UC Santa Cruz

UC Santa Cruz Previously Published Works

Title

Implementing Correct and Efficient Collision Avoidance in Multi-Hop Ad-Hoc Networks

Permalink

<https://escholarship.org/uc/item/4qx648d5>

Author

Garcia-Luna-Aceves, J.J.

Publication Date

2018-11-01

Peer reviewed

Implementing Correct and Efficient Collision Avoidance in Multi-Hop Ad-Hoc Networks

J.J. Garcia-Luna-Aceves

Computer Science and Engineering Department, University of California, Santa Cruz, CA 95064
PARC, Palo Alto, CA 94304
jj@soe.ucsc.edu

Abstract—CSMA/CAP (Carrier-Sense Multiple Access with Collision Avoidance and Pilots) is introduced for ad-hoc networks in which each node has a single half-duplex radio. Using carrier sensing to access the common channel, a node with a data packet to send transmits a request-to-send (RTS) packet. If the RTS is sent without interference, the receiver sends a clear-to-send (CTS) packet followed by a pilot. A sender that receives a CTS for itself sends its data packet after a delay to let the pilot be heard and then transmits its own pilot to make the total transmission time equal to a maximum data-packet length. The receiver sends its ACK after receiving the data packet and pilot from the sender. It is shown that no channel-access protocol based on the traditional RTS-CTS handshake over a single channel can guarantee collision-free transmissions of variable-length data packets and ACK's, and that CSMA/CAP does ensure that data packets and their ACK's are sent without multiple-access interference. The throughput of CSMA/CAP is compared with the throughput of CSMA in networks with and without hidden terminals, and the results show that the overhead of CSMA/CAP to eliminate collisions is small and that CSMA/CAP performs far better than CSMA when hidden terminals are present.

I. INTRODUCTION

Carrier-sense multiple access (CSMA) [13] is arguably the most widely used technique for the sharing of common radio channels in ad-hoc networks today, as it is an integral part of the IEEE 802.11 protocol standard. It is well known that while carrier sensing renders far better throughput than simply transmitting data packets without any coordination among nodes, which is the case of the ALOHA protocol [1], the performance of a CSMA degrades substantially in the presence of hidden terminals [14]. The main problem introduced by hidden terminals is that two or more transmitters around a receiver are unable to hear the transmissions from one another, which renders carrier sensing useless.

As Section II summarizes, many approaches have been developed over the years to limit or eliminate the negative effects of multiple-access interference (MAI) due to hidden terminals. These approaches can be classified into collision-avoidance schemes (e.g., [3], [5]) and busy-tone schemes (e.g., [8], [10], [14]). A few approaches have also been advanced to emulate collision detection using half-duplex radios [4], [9] in fully-connected wireless networks. Lastly, some approaches have been proposed based on full-duplex radios or self-interference cancellation (SIC) at the physical layer to support

full-duplex communication or implement collision detection [6].

Ad-hoc networks based on nodes endowed with a single half-duplex radio and operating in a single channel are likely to be the preferred choice for some time due to cost considerations and design complexity. In this light, it is important to point out that no channel-access protocol has been proposed to date that eliminates MAI on transmitted data packets and their acknowledgments (ACK) in the presence of hidden terminals while using a single half-duplex transceiver per node. The main contribution of this paper is introducing and verifying This paper introduces the first channel-access protocol that eliminates MAI on variable-length data packets and their ACK's transmitted over a single channel.

Section III describes **CSMA/CAP** (*Carrier-Sense Multiple Access with Collision Avoidance and Pilots*). It is based on a surprisingly simple extension of the traditional CSMA/CA approach taking advantage of conventional carrier-detection techniques at the physical layer based on physical-layer convergence procedure (PLCP) framing. By means of added waiting periods and pilots that consist of special PLCP frames sent by senders and receivers, nodes augment the traditional collision avoidance (CA) handshake over a single channel to ensure that both data packets and ACK's are sent without MAI.

In CSMA/CAP, a node with a data packet to send uses carrier sensing to transmit a request-to-send (RTS) packet. The intended receiver replies with a clear-to-send (CTS) packet followed by a pilot intended to block hidden sources that may be attempting to send RTS's. The sender of a successful RTS sends its data packet after receiving the receiver's CTS and pilot, and transmits its own pilot that makes the virtual-carrier time equal to the longest-allowed length of a data packet. The receiver sends an acknowledgment (ACK) after receiving the pilot from the sender. The signaling and timing used with pilots and the traditional CA handshake are designed to ensure that data packets and their acknowledgments (ACK) are sent without multiple access interference (MAI).

Section IV shows that CSMA/CAP prevents the collision of data packets with other transmissions even in the presence of hidden terminals, and allows receivers to inform senders of the correct reception of data packets. Sections V and VI analyze the throughput of CSMA/CAP and compare it against the throughput of CSMA with collision avoidance (CSMA/CA). The results of the analysis show that CSMA/CAP is much

more efficient than traditional CSMA/CA. Section VII presents our conclusions.

II. RELATED WORK

The channel-access protocols that have been developed to date to address the negative effect of multiple-access interference (MAI) caused by hidden terminals in CSMA [14] can be classified in two types: protocols based on collision-avoidance (CA) handshakes and protocols based on busy tones sent over secondary channels.

One of the first channel-access protocols based on CA handshakes was Multiple Access with Collision Avoidance (MACA) [12], which consists of a transmitter sending a request-to-send (RTS) packet to an intended receiver and the receiver sending a clear-to-send (CTS) packet if the RTS is successful. MACA does not use carrier sensing and its performance degrades in the presence of hidden terminals. Many subsequent variants of channel-access protocols based on CA handshakes have been proposed and analyzed since the introduction of MACA and have integrated carrier sensing together with CA handshakes. In some schemes the transmitter initiates the handshake [3] and in others the receiver does [5]. The IEEE 802.11 distributed coordination function (DCF) is arguably the most popular example of combining carrier sensing with the RTS-CTS handshake followed by a data packet and an ACK in successful cases.

Figure 1 illustrates the fact that, although CSMA/CA is intended to cope with hidden-terminal interference, collisions can occur in multi-hop ad hoc networks if the duration of CTS's is similar to the duration of RTS's. In the example, transmitter T_2 sends its RTS to R_2 while the CTS from R_1 is being received. Because RTS's and CTS's last roughly the same time, T_2 does not hear the carrier of the CTS from R_1 , receives the CTS from R_2 and transmits its data packet, which collides at R_1 with the data packet sent by T_1 .

