On the Hidden Terminal Jamming Problem in IEEE 802.11 Mobile Ad Hoc Networks

Christopher Ware, Tadeusz Wysocki, Joe Chicharo
Telecommunications Research Centre
University Of Wollongong
Wollongong, Australia, 2522
chris@snrc.uow.edu.au

Abstract—**This paper addresses recent experimental measurements from an IEEE 802.11 ad hoc network testbed, which indicate a strong signal strength dependence in the ability of a hidden terminal to gain access to the radio channel. We present analytical results investigating the 'hidden terminal jamming' ability of the IEEE 802.11 DSSS physical layer. Results indicate that in a hidden terminal topology, the presence of an interfering transmission with a signal strength marginally greater than the transmission currently being received will result in an intolerable increase in BER, effectively jamming the ongoing transmission. These results confirm previous experimental measurements which show that after a number of MAC layer timeout/retransmission periods, the original (weaker) connection is effectively prevented from gaining access to the channel.**

I. Introduction

The continued desire for mobile, 'anywhere, anytime' networking has contributed greatly to the current interest in Mobile Ad Hoc Networks (MANET's). The dynamic nature of a MANET is such that hidden terminal scenario is likely to be common. Therefore, a MAC protocol capable of overcoming this problem needs to be employed. The IEEE 802.11 MAC protocol potentially represents a good solution for MANET's, having been implemented by many manufacturers, and also including the Request-To-Send / Clear-To-Send (RTS/CTS) handshake to provide MAC layer protection against hidden terminal collisions.

However, recent experimental measurements [1] have indicated that the IEEE 802.11 [2], [3] medium access control and physical layer protocols may be inherently susceptible to hidden terminal induced channel capture. We define 'hidden terminal jamming' as the phenomena where transmissions from a hidden transmitter using a spreading code within the available sequence set can effectively jam an ongoing hidden transmission. We investigate the hidden terminal jamming capability of 802.11 in an identical scenario to that employed experimentally in [1], in an effort to explain these results.

In this paper we use previous results [4], [5] for a Binary Phase Shift Keying (BPSK) modulated Direct Sequence Spread Spectrum (DSSS) signal to investigate the impact an interfering transmission has on the Bit Error Rate (BER) experienced by an existing transmission for the 802.11 DSSS physical layer. Our results indicate that the DSSS physical layer is susceptible to jamming when hidden terminals are competing for channel access.

IEEE 802.11 Distributed Coordinate Function (DCF) compliant modems employed in a hidden terminal ad hoc mode have illustrated a strong signal power dependence on the ability of contending hidden connections to gain access to a radio channel [1], despite the RTS/CTS handshake. Measurements indicate that a difference of < 5 dB was sufficient to prevent a weaker host from accessing the channel, while the stronger host was able to achieve reliable, consistent throughput. In the case where signal levels were equal, the channel was effectively shared using the RTS/CTS handshake. This is contrary to expectation, as with this handshake we anticipate a reasonably fair distribution of channel access relatively independent (within reason) of the signal strength of either receiver particularly given the capture ability of the radio modem providing some immunity to an external noise signal.

The remainder of the paper is organised as follows: in Section II we review details of the 802.11 DSSS physical layers, in Section III we present our analysis of the experimental scenario employed in [1], with numerical results following in Section IV. Section V concludes the paper.

II. IEEE 802.11

The original IEEE 802.11 standard [2] defines a Medium Access (MAC) Protocol, and three distinct physical layers: an Infra-Red physical layer (IR), and two spread spectrum layers, one based on Frequency Hopping Spread Spectrum (FHSS), and another using Direct Sequence Spread Spectrum (DSSS). The 802.11 standard was updated [3] with the addition of the High Rate (HR) physical layer extensions. This allowed the DSSS physical layer to operate at 5.5 Mbit/sec and 11 Mbit/sec in addition to the original 1 and 2 Mbit/sec.

