, vol. 50, pp. 975–985, June 2002.
[5] J. Peng, L. Cheng, and B. Sikdar, "A new MAC protocol for wireless packet networks," in *IEEE GLOBECOM 2006*, San Francisco, CA, Nov.-Dec. 2006.
[6] A. Colvin, "CSMA with collision avoidance," *Computer Commun.*, vol. 6, pp. 227–235, 1983.
[7] P. Karn, "MACA - a newchannel accessmethod for packet radio," in *Proc. of the 9th ARRL Computer Networking Conference*, Ontario, Canada, 1990.
[8] C. L. Fullmer and J. J. Garcia-Luna-Aceves, "Floor acquisition multiple access (FAMA) for packet-radio networks," in *Proc. of the ACM SIGCOMM*, September 1995.
[9] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, "MACAW: a medium access protocol for wireless LANs," in *Proc. of the ACM SIGCOMM*, London, United Kingdom, August 1994.
[10] C. L. Fullmer and J. J. Garcia-Luna-Aceves, "Solutions to hidden terminal problems in wireless networks," in *Proc. of the ACM SIGCOMM*, French Riviera, France, September 1997.
[11] IEEE 802.11 wireless local area networks. [Online]. Available: http://grouper.ieee.org/groups/802/11/
[12] K. Xu,M. Gerla, and S. Bae, "How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks?" in *Proc. of the IEEE GLOBECOM*, Taipei, Taiwan, November 2002.
[13] The network simulator - ns-2. [Online]. Available: http://www.isi.edu/nsnam/ns/
[14] D. B. Johnson, D. A. Maltz, and Y.-C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (DSR)," *IETF Interet draft, draft-ietf-manet-dsr-10.txt*, July 2004.
[15] F. Cali, M. Conti, and E. Gregori, "Dynamic tuning of the IEEE 802.11 protocol," *IEEE/ACM Transactions on Networking*, vol. 8, pp. 785 – 799, Dec. 2000.
[16] G. Bianchi and I. Tinnirello, "Kalman filter estimation of the number of competing terminals in an IEEE 802.11 network," in *Proc. of the IEEE INFOCOM*, 2003.
[17] Y. Kwon, Y. Fang, andH. Latchman, "A novelMAC protocolwith fast collision resolution for wireless LANs," in *Proc. of the IEEE INFOCOM*, 2003.
[18] H.Ma, H. Li, P. Zhang, S. Luo, C. Yuan, and X. Li, "Dynamic optimization of IEEE 802.11 CSMA/CA based on the number of competing stations," in *Proc. of the IEEE ICC*, 2004.
[19] Y. Yang, J. Wang, and R. Kravets, "Distributed optimal contention window control for elastic traffic in wireless LANs," in *Proc. of the IEEE INFOCOM*, 2005.
[20] M. Heusse, F. Rousseau, R. Guillier, and A. Duda, "Idle Sense: An optimal accessmethod for high throughput and fairness in rate diverse wireless LANs," in *Proc. of the ACM SIGCOMM*, 2005.
[21] B. Sadeghi, V. Kanodia, A. Sabharwal, and E. Knightly, "Opportunistic media access for multirate ad hoc networks," in *Proc. of the ACM MOBICOM*, 2002.
[22] M. Cesana, D. Maniezzo, P. Bergamo, and M. Gerla, "Interference aware (IA) MAC: an enhancement to IEEE802.11b DCF," in *Proc. of the VTC*, 2003.
[23] N. Sarkar and K. Sowerby, "Buffer unit multiple access (BUMA) protocol: an enhancement to IEEE 802.11b DCF," in *Proc. of the IEEE GLOBECOM*, 2005.
[24] H. Zhu and G. Cao, "rDCF: A Relay-enabled Medium Access Control Protocol for Wireless Ad Hoc Networks," in *Proc. of the IEEE INFOCOM*, 2005.



Communications and Networking

Edited by Jun Peng

ISBN 978-953-307-114-5
Hard cover, 434 pages
Publisher Sciyo
Published online 28, September, 2010
Published in print edition September, 2010

This book "Communications and Networking" focuses on the issues at the lowest two layers of communications and networking and provides recent research results on some of these issues. In particular, it first introduces recent research results on many important issues at the physical layer and data link layer of communications and networking and then briefly shows some results on some other important topics such as security and the application of wireless networks. In summary, this book covers a wide range of interesting topics of communications and networking. The introductions, data, and references in this book will help the readers know more abut this topic and help them explore this exciting and fast-evolving field.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Jun Peng (2010). Medium Access Control in Distributed Wireless Networks, Communications and Networking, Jun Peng (Ed.), ISBN: 978-953-307-114-5, InTech, Available from: http://www.intechopen.com/books/communications-and-networking/medium-access-control-in-distributed-wireless-networks

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821