Fig. 1. Collisions due to hidden terminals in CSMA/CA

Fig. 2. Multiple-access interference from exposed-transmitters in CSMA/CA

Figure 2 illustrates another major limitation of CSMA/CA when it is used in a multi-hop ad hoc network. In the example,

sources T_1 and T_2 send RTS's around the same time, both sources receive the CTS's from the intended receivers, and the data packet from T_2 lasts much longer than the data packet from T_1 . The problem is that, although receivers R_1 and R_2 receive the data packets without MAI, the data packet from T_2 interferes with the ACK from R_1 needed by T_1 . A similar MAI problem arises with exposed receivers (e.g., interchanging R_1 and T_1 , and R_2 and T_2). In such a case, the ACK from one receiver, say R_1 , interferes with a longer data packet being received by a neighboring receiver, say R_2 .

The only known CA handshake that has been shown to avoid MAI from hidden terminals while operating in a single channel requires that the CTS from a receiver be much longer than the length of an RTS in order to serve as a busy tone detected by hidden senders that transmitted RTS's concurrently with a CTS [3]. However, this approach *does not* work correctly when ACK's are used as part of the CA handshake and data packets have variable length. For example, the same interference from exposed transmitters can occur even with CTS packets that are much longer than RTS packets.

The Busy-Tone Multiple Access (BTMA) [14] eliminates multiple-access interference around a central receiver. The available channel is partitioned into a data channel and the busy-tone channel. The central receiver has radio connectivity with all other nodes in the system and transmits a busy tone over the busy-tone channel as soon as it detects carrier in the data channel resulting from transmissions from any subset of transmitters. A number of subsequent approaches based on one or multiple busy tones, also called carrier tones, have been proposed (e.g., [10]), and some of them ensure that ACK's are received without MAI and even emulate collision detection [8]. The performance of a few of these approaches is much better than that of CSMA/CA; however, all busy-tone approaches require one or two additional control channels, and the corresponding number of additional transceivers operating concurrently.

A few approaches have been proposed based on full-duplex transceivers, and an approach to use collision avoidance and detection in CSMA was recently proposed [6] assuming the use of self-interference cancellation (SIC) at the physical layer. While this approach is promising given that the technologies needed for full-duplex transceivers and SIC are evolving rapidly, ad-hoc networks today require the use of half-duplex transceivers. A few proposals have been reported on how to emulate CSMA/CD using half-duplex radios (e.g., [4], [9]) but they work correctly only in fully-connected wireless local area networks (WLAN).

III. CSMA/CAP

The objectives in the design of CSMA/CAP are to: (a) Allow the use of a single half-duplex transceiver per node in a multi-hop ad hoc network; (b) eliminate multiple access interference (MAI) on data packets and their acknowledgments (ACK); and (c) inform senders when their packets are received successfully.

There are various ways to implement carrier detection at the physical layer [11], and CSMA/CAP assumes the combined use of carrier sensing based on energy detection and preamble detection, given that both techniques are well established today. Energy detection consists of comparing the signal strength readings obtained from the radio front end (the Received Signal Strength Indicator or RSSI reading) and a carrier-sense threshold used as the noise floor corresponding to the channel being idle. A node determines that the channel is busy when the instantaneous RSSI reading is larger than its carrier-sense threshold. Preamble detection uses the fact that each transmission begins with a common preamble sequence used as part of the physical-layer convergence procedure (PLCP) framing, such that there is a high likelihood that a transmission is taking place if the radio decodes a preamble.

CSMA/CAP extends the CA handshake in IEEE 802.11 by introducing *pilots* transmitted by a receiver after it sends a CTS and after a sender transmits a data packet. A pilot is simply a bit pattern sent as a PLCP frame that can be used at the physical layer to detect the presence of either a single pilot or multiple pilots using energy detection and preamble detection. We denote the length of a pilot by ρ . A pilot could be a PLCP preamble consisting of a synchronization field and a frame delimiter field indicating the end of the PLCP frame. For example, according to the IEEE 802.11 specifications, the length of such a pilot for a direct sequence spread spectrum (DSSS) physical layer would be 144 bits, and the transmission time of such a pilot is longer than a propagation delay and a turnaround time in a typical scenario.

The length the MAC header of a CTS and ACK in IEEE 802.11 is 14 bytes while the length of the MAC header of an RTS is 20 bytes and each packet also has a PLCP header. Accordingly, for convenience, we will assume that the length of all these packets is the same and denote it by γ . We also assume that a pilot lasts $\rho = 2(\tau + \omega)$, where τ is the maximum propagation delay and ω is the turnaround time. We show subsequently that this pilot length ensures that any hidden source to be forced to back off.

A. Pilot-based Collision Avoidance

The design of CSMA/CAP can be viewed as an improvement on FAMA protocols that allows the use of ACK's. The intent of requiring the receiver to transmit a pilot after its CTS is to have the pilot act as a "busy tone" around a receiver expecting a data packet. A hidden source that sent an RTS around the same time as the CTS was sent is forced to detect the carrier from the receiver's pilot and back off. Figure 3 illustrates the role of pilots in eliminating MAI due to hidden sources using the same example of Figure 1. In the example, source T_2 hidden from source T_1 is forced to back off by the carrier produced by the pilot sent by receiver R_1 even if it cannot hear the CTS from R_1 while transmitting its own RTS.

The intent of requiring the sender of a data packet to transmit a pilot after some delay following its packet transmission is to eliminate MAI in scenarios involving exposed

transmitters and exposed receivers. The delay used for the transmission of a pilot by the sender is such that the total time elapsed from the start of its data packet to the end of its pilot equals the transmission time of the longest data-packet packet transmission allowed. Because RTS's sent by exposed transmitters or CTS's sent by exposed receivers must occur within a maximum propagation delay of each other, the approach results in data packets being received without MAI from ACK's or pilots.