At the MAC layer, the Distributed Co-ordinate Function (DCF) implements CSMA/CA, with an RTS-CTS-DATA-ACK handshake. This scheme is able to operate in a peer-to-peer ad hoc mode, being a fully distributed MAC protocol. There is also an optional Point Co-ordinate Function (PCF) which implements a polling scheme, controlled by a central base station. This approach may potentially operate quite well with hidden terminals, though currently is unable to be employed in an ad hoc mode. The analysis in this paper will concentrate on the self jamming ability of the DSSS physical layer, therefore we briefly review the properties of both the Basic and High Rate DSSS.

TABLE I

802.11 DSSS Modulation Techniques and Spreading Codes

Bit Rate (MBit/s)	**Coding Scheme**	**Modulation Technique**	**Bits per Symbol**
1	Barker Sequence (11 Chip)	DBPSK	1
2	Barker Sequence (11 Chip)	DQPSK	2
5.5	CCK or optional BCC	DQPSK	4
11	CCK or optional BCC	QPSK	8

TABLE II

QPSK Encoding Scheme

Bit Pattern[d_i, d_{i+1}]	**Phase**
00	0
01	$\pi/2$
10	π
11	$3\pi/2(-\pi/2)$

A. Direct Sequence Spread Spectrum Physical Layer

The DSSS physical layer for 802.11 provides 4 different bit rates. As illustrated in Table I, each of the 4 data rates employ a different combination of modulation technique and spreading code to achieve the desired symbol rate, and number of bits per symbol. The Basic Rate (BR) comprises the 1 and 2 Mbit/s data rates, and employs a Barker spreading code with DBPSK or DQPSK respectively. The common 11 chip code used by all stations for both the 1 and 2 Mbit/sec physical layers is

+1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1

The HR-DSSS physical layer, comprising the 5.5 and 11 Mbit/s rates, employs Complementary Code Keying (CCK) with a spreading code of length 8, generated by a generalised Haddamard transform (1) where ϕ_1 is added to all code chips, ϕ_2 to all odd code chips, ϕ_3 to all odd pairs, and ϕ_4 to all odd quads of code chips. In each case, the chipping rate is 11 Mchip/sec.

$$\begin{aligned} c \quad = \quad & e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_3+\phi_4)}, \\ & e^{j(\phi_1+\phi_2+\phi_4)}, -e^{j(\phi_1+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_3)}, \\ & e^{j(\phi_1+\phi_3)}, -e^{j(\phi_1+\phi_2)}, e^{j\phi_1} \qquad (1) \end{aligned}$$

(1) is used to create 8 complex chips (c_0 to c_7) with c_0 transmitted first in time. For CCK 5.5 MBit/s modulation at 4 bits/symbol, ϕ_1 is encoded by data bits d_0 and d_1 based on DQPSK. Data bits d_2 and d_3 CCK encode the basic symbol by

$$\phi_2 \quad = \quad d_2 \times \pi + \frac{\pi}{2} \qquad (2)$$

$$\phi_3 \quad = \quad 0 \qquad (3)$$

$$\phi_4 \quad = \quad d_3 \times \pi \qquad (4)$$

This leads to a family of 16 distinct spreading sequences which are used to indicate the symbol transferred.

For CCK 11 Mbit/sec modulation (at 8 bits/symbol), ϕ_1 is again encoded by d_0 and d_1 using DQPSK. Data bits (d_2, d_3), (d_4, d_5),and (d_6, d_7) are used to QPSK encode ϕ_2, ϕ_3, and ϕ_4 respectively, as shown in Table II

This leads to a matrix of 256 potential spreading sequences supporting the transmission of 8 bits per symbol.

III. Error Probability of Received Frame

The results presented in [1] illustrate a distinct relationship between the ability of a host to capture the radio channel, and the signal strength of each contending frame measured at the receiver. This is a problem specific to the hidden terminal topology, where the standard CSMA/CA access mechanism is unable to sense a transmission that may result in a collision at the intended receiver. A successful transmission relies on the reception of an RTS frame by the intended receiver.