Fig. 3. Hidden source is forced to back off by pilot sent after CTS

Fig. 4. Eliminating MAI from exposed transmitters using pilots

Fig. 5. Eliminating MAI from exposed receivers using pilots

Figure 4 illustrates the role of pilots in eliminating MAI due to exposed transmitters using the same example discussed for CSMA/CA, and Figure 5 illustrates the role of pilots in eliminating MAI due to exposed receivers. As the figures show, the approach makes all exposed senders (T_1 and T_2 in Figure 4) or hidden senders around exposed receivers (R_1 and R_2 in Figure 5) send their pilots within one propagation delay from each other, which suffices to allow the ACK's from receivers to arrive without MAI because data packets and ACK's that may cause MAI at neighboring nodes must

be sent within a propagation delay of one another due to the CA handshakes, and a pilot lasts $2(\omega + \tau)$ seconds.

B. CSMA/CAP State Machine

Fig. 6 illustrates the state machine of CSMA/CAP assuming a non-persistent transmission strategy. It is assumed that a single packet is passed to the MAC layer for transmission.

If a node is in the PASSIVE state, there is no carrier in the channel, and the node receives a packet to send, then it transmits an RTS and transitions to the RTS state to wait for a CTS from the intended receiver. A node in the PASSIVE state that receives an RTS for itself transmits a CTS followed by a pilot and transitions to the CTS state. Alternatively, if a node in the PASSIVE state detects any pilot or a valid packet to some other node, the node transitions to the BACK-OFF state. A node in the BACK-OFF state computes a random back-off time (TO) and transitions to the PASSIVE state after that time has elapsed or the node decodes an ACK. The back-off time is longer than the time needed for the longest allowed data packet and an ACK to be exchanged. A back-off discipline is used to account for unsuccessful retransmission attempts for the same data packet and limit congestion. We simply assume that the back-off time is much larger than the time needed for a successful RTS-CTS-pilot-DATA-pilot-ACK transaction to take place.

Fig. 6. Non-persistent CSMA/CAP

A node in the RTS state transitions to the PILOT state if it receives a CTS for itself, and transitions to the BACK-OFF state if it receives no CTS after a timeout or detects carrier from a pilot while waiting for a CTS. A node in the PILOT state enters the transmission mode and simply waits for a period of time $W = \omega + 2\tau$ that is long enough for the receiver to be ready to receive its data after completing the pilot transmission. The node transmits its data packet after that time and transitions to the DATA state.

Once in the DATA state, the node simply transmits a pilot after a delay d and transitions to the WACK state. The delay d is designed to make the elapsed time from the start of its data-packet transmission to the end of its transmitted pilot equal to the maximum length of a data-packet transmission.

A node in the WACK state transitions to the PASSIVE state if it receives an ACK from the receiver of its data packet. Alternatively, it transitions to the BACK-OFF state if it receives no ACK after a timeout.

A node in the CTS state remembers whether a local packet is ready for transmission while in that state. The node transitions to the ACK state if it receives a data packet for itself from the remote sender. Alternatively, the node transitions to the passive state if it receives no data packet from the remote sender after a timeout and it has no local packet to send, or to the BACK-OFF state if it has a local packet to send.

If a node receives a valid pilot once it is in the ACK state, the node waits for $\rho + \omega + 2\tau$ seconds before transmitting its ACK to the sender and then transitions to the PASSIVE state if it has no local packet to transmit or to the BACK-OFF state if it has a local packet to transmit. The waiting time is used to prevent collisions of ACK's at the sender. Alternatively, the node transitions to the BACK-OFF state after a timeout period if it does not receive a valid pilot.

IV. CORRECTNESS OF CSMA/CAP

We make the following assumptions to prove the correctness of CSMA/CAP: (a) A node knows the addresses of its neighboring nodes through some means external to the channel-access protocol and node connectivity does not change; (b) nodes execute the protocol correctly; (c) the propagation delay t_p between any two neighboring nodes is $0 < t_p \leq \tau$ and each transmission from a node can be detected by each of its neighbors; (d) the transmit-to-receive and receive-to-transmit turn-around times are at most ω seconds, and the time needed to detect carrier based on energy detection is $\xi < \omega$; (e) the transmission time of a pilot is ρ seconds; and (f) the transmission time of a data packet or a signaling packet consists of a physical-layer portion and a medium-access control (MAC) portion.

The following theorem shows that CSMA/CAP prevents MAI on data packets and ACK's even in the presence of hidden terminals, exposed transmitters or exposed receivers.

Theorem 1: CSMA/CAP ensures that no data packets or their ACKs collide with any other transmissions.

Proof: For a data packet from transmitter T to be sent to receiver R , a successful pilot-based CA handshake must first take place between T and R . This implies that T must be able to send an RTS, R must receive the RTS from T free of collisions, and T must receive the CTS from R free of collisions as well as the pilot from R . Accordingly, the rest of the proof must show that, if a handshake succeeds between T and R up to the reception of a CTS and a pilot at the transmitter T , any neighbor of T or R must back off long enough to allow the data and ACK to be sent between T and R without MAI.

Fig. 7 illustrates the type of MAI that T and R may experience from neighboring nodes. Solid lines indicate radio connectivity and dashed lines indicate possible radio connectivity. Node n_R is a neighbor of R other than T that may be connected to or hidden from R , and node n_T is a neighbor

of T other than R that may be connected to or hidden from T . Nodes x and y are neighbors of n_T and n_R , respectively, which may cause n_T and n_R to create interference at T or R . The proof of this theorem follows directly from the following two lemmas. ■

Fig. 7. Nodes that may cause MAI for a receiver R and a transmitter T

Lemma 1: CSMA/CAP ensures that data packets are received without MAI.

Proof: According to the operation of CSMA/CAP, R can receive a data packet from transmitter T only after it sends a CTS and a pilot to T . Therefore, the proof must assume that R sends its CTS and pilot to T . Let t_r be the time when R starts transmitting its CTS. Because R sends its CTS, a neighbor n_R can cause MAI on the data packet from T only by starting a new CA handshake (Case 1) or by responding to a handshake initiated by another node (Case 2).

Case 1: Assume that n_R starts a new CA handshake by transmitting an RTS at time t_{nr} . The RTS from n_R arrives in its entirety at R at time t_{nri} . By assumption, n_R transmits its CTS at time t_r ; hence, $t_{nr} \leq t_r + \omega + \tau$, because the turnaround time is ω and propagation delays are at most τ . Accordingly,

$$t_{nri} \leq t_{nr} + \gamma + \tau \leq t_r + \gamma + \omega + 2\tau \quad (1)$$

Node R cannot listen to the channel while sending its CTS followed by its pilot. Hence, given that $\rho = 2(\omega + \tau)$, the earliest time when node R could detect an RTS from n_R is

$$t_{cts} = t_r + \rho + \gamma = t_r + \gamma + 2\omega + 2\tau \quad (2)$$

From Eqs. (1) and (2), $t_{cts} > t_{nri}$ and the RTS from n_R cannot disrupt R . On the other hand, n_R must back off if it detects carrier after sending its RTS and is unable to decode a CTS from its intended receiver. Also, for n_R to decode such a CTS, it must arrive without any MAI from the CTS sent by R . Let t_{inr} be the time when the entire CTS and pilot from R are received at n_R and let t_{cnr} be the time when n_R starts listening for carrier after sending its RTS.

Neighbor n_R can detect the carrier of the CTS from R starting at $t_r + \tau$ and hence it can start its RTS no later than $t_r + \tau + \omega$. Given that an RTS lasts γ and n_R starts listening to the channel after a turnaround delay, it follows that

$$t_{cnr} \leq t_r + \gamma + (\tau + \omega) + \omega = t_r + \gamma + 2\omega + \tau \quad (3)$$

However, given that propagation delays are non-zero, the carrier created by the CTS and pilot from R must persist at n_R until time

$$t_{inr} > t_r + \gamma + \rho = t_r + \gamma + 2\omega + 2\tau \quad (4)$$

It follows from Eqs. (3) and (4) that $t_{inr} > t_{cnr}$ and hence the CTS and pilot from R must force n_R to back off, which

means that n_R cannot cause MAI on the data packet sent to R if it starts a CA handshake.

Case 2: Assume that n_R responds to a CA handshake. Because R starts sending its CTS at time t_r by assumption, n_R can respond to a CA handshake only by starting a CTS no earlier than $t_r - (\tau + \omega)$ and no later than $t_r + (\tau + \omega)$, for otherwise either R could not send its CTS at time t_r or n_R would detect carrier.

Let t_{rd} be the time when R starts receiving the data packet from T and t_{rp} be the time when the entire pilot from n_R has arrived at R . Because propagation delays are non-zero and T waits $\omega + 2\tau$ seconds to send its data packet after receiving a pilot from R , we must have that

$$t_{rd} > t_r + \gamma + \rho + \omega + 2\tau = t_r + \gamma + 3\omega + 4\tau \quad (5)$$

On the other hand, because propagation delays are non-zero and the pilot from n_R starts at most $\omega + \tau$ seconds after the pilot from R starts, we must have

$$t_{rp} \leq t_r + \gamma + \rho + (\omega + \tau) + \tau = t_r + \gamma + 3\omega + 4\tau \quad (6)$$

It follows from Eqs. (5) and (6) that $t_{rd} > t_{rp}$ and hence the pilot from n_R sent after its CTS cannot interfere with the data packet from T at R .

Let t_{tep} be the time when T stops transmitting its pilot following its data packet, and let t_{nep} be the time when a neighbor H of n_R stops transmitting its pilot following its data packet to n_R . Because the time between the start of a data packet and the end of the pilot following the packet transmission must equal a maximum-allowed data-packet transmission time δ , it must be true that $t_{nep} > t_{tep} - (\omega + 2\tau)$.

Let t_{nak} be the time when the ACK from n_R starts arriving at R and t_{rp} be the time when the pilot from T arrives completely at R . Because propagation delays are non-zero and n_R must wait $\rho + \omega + 2\tau$ seconds before sending its ACK to H , we have

$$t_{nak} > t_{nep} + \rho + \omega + 2\tau > t_{tep} + 2\omega + 3\tau \quad (7)$$

On the other hand, because propagation delays are at most τ , we must have that

$$t_{rp} \leq t_{tep} + \rho + \tau = t_{tep} + 2\omega + 3\tau \quad (8)$$

It follows from Eqs. (7) and (8) that $t_{nak} > t_{rp}$ and hence the NACK from n_R sent to its neighbor H cannot interfere with the pilot sent from T to R . Therefore, the lemma is true. ■

Lemma 2: CSMA/CAP ensures that ACK's are received without MAI.

Proof: According to the operation of CSMA/CAP, sender T can send an ACK to R only after receiving the data packet and pilot from T . Let t_s be the time when T completes transmitting its pilot following the data packet sent to R and let t_{ack} be the time when T starts receiving the ACK from R . It follows from Lemma 1 that R must receive the pilot from T without any MAI.

Neighbor n_T can only interfere with the ACK received by T with a data packet and pilot transmission. Let t_{ntp}

be the time when the end of a pilot from n_T arrives at T . According to the operation of CSMA/CAP, n_T must start its transmission no later than $\omega + \tau$ seconds after T starts its own transmission; otherwise, n_T would detect the carrier from T , which corresponds to an invalid pilot forcing n_T to back off. Furthermore, the time elapsed from the start of the data packet and the end of the pilot sent by T and any source corresponds to one maximum data-packet transmission time δ . Accordingly, given that propagation delays are at most τ seconds, we have

$$t_{ntp} \leq t_s + (\omega + \tau) + \tau = t_s + \omega + 2\tau \quad (9)$$

Because propagation delays are non-zero and R waits $\rho + \omega + 2\tau$ seconds before sending its ACK, it must be true that

$$t_{ack} > t_s + \rho + \omega + 2\tau > t_s + 2\omega + 2\tau \quad (10)$$

It follows from Eqs. (9) and (10) that $t_{ack} > t_{ntp}$ and hence the pilot from n_T cannot interfere with the ACK from R received by T . Therefore, the lemma is true. ■

V. THROUGHPUT ANALYSIS

We analyze the non-persistent version of CSMA/CAP and compare it against CSMA with priority ACKs using the traffic model first introduced by Kleinrock and Tobagi [13]. We consider two scenarios. A fully-connected scenario is used to illustrate the additional overhead introduced by CSMA/CAP when no hidden terminals are present. To illustrate the importance of eliminating collisions in the presence of hidden terminals we use a star configuration in which all sources transmit to a central receiver and all sources are hidden from each other.