Referring to Fig. 1, when hidden terminals are attempting to communicate with a common receiver, we consider two possible collisions which may occur at the receiver:

1. an RTS frame from connection A collides with a DATA frame from connection B
2. an RTS frame from connection A collides with an RTS currently under reception from connection B

In each case the eventual behaviour will be dependent on many additional factors, including the timing of the interfering frame arrival, and the relative signal power of both transmissions. In case 1 the contention will be handled by the MAC protocol. However, the measurements in [1] show that the stronger host will able to capture the channel after a number of backoff periods. Even though the RTS frame is relatively small, 40 bytes compared to several hundred for the data frame, there is a high probability that the data frame will be corrupted by the collision if the signal energy is sufficiently high. This then provides an opportunity for the stronger host to prevent a weaker host from gaining access to the channel through a number of timeout and retransmission cycles. This case is further complicated by the fact that all control messaging (RTS/CTS etc.) are transmitted at the highest common transmission rate supported by all known nodes in the network. Thus there is the potential for a transmission spread using the Barker sequence to collide with a data frame spread using the CCK codes generated with (1).

In case 2, the receiver will either retain capture of the original RTS frame and return a valid CTS, or will loose both of the frames, unable to respond with a CTS until an RTS is correctly received. The experimental results in [1] suggest that the stronger host will win this contention period, and be able to capture the channel.

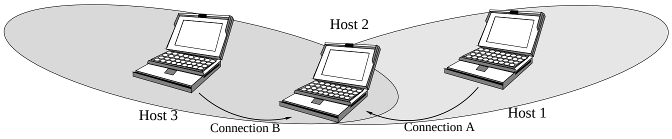

Fig. 1. Experimental Topology

To examine the impact of an interfering transmission on the reception of a previously acquired frame, we have investigated the resulting BER obtained at the output of a correlation spread spectrum receiver. The model assumes that the initial frame, y, is currently being received, at $T > T_a$, where T_a is the time required by the correlation receiver to acquire and achieve synchronisation with the signal, the *acquisition time*. An asynchronous interfering frame, x, arrives at a time $T_2 > T_a$. For both the BR-DSSS and HR-DSSS physical layers, we determine the impact this has on the correlation receiver output BER as a function of the relative power difference between the signals, and hence the ability of the receiver to maintain capture of the initial frame.

Our analysis for the DSSS physical layer is based on results in [4]. The original result for the SNR experienced by the yth user, at the correlator output of a BPSK asynchronous DS-CDMA receiver is given by

$$SNR_y = \left[\frac{N_o}{2E_{by}} + \frac{1}{6N^3} \sum_{x=1, x \neq y}^{K} r_{x,y} \right]^{-\frac{1}{2}} \tag{5}$$

where K is the total number of concurrent transmissions received (including the yth frame whose BER we are investigating), N_o the one sided noise power spectral density, E_{b1} the bit energy of the yth frame, N the sequence length, and $r_{x,y}$ is the Average Interference Parameter (AIP). The AIP can be approximated [6] as

$$r_{x,y} \simeq 2 \sum_{l=1-N}^{N-1} |C_{XY}(l)|^2 \tag{6}$$

where C_{XY} is the aperiodic cross correlation between the two sequences, defined as

$$C_{XY}(l) = \begin{cases} \sum_{k=0}^{N-1-l} u_X(k) u_Y^*(k+l) & 0 \leq l \leq N-1 \\ \sum_{k=0}^{N-1+l} u_X(k-l) u_Y^*(k) & 1-N \leq l \leq 0 \\ 0 & \text{elsewhere} \end{cases} \tag{7}$$

We define the relative signal strength between the contending frames as

$$\delta_x = \frac{E_{bx}}{E_{by}} \tag{8}$$

where E_{bx} and E_{by} are the respective signal bit energies for each frame. If we assume that the interferring frame x arrives with a signal power δ_x times greater than the current frame y, (5) can be written as

$$SNR_y = \left[\frac{N_o}{2E_{by}} + \frac{1}{3N^3} \sum_{x=1, x \neq y}^{K} \delta_x^2 \sum_{l=1-N}^{N-1} |C_{XY}(l)|^2 \right]^{-\frac{1}{2}} \tag{9}$$

The BER is then expressed as

$$BER_y = Q\left(SNR_y\right) \tag{10}$$

where Q is the complementary error function.