There is a large number of stations that constitute a Poisson source sending data packets or RTS's to the the channel with an aggregate rate of λ packets per unit time. Each node is assumed to have at most one data packet to send at any time, and a node retransmits after a random retransmission delay that on the average is much larger than the time needed for a successful transaction between a transmitter and a receiver and such that all transmissions of RTS's or data packets can be assumed to be independent of one another. The channel is assumed to introduce no errors, so multiple access interference (MAI) is the only source of errors. Nodes are assumed to detect carrier or busy tones perfectly, and the probability of false busy-tone detection is 0.

We assume that there is no power capture by any transmission and hence two or more transmissions that overlap in time in the channel must all be retransmitted, and that any packet propagates to all nodes in exactly τ seconds. The transmit-to-receive and receive-to-transmit turn-around times in the data channel required by a node is ω and is assumed to be larger than the propagation delay τ , which agrees with the parameters assumed in IEEE 802.11 DCF. The transmission time of an ACK, an RTS, or a CTS is γ . In IEEE 802.11, the actual length of a CTS or an ACK is slightly shorter than the length of an RTS, but only by a few bit times, which does not impact

the analysis. The maximum data transmission time allowed in CSMA/CAP is δ and a data-packet length is at most δ .

We assume that processing delays are negligible, which includes the time ξ to detect carrier. The protocols are assumed to operate in steady state, with no possibility of collapse, and hence the average channel utilization of the channel is given by [13]

$$S = \frac{\bar{U}}{\bar{B} + \bar{I}}. \quad (11)$$

where $\bar{B}$ is the expected duration of a busy period, defined to be a period of time during which the channel is being utilized; $\bar{I}$ is the expected duration of an idle period, defined as the time interval between two consecutive busy periods; and $\bar{U}$ is the time during a busy period that the channel is used for transmitting user data successfully.

A. Fully-Connected Scenario

The utilization of the channel with CSMA/CAP in a fully-connected network consists only of idle periods, successful transmission periods during which data packets are sent as part of successful handshakes, or RTS collision intervals (RCI) resulting from the collision of two or more RTS's. Fig. 8 illustrates the idle and busy periods that may occur with CSMA/CAP when all nodes are τ seconds from one another and the length of each data packet is δ . We assume that the length of a pilot is $\rho = 2(\omega + \tau)$.

Fig. 8. Transmission periods in CSMA/CAP

Theorem 2: The throughput of non-persistent CSMA/CAP in a fully-connected network is

$$S_{CAP} = \frac{\delta}{\delta + 2\gamma + 9\omega + 8\tau + \frac{1}{\lambda} + e^{\lambda(\omega + \tau)} (\gamma + \omega + 2\tau)} \quad (12)$$

Proof: A node with a packet to send must first sense the channel before transmitting an RTS, which forces the node to incur a turnaround time ω during which it is unable to listen to the channel. Therefore, the vulnerability period of an RTS is $\omega + \tau$, and the probability that an RTS is transmitted without interference from other RTS's is $P_S = e^{-\lambda(\omega + \tau)}$.

If an RTS is sent without multiple access interference, the intended receiver transmits its CTS back to the sender after receiving the RTS and transmits its pilot immediately

following its CTS. The sender gets ready to transmit its data packet immediately after receiving the CTS, which lasts longer than $\omega + \tau$. The sender waits for $W = \rho + \omega + \tau$ after receiving a CTS to allow the receiver to be listening to its data packet. With the assumption that all data packets have the same length, the delay d imposed on the sender to send its pilot can be set to and hence the sender transmits its pilot immediately after transmitting its data packet. The receiver sends its ACK to the sender after receiving the pilot from the sender. Accordingly, as Fig. 8 illustrates, the length of a successful exchange lasts $T = \delta + 3\gamma + 3(\rho + \omega + 2\tau) + \tau$ seconds. With the assumptions we have made and with $\rho = 2(\omega + \tau)$ we have $T = \delta + 3(\gamma + 3\omega + 3\tau)$.

On the other hand, as shown in Fig. 8, an RTS collision interval (RCI) lasts $Y + \gamma + \tau$ if multiple RTS's collide with one another, where Y is a random variable denoting the length of time between the start of the RCI and the start of the last RTS in the interval.

A collision interval occurs with probability $1 - P_S$. Because arrivals of RTS's are assumed to be Poisson distributed, no more than one RTS can arrive at any one instant and hence $Y = 0$ can occur only when an RTS is successful. Accordingly, the length of an average busy period equals

$$\begin{aligned} \bar{B} &= \bar{Y} + (\gamma + \tau)(1 - e^{-\lambda(\tau + \omega)}) + T e^{-\lambda(\tau + \omega)} \\ &= \bar{Y} + \gamma + \tau + e^{-\lambda(\tau + \omega)}(\delta + 2\gamma + 9\omega + 8\tau) \end{aligned} \quad (13)$$

If the time period between the start of the first and the last RTS in a collision interval equals y seconds, then there are no more RTS arrivals in the remaining time of the vulnerability period of the first RTS of the collision interval, i.e., $\omega + \tau - y$ seconds. Accordingly,

$$\begin{aligned} P(Y \leq y) &= F_Y(y) = P\{\text{no arrivals in } \omega + \tau - y\} \\ &= e^{-\lambda(\omega + \tau - y)} \end{aligned}$$

Therefore, given that Y assumes only non-negative values, the average value of Y equals

$$\begin{aligned} \bar{Y} &= \int_0^\infty (1 - F_Y(t)) dt = \int_0^{\omega + \tau} (1 - e^{-\lambda(\omega + \tau - t)}) dt \\ &= \omega + \tau - \frac{1 - e^{-\lambda(\omega + \tau)}}{\lambda} \end{aligned} \quad (14)$$

Substituting Eq. (14) in Eq. (13) we obtain

$$\bar{B} = e^{-\lambda(\omega + \tau)} \left(\delta + 2\gamma + 9\omega + 8\tau + \frac{1}{\lambda} \right) + \gamma + \omega + 2\tau - \frac{1}{\lambda}$$

The average length of an idle period $\bar{I}$ is simply the average inter-arrival time of packets, which are preceded by pilot transmissions, and this equals $1/\lambda$ because inter-arrival times are exponentially distributed with parameter λ .

The average time period used to transmit useful data $\bar{U}$ is the useful portion of a *successful* busy period, which occurs with probability $e^{-\lambda(\omega + \tau)}$. Accordingly, $\bar{U} = \delta e^{-\lambda(\omega + \tau)}$.

Substituting the values of $\bar{U}$, $\bar{B}$, and $\bar{I}$ into Eq. (11) we obtain Eq. (12). ■

B. Hidden-Terminal Scenario

In this scenario all traffic is sent to a central receiver r and all nodes other than r are hidden from one another.

1) CSMA/CAP: Figure 9 illustrates the collision intervals that may occur in non-persistent CSMA/CAP in our star-network scenario. As the figure shows, the types of transmission periods that may occur in CSMA/CAP with the assumptions we have made are: successful CA handshakes, RTS collision intervals, and idle transmission periods. The following theorem provides the throughput of CSMA/CAP.

Theorem 3: The throughput of non-persistent CSMA/CAP at a central receiver r with a very large population of sources hidden from each other is

$$S_{CAP} = \frac{\delta}{\delta + 3\gamma + 9(\omega + \tau) + \frac{1}{\lambda} + e^{\lambda\gamma} \left(\tau + \frac{1}{\lambda} (e^{\lambda\gamma} - 1) \right)} \quad (15)$$

Fig. 9. Transmission periods in CSMA/CAP with hidden terminals

Proof: A busy period is either an RTS collision interval or a successful CA handshake as illustrated in Fig. 9. Receiver r receives an RTS without MAI if no other RTS is sent during its transmission because all sources are hidden from one another. Therefore, a successful handshake of T seconds occurs with probability $P_S = e^{-\lambda\gamma}$.

If r obtains an RTS without MAI from a given neighbor, it can transmit a CTS to that neighbor and receive its data packet without MAI even when other neighbors transmit RTS's to r concurrently. This is because the additional RTS's sent to r must be transmitted within $\tau + \omega$ of the start of the CTS from r , after which all neighbors of r must detect carrier from the CTS. Once receiver r starts transmitting its CTS, it is unable to hear any transmission from hidden sources until ω seconds after it stops transmitting its pilot. Therefore, given that r ends the transmission of its pilot after all RTS's from hidden sources arrive at r , none of those RTS's is heard by r . On the other hand, the neighbors of r are hidden from each other and the neighbor that sent the first RTS is able to decode the CTS from r successfully. As a result, if an RTS is sent without MAI with probability P_S , the length of time Y between the CTS sent by r and the last RTS sent to r concurrently (see Fig. 9) has no impact on the success of the CA handshake or the duration of the busy period. Accordingly, we have that a

successful transmission period has the same length as in the fully-connected scenario, that is,

$$T = \delta + 3\gamma + 9\omega + 9\tau \quad (16)$$

An RTS collision interval (RCI) consists of a sequence of complete RTS transmissions and all the neighbors of receiver r may participate in the RCI. This results from the fact that the vulnerability period of an RTS is its entire transmission time. An RCI takes place if the first RTS of the interval suffers MAI with probability $1 - P_S$. Each RCI lasts $\tau + R$ seconds, where R is a random variable whose value depends on the number of RTS's involved in the collision interval and the inter-arrival times of the RTS's.

For an RCI to have k RTS's, there must be an RTS arriving during the transmission time of each of the first $k-1$ RTS's and no RTS arriving during the transmission time of the last RTS in the RCI. Given our simplifying assumption of an essentially infinite number of sources around receiver r , this corresponds to the geometric random variable in which the probability of successfully ending the RCI is the probability that no RTS arrives during the γ seconds of the RTS transmission, or $e^{-\lambda\gamma}$. Hence, the average number of RTS's in an RCI is $e^{\lambda\gamma}$.

The inter-arrival times between consecutive RTS's in an RCI are exponentially distributed and each can be at most γ seconds. Therefore, the average of such times is

$$\bar{X} = \int_0^\infty (1 - F_X(t)) dt = \int_0^\gamma e^{-\lambda t} dt = \frac{1}{\lambda} (1 - e^{-\lambda\gamma}) \quad (17)$$

It thus follows that the average value of R is given by

$$\bar{R} = e^{\lambda\gamma} \bar{X} = \frac{e^{\lambda\gamma}}{\lambda} (1 - e^{-\lambda\gamma}) = \frac{e^{\lambda\gamma} - 1}{\lambda} \quad (18)$$

The average length of a busy period is simply

$$\bar{B} = T e^{-\lambda\gamma} + (\bar{R} + \tau)(1 - e^{-\lambda\gamma}) \quad (19)$$

Substituting Eqs. (16) and (18) in Eq. (19) we have

$$\bar{B} = e^{-\lambda\gamma} \left(\delta + 3\gamma + 9\omega + 9\tau \right) + \frac{1}{\lambda} + \tau + \frac{e^{\lambda\gamma} - 2}{\lambda}$$

The proportion of time that the channel is used for data during a successful handshake is $\bar{U} = \delta P_S = \delta e^{-\lambda\gamma}$, and the length of an average idle period is the same as the average inter arrival time of RTS's $\bar{I} = 1/\lambda$. Substituting the values of $\bar{U}$, $\bar{I}$, and $\bar{B}$ into Eq. (11) we obtain Eq. (15). ■

2) *Non-Persistent CSMA with ACK's*: As Figure 10 illustrates, the types of transmission periods that may occur in CSMA with the assumptions of a central receiver and sources hidden from one another are successful transmissions, collision intervals, and idle transmission periods. However, as Figure 11 illustrates, packet transmissions from hidden sources may be sent to the central receiver while the receiver transmits its ACK for a prior data packet received correctly as well as after the ACK is sent. We assume that a source with a packet to send that detects carrier from the central receiver simply backs off for a random time that is larger than the time needed to send a packet and its ACK.

The following theorem provides the throughput of CSMA with ACKs under the assumptions we have made.

Theorem 4: The throughput of non-persistent CSMA with ACKs at a central receiver r with a very large population of sources hidden from each other is

$$S_{CSMA} = \frac{\delta}{\delta + 2\tau + \frac{1}{\lambda} + U e^{\lambda\delta} + V e^{-\lambda\omega} + (\omega + \gamma) e^{-\lambda(\omega + \tau)}} \quad (20)$$

where

$$U = \tau + \frac{e^{\lambda\delta} - e^{-\lambda(\omega + \tau)}}{\lambda} \quad \text{and} \quad V = \frac{e^{-\lambda(\omega + \tau)} - 1}{\lambda}$$

Fig. 10. Example transmission periods in CSMA with hidden sources

Fig. 11. Successful busy period in CSMA with concurrent packets from hidden sources

Proof: To transmit a data packet a source must first sense the channel; however, because all sources are hidden from each other, the central receiver is able to decode a data packet successfully only if no other data packet is transmitted during the transmission time of the data packet being received. Therefore, a successful data packet occurs with probability $P_S = e^{-\lambda\delta}$.