A. DSSS Basic Rate Physical Layer

The use of a single spreading code for the both basic rates allows us to simplify (9). The aperiodic cross correlation C_{XY} is replaced by the autocorrelation function, C_{XX} for the Barker sequence employed. Combined with the approximation derived in [6], the final SNR expression reduces to

$$SNR_y = \left[\frac{1}{2} \frac{N_o}{E_{by}} + \sum_{x=1, x \neq y}^{K} \alpha \delta_x^2 \right]^{-\frac{1}{2}} \tag{11}$$

where $\alpha = 480.3$. This analysis assumes BPSK modulation. The BR-DSSS PHYS employs DBPSK for the 1 Mbit/s rate, and DQPSK for the 2 Mbit/s rate. A practical system employing differential modulation will require even higher SNR at the receiver to achieve equivalent BER performance [7].

B. DSSS High Rate Physical Layer

Spreading codes for the high rate physical layer are generated using (1) resulting in 16 complex codes for the 5.5 Mbit/s rate at to 4 bits per symbol, and 256 distinct complex spreading codes for the 11 Mbit/s rate at 8 bits per symbol. For each rate, we use (5) to generate an expression for the output BER.

If we again use the ratio of bit energies for the current and interfering frame, δ_x, and the approximations of the previous section, we can use (9) to determine the SNR for the yth frame, averaging this result across all sequences in the set to determine the average probability of error.

IV. Numerical Results

A. Single Interferer

This scenario corresponds to Host 1 in Fig. 1 attempting to send an RTS or DATA frame to Host 2, who is currently involved in the reception of a frame from Host 3. The BER given by (10),(11), and (5) has been calculated for a range of E_{b1}/N_o values, as a function of δ. In each of Fig. 2, 3, and 4 it is evident that the presence of the single interfering frame from Host 1 has a detrimental impact on the BER of the frame currently being received from Host 2.

The results for the BR-DSSS 1 and 2 Mbit/s rates are shown in Fig. 2. With $\delta = 0$ dB, the interfering frame arrives with a signal power equal to the current frame. At higher E_{b1}/N_o the presence of the interfering transmission will increase the BER of the initial frame, but will still allow a high probability of successful reception of the initial frame. In this case, both connections will have an equal impact on the other, providing the MAC protocol with a relatively fair scenario to operate. This result provides a strong basis for the fair channel access reported in [1] in the case where each connection had an equal SNR measured at the receiving host.

With $\delta = 5$ dB, the presence of the interfering frame raises the BER to $\sim 10^{-1.5}$, significantly reducing the probability of successful reception of the initial frame. Again, this explains the results in [1] where a 5dB difference in signal power on the 'stronger' link is sufficient to prevent the weaker host from obtaining access to the channel.

It is also possible to view the curves in reverse. If an interfering frame arrives with $\delta < 0$ dB, then the current frame will suffer little increase in BER and retain a high probability of successful reception.

The calculations for the HR-DSSS were performed by averaging the SNR as given by (5) across the entire number of sequences in the set. This requires the calculation of the interference parameter, $r_{x,y}$ for each sequence in the set. In this case, the 'x' sequence corresponds to the sequence currently being received, and the 'y' sequence the interferer. The number of codes in the set represents the number of interfering transmissions across which the result must be averaged.

For the 5.5 Mbit high rate sequence set shown in Fig. 3 the BER follows very closely that of the single barker sequence employed by the BR-DSSS. In the case of the 11 Mbit/s rate (Fig. 4) the BER impact is marginally worse, being approximately $10^{-0.5}$ higher than for the BR-DSSS at $\delta = 0$ dB. This difference is relatively insignificant, as in either case, the presence of an interfering frame with $\delta > 0$ dB will, with a high probability, corrupt the current transmission.

B. Multiple Interferers

Fig. 5 illustrates the impact multiple interferers have on the average BER for the BR-DSSS 1 and 2 Mbit/s rates. As the number of interfering frames is increased, the average BER is increased significantly.

Fig. 6 illustrates this for 11 Mbit/s with $E_b/N_o = 20$ dB. Again, as the number of interferers is increased, the BER is significantly increased. In practice, a single interferer with $delta > 2$ dB will be sufficient to jam a competing hidden transmission.

These results indicate that a host may be unable to successfully access the radio channel when competing with a hidden terminal having a marginally higher signal strength. Transmissions from any terminal are potentially jammed by the stronger connection, making the RTS/CTS handshake effective for the strongest host only.

As stated earlier, this analysis is based on the assumption of a BPSK modulated signal. Therefore, the results can be considered to represent an ideal case, as more complex modulation schemes require a higher signal strength at the receiver to achieve an equal BER. Given this analysis indicates quite conclusively that the hidden terminal jamming problem is responsible for the behaviour presented in [1], analysis of differential and quadrature modulation schemes are not considered necessary.

The results presented here illustrate that an interfering frame

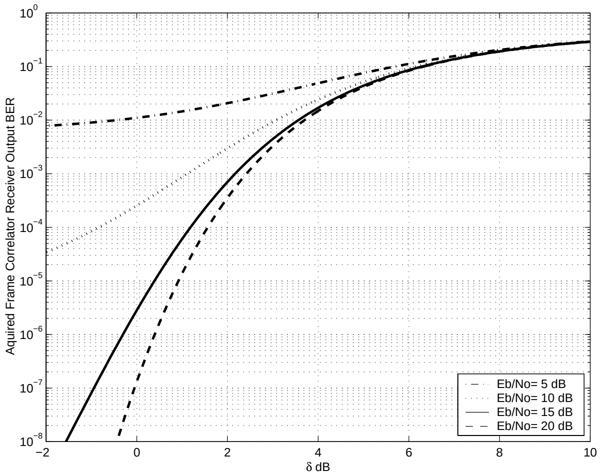

Fig. 2. Correlator Output BER Experienced by Initial Frame for 2 Mbit/s Barker spreading code

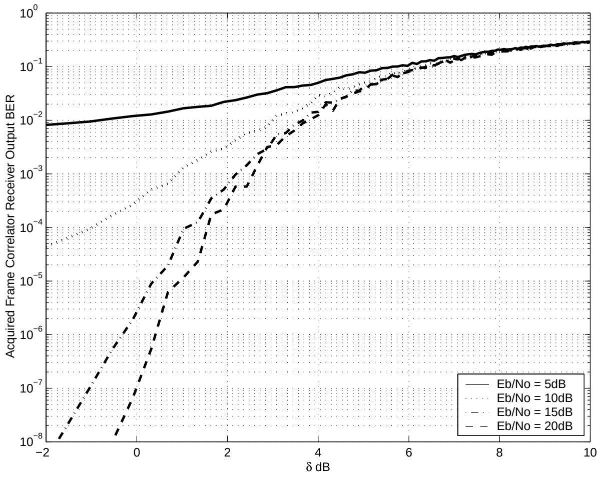

Fig. 3. Correlator Output BER Experienced by Initial Frame for 5.5 Mbit/s Spreading Sequence Set

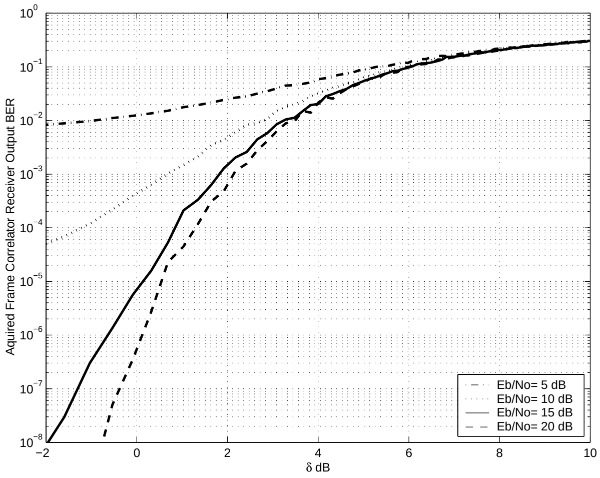

Fig. 4. Correlator Output BER Experienced by Initial Frame for 11 Mbit/s Spreading Sequence Set