The average length of an idle period $\bar{I}$ is $1/\lambda$ as in the previous protocols, and the average time period used to transmit useful data $\bar{U}$ is simply $\delta P_S = \delta e^{-\lambda\delta}$.

As Figs. 10 and 11 illustrate, a busy period is either a collision interval (CI) or a successful transmission period. A CI occurs if the first packet of the interval suffers MAI with probability $1 - P_S$. Each CI lasts $R + \tau$ seconds, where R is a random variable whose value depends on the number of packets involved in the CI and the packet inter-arrival times. Hence, the average length of a busy periods is

$$\bar{B} = \bar{T} e^{-\lambda\delta} + (\bar{R} + \tau)(1 - e^{-\lambda\delta}) \quad (21)$$

where $\bar{T}$ is the average length of a successful busy period.

For a CI to have k packets there must be a packet arrival during the transmission time of each of the first $k-1$ packets

and no arrival during the transmission time of the last packet of the CI. As it was the case in the proof of Theorem 3, this corresponds to the geometric random variable in which the probability of successfully ending the CI is the probability that no arrivals occur during the δ seconds of the last packet transmission in the CI, i.e., $e^{-\lambda\delta}$. Hence, the average number of packets in a CI is $e^{\lambda\delta}$.

The inter-arrival times between consecutive packets in a CI are exponentially distributed and each can be at most δ seconds. Therefore, the average of such times is

$$\bar{X} = \int_0^\infty (1 - F_X(t))dt = \int_0^\delta e^{-\lambda t} dt = \frac{1}{\lambda} (1 - e^{-\lambda\delta}) \quad (22)$$

Therefore, the average value of R is

$$\bar{R} = e^{\lambda\delta} \bar{X} = \frac{e^{\lambda\delta}}{\lambda} (1 - e^{-\lambda\delta}) = \frac{e^{\lambda\delta} - 1}{\lambda} \quad (23)$$

As Figs. 10 and 11 illustrate, a successful busy period lasts only $\delta + \gamma + \omega + 2\tau$ seconds if no data packets are transmitted concurrently with the ACK from the central receiver (see Fig. 10) or much longer if sources transmit data packets concurrently or after the ACK from the central receiver (see Fig. 11). The first case occurs with probability $e^{-\lambda(\omega+\tau)}$, because the receiver incurs ω seconds of turnaround delay before it sends its ACK and the ACK itself propagates to all other nodes in τ seconds, after which nodes detect carrier and must back off if they have data packets to send while the ACK is still being transmitted. The second case of course occurs with probability $1 - e^{-\lambda(\omega+\tau)}$.

Figure 11 illustrates the case in which data packet transmissions occur concurrently with the ACK transmission from the central receiver r . The busy period is considered from the standpoint of receiver r . Given that source nodes cannot hear one another, the data packets arriving at receiver r cannot interfere with the reception of the ACK at the source node being addressed by r . However, hidden sources may transmit data packets up to ω seconds before the ACK from r and transmissions of data packets may continue arriving at r after it finishes transmitting its ACK.

The average length of a successful busy period in which data packets are sent concurrently with the ACK from the central receiver equals $\delta + \tau + \bar{Z} + \bar{R} + \tau$, where Z and R are two random variables.

The length of R is determined by the Poisson arrival times of data packets at the central receiver and hence $\bar{R}$ is given by Eq. (18). The length of random variable Z is the time from the arrival of the successful data packet at receiver r to the arrival at r of the *first* data packet sent by a hidden source. Hence, it can assume values in the interval $[0, \omega]$ and we can compute $\bar{Z}$ as we did in the proof of Theorems 2 and 3 as follows:

$$\bar{Z} = \int_0^\omega (1 - P(Z \leq t))dt = \int_0^\omega e^{-\lambda t} dt = \frac{1}{\lambda} (1 - e^{-\lambda\omega}) \quad (24)$$

From the above, we have that a successful busy period always starts with a successful data packet that propagates

to the central receiver r , followed by either the transmission of an ACK from r with no concurrent data packet transmissions (which occurs with probability $e^{-\lambda(\tau+\omega)}$) or an ACK transmitted concurrently with data packets from other sources (which occurs with probability $1 - e^{-\lambda(\tau+\omega)}$). Accordingly, the average length of a successful busy period is

$$\bar{T} = \delta + \tau + e^{-\lambda(\tau+\omega)}(\gamma + \omega + \tau) + (1 - e^{-\lambda(\tau+\omega)})(\bar{Z} + \bar{R} + \tau) \quad (25)$$

Substituting Eqs. (23) and (24) In Eq. (25) we have

$$\bar{T} = \delta + 2\tau + e^{-\lambda(\tau+\omega)} \left[\gamma + \omega + \frac{e^{-\lambda\omega}}{\lambda} \right] + \frac{(1 - e^{-\lambda\tau})e^{\lambda-\omega}}{\lambda} \quad (26)$$

Substituting Eqs. (23) and (26) in Eq. (21) results in the following expression for $\bar{B}$ after some simplification:

$$\begin{aligned} \bar{B} = & \frac{(e^{\lambda\delta} - 1)}{\lambda} + \tau + e^{-\lambda\delta} \left[\delta + 2\tau + \frac{1 - e^{-\lambda\omega}}{\lambda} \right] \\ & + e^{-\lambda\delta} e^{-\lambda(\omega+\tau)} \left[\omega + \gamma + \frac{e^{-\lambda\omega} - e^{-\lambda\delta}}{\lambda} \right] \end{aligned} \quad (27)$$

Substituting the values of $\bar{T}$ and $\bar{U}$ and Eq. (27) in Eq. (11) we obtain Eq. (20) after some simplification. ■

VI. PERFORMANCE COMPARISON

We assume that the data rate is 1 Mbps for the entire available bandwidth, and that an RTS and an ACK lasts 352 bits including the MAC and the physical-layer headers. We also assume that ω is 10 μ s, which agrees with the characteristics of half-duplex transceivers available today.