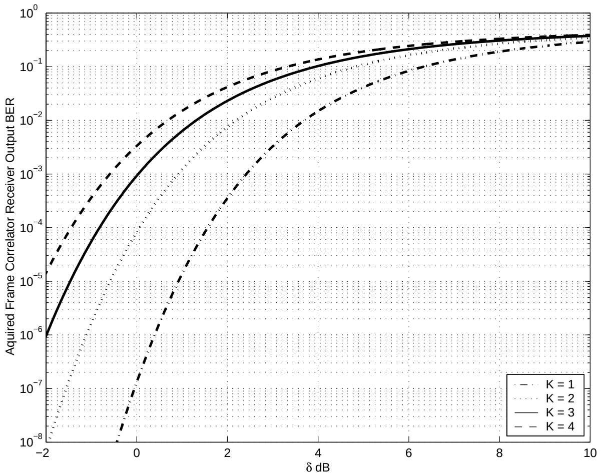

Fig. 5. Barker Code K interferers, $E_b/N_o = 20dB$

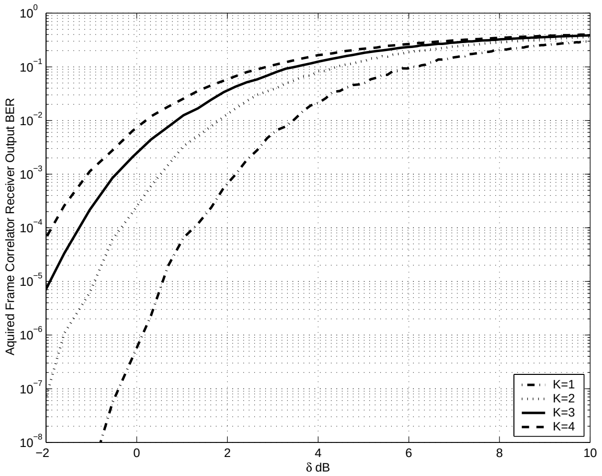

Fig. 6. CCK codes, K interferers, $E_b/N_o = 20dB$

with a higher signal strength, arising from a hidden terminal has the potential to effectively jam the reception of a prior frame. This phenomena is particularly likely in mobile ad hoc networks, where hidden terminals can be expected to be common.

V. Conclusions

In this paper we have presented analytical and numerical results describing the hidden terminal jamming problem present in IEEE 802.11 ad hoc networks. We have developed specific analytical expressions describing the BER of a received frame for the IEEE 802.11 DSSS physical layers, providing an explanation for this phenomena. Our results indicate that a signal differential as small as 2dB is sufficient for the stronger transmission to effectively jam a weaker transmission, closely matching experimental measurements. This renders the RTS/CTS handshake ineffective for all but the connection with the highest signal strength. Such scenarios are likely for a hidden terminal topology where the MAC protocol relies on the RTS/CTS handshake to prevent hidden terminal collisions. This leads to the conclusion that improvements are required in the current IEEE 802.11 physical layer to prevent such multiple access interference if it is to be used reliably in future ad hoc network applications.

References

[1] C G Ware, J Judge, J F Chicharo, and E Dutkiewicz. Unfairness and capture behaviour in 802.11 adhoc networks. In *International Conference on Communications*, volume 1, New Orleans, 2000. IEEE Press.

[2] Institution of Electrical and Electronic Engineers. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1997.

[3] Institution of Electrical and Electronic Engineers. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Higher Speed Physical Layer Extension in the 2.4 GHz Band, 1999.

[4] M B Pursley. Performance evaluation for phase coded spread spectrum multiple access communication - part 1: System analysis. *IEEE Transactions on Communications*, COM-25(8):795–799, 1977.

[5] I Opperman and B S Vucetic. Complex spreading sequences with a wide range of correlation properties. *IEEE Transactions on Communications*, 45(3):365–375, 1997.

[6] K. H. Karkkainen. Mean-square cross correlation as a performance measure for spreading code families. In *IEEE 2nd Int. Symp. on Spread Spectrum Techniques and Applications*, Yokohama, Japan, 1992.

[7] John G. Proakis. *Digital Communications*. McGraw Hill, third edition, 1995.