A. Results for Fully-Connected Scenario

We use Eq. (12) for CSMA/CAP and the following result for CSMA, which is derived in [7] using the same assumptions made in this paper.

$$S_{CSMA} = \frac{\delta}{\alpha + \omega + \tau + \frac{1}{\lambda} + e^{\lambda(\omega+\tau)}(\delta + \omega + 2\tau)} \quad (28)$$

Figure 12 shows the results for a wireless local-area network (WLAN) scenario that highlights the additional overhead incurred by CSMA/CAP over CSMA in order to eliminate MAI on data packets and ACK's. Physical distances are around 500 meters, and the duration of a data packet is 1500 bytes including the physical and MAC-layer headers, which corresponds to an average-length IP packet and takes 0.012s to transmit at 1 Mbps. We use a normalized propagation delay of 1×10^{-4} .

As expected, the maximum throughput attained by CSMA/CAP is lower than the one attained by CSMA. This is a direct consequence of the additional signaling and waiting times used in CSMA/CAP to prevent MAI on data packets or ACK's. However, as the results also show, CSMA/CAP is more stable than CSMA as channel load increases, which is due to the shorter duration of collision intervals in CSMA/CAP compared to CSMA.

B. Results with Hidden Terminals

Figure 13 shows the throughput of pure ALOHA [1], CSMA/CAP (Eq. (15)), and CSMA (Eq. (20)). The same parameter values of the fully-connected scenario are used.

The results illustrate the advantage of using pilots as part of collision avoidance compared to simply using carrier sensing in the presence of hidden terminals. The throughput of CSMA with ACKs degrades to almost that of ideal ALOHA with no ACKs. This performance degradation can be understood intuitively from Figures 10 and 11. As the figures illustrate, both successful and unsuccessful busy periods in CSMA with ACKs contain trains of colliding data packets and the vulnerability period of any such packet is its entire transmission time, just as in pure ALOHA. Only a few successful transmission periods consist of a single data packet and an ACK, and only a relatively small number of sources with packets to send back off after detecting carrier from the ACK (see Figure 10). The performance degradation due to hidden terminals in CSMA/CAP is due to the fact that, as Figure 9 illustrates, an RTS arriving at the central receiver is vulnerable for its entire duration, rather than just for $\tau + \omega$ seconds.

Fig. 12. S vs. G in a fully-connected network

Fig. 13. S vs. G with hidden terminals

VII. CONCLUSIONS

We introduced CSMA/CAP and showed that no data packets or ACK's can collide with other transmissions at the intended receivers, and that senders receive ACK's correctly. We compared the throughput attained with CSMA/CAP and CSMA when all data packets have the same length in a fully-connected WLAN and a worst-case scenario of hidden terminals in which no source can hear other sources when transmitting to a central receiver. The results clearly show that CSMA/CAP is a viable approach to implementing collision avoidance correctly and efficiently in multi-hop ad-hoc networks. It provides a marked improvement over CSMA in multi-hop ad-hoc networks, and the degradation in maximum throughput for CSMA/CAP compared to CSMA is relatively small in fully-connected networks.

Our future work focuses on embedding CSMA/CAP in IEEE 802.11 DCF, analyzing the energy consumption [2] and performance of CSMA/CAP in more complex scenarios, and comparing CSMA and CSMA/CAP with variable-length packets is important. The third topic is important. Sending packets shorter than the maximum length allowed reduces the throughput of CSMA/CAP; however, it is well known that allowing variable-length data packets causes a significant decrease in the throughput of channel access protocols like ALOHA and CSMA [1].

ACKNOWLEDGMENTS

This work was supported in part by the Jack Baskin Chair of Computer Engineering at UC Santa Cruz.

REFERENCES

- [1] N. Abramson, "The Throughput of Packet Broadcasting Channels," *IEEE Trans. Commun.*, Jan. 1977.
- [2] M. Carvalho et al., "Modeling Energy Consumption in Single-Hop IEEE 802.11 Ad Hoc Networks," *Proc. IEEE ICCCN '04*, 2004.
- [3] C. L. Fullmer and J.J. Garcia-Luna-Aceves, "Solutions to Hidden Terminal Problems in Wireless Networks," *Proc. ACM SIGCOMM '97*, 1997.
- [4] C. L. Fullmer and J.J. Garcia-Luna-Aceves, "FAMA-PJ: a channel access protocol for wireless LANs," *Proc. ACM MobiCom '95*, 1995.
- [5] J.J. Garcia-Luna-Aceves and A. Tzamaloukas, "Receiver-Initiated Collision Avoidance in Wireless Networks," *Wireless Networks*, 2002.
- [6] J.J. Garcia-Luna-Aceves, "Carrier-Sense Multiple Access with Collision Avoidance and Detection," *Proc. ACM MSWIM '17*, 2017.
- [7] J.J. Garcia-Luna-Aceves, "Carrier Resolution Multiple Access," *Proc. ACM PE-WASUN '17*, 2017.
- [8] J.J. Garcia-Luna-Aceves, "Carrier-Tone Multiple Access with Collision Avoidance and Detection," *Proc. IEEE WCNC '18*, 2018.
- [9] J.J. Garcia-Luna-Aceves and Marcelo M. Carvalho, "Collaborative Collision Detection with Half-Duplex Radios," *Proc. IEEE WCNC '18*, 2018.
- [10] Z. Haas and J. Deng, "Dual Busy Tone Multiple Access (DBTMA)—A Multiple Access Control Scheme for Ad Hoc Networks," *IEEE Trans. Commun.*, June 2002.
- [11] K. Jamieson et al., "Understanding The Real-World Performance of Carrier Sense," *Proc. ACM E-WIND '05*, 2005.
- [12] P. Karn, "MACA—A New Channel Access Method for Packet Radio," *Proc. ARRL/CRRL*, 1990.
- [13] L. Kleinrock and F. A. Tobagi, "Packet Switching in Radio Channels: Part I - Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics," *IEEE Trans. Commun.*, 1975.
- [14] F. A. Tobagi and L. Kleinrock, "Packet Switching in Radio Channels: Part II - The Hidden Terminal Problem in Carrier Sense Multiple-Access Modes and The Busy-Tone Solution," *IEEE Trans. Commun.*, 1975.