IEEE 802.11
Wireless Access Method and Physical Layer Specifications

Hidden Terminal Problems in Wireless LANs

June 17, 1993

Dick Allen
Apple Computer, Inc.
One Infinite Loop, MS 301-4J
Cupertino, CA 95014

Abstract
Indoor propagation conditions create a severe hidden terminal problem for wireless LANs depending on carrier sense methods. This problem is more severe than widely recognized and will cause serious degradation of such systems unless robustness is provided through other means.

MAC proposals employing "RTS-CTS-ACK" attempt to propagate channel use information over a wider area to inhibit possible colliding transmissions. These systems are shown to be inadequate when used in typical indoor environments, pointing-out the need for additional robustness at the PHY layer.

Introduction

Carrier Sense Multiple Access (CSMA) protocols have been proposed for wireless LANs to distribute the medium access method among all terminals, allowing creation of ad hoc LANs. These methods have been criticized by others (Chandros Rypinski, "Limitations of CSMA in 802.11 Radiolan Applications," IEEE P802.11/91-46a and Dale Buchholz, "Comments on CSMA," IEEE P802.11/91-49). The objections of Chandos Rypinski:

> "...a small system on a given channel would be inhibited from transmitting by signals originating from an illogically great distance..."; and
> "There is a non-obvious difficulty with CSMA. When a Station about to transmit hears no signal, it is not a conclusive indication that no interference will be created. The case exists for a distant communication where the distant transmitter is inaudible, but if transmission is initiated, the distant receiver will be interfered with."

One proposal to 802.11 for a wireless MAC attempting to overcome the above objections is a variation of a protocol described by Phil Karn ("MACA-A New Channel Access Method for Packet Radio," ARRL/CRRL Amateur Radio 9th Computer Networking Conference, September 22, 1990) and expanded by Ken Biba ("A Hybrid Wireless MAC Protocol Supporting Asynchronous and Synchronous MSDU Delivery Services", IEEE 802.11/91-92) known as "RTS-CTS-ACK." This, in turn, is built on the "RTS-CTS" protocol used by Apple's LocalTalk network. Briefly, a station desiring to transmit, after listening to determine that the channel is not in use, sends a Request to Send packet (RTS) containing the destination address and the length of the packet to be sent. The destination terminal responds with a Clear to Send (CTS) packet containing the length it received in the RTS packet. On receipt of a CTS, the original terminal sends the data packet which is then acknowledged (ACK) by the destination terminal if it is correctly received.

These proposals attempt to minimize the possibility that terminals beyond the range of the originating terminal will unwittingly transmit during the data packet. This is accomplished by having the receiving terminal transmit the CTS containing the packet length. Any station receiving either the RTS or CTS knows that it must not transmit during a definite time interval determined by the packet length. Thus possible collisions from terminals which can receive the CTS but not the RTS are avoided. The channel-in-use information is broadcast over a wider range than could be attained by the originator.

Unfortunately, terminals which are unable to receive either the RTS or the CTS will not be aware of the possible collision and may disrupt the data transmission. I will show that a large number of potential interferers may be unable to receive either the RTS or the CTS.

Indoor Propagation Model

The propagation model is based on the submission by Bruce Tuch (IEEE P802.11/91-69) applied to a single floor. An attenuation exponent of -3.6 and a 2nd order crossover point of 8.5 meters is used. The average attenuation (assuming a distance greater than the second order crossover) is then 36 log(d/8.5)+20 log(8.5/1)+ 20 log(4π/lambda). For example, at 50 meters the average attenuation is 86.3 dB.

In a multipath environment, fading complicates the picture. In addition to the average propagation, a signal may be attenuated by destructive interference caused by differing phase shifts along the multiple propagation paths. The Rayleigh fading model has been proposed for indoor propagation and gives a reasonable match to empirical data (Bruce Tuch, "An Engineer's Summary of an ISM Band Wireless LAN," IEEE P802.11/91-68). This multipath channel is usually characterized statistically to answer the question: "Given a percentage of time a fading attenuation value may be exceeded what is the maximum fading value which must be allowed for." This paper will work with a 99.9% coverage area (0.1% of the area exceeds the resulting fade level). Without any antenna diversity Rayleigh fading produces a fade of 28 dB at 99.9% coverage. With two level switched antenna diversity (a method which has been proposed to reduce the required fade margin) the fade is reduced to 12 dB at 99.9% coverage. (See "Communication Systems & Techniques", Schwartz, Bennett, Stein.)

Capture Effects

The effect of co-channel interference may be reduced in frequency modulation systems by the so called capture effect. If a desired signal exceeds the sum of all the interfering signals by some amount, the interferers are suppressed. Typical systems may have capture effects allowing successful reception if the interferers are 10 dB below the desired signal.

The Interference Problem

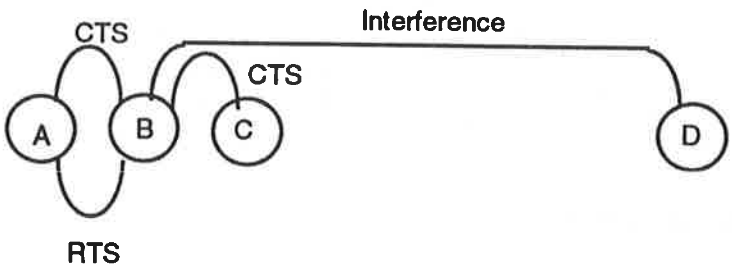

Fig. 1

In Fig. 1, The design transmission distance is assumed to be 50 meters. Beyond this distance, reliable communication is assumed to be impossible. Terminal A and B are assumed to be separated by a distance of 50 meters. Terminal C is assumed to be separated from terminal B by a distance of 50 meters. Terminal A initiates transmission to terminal B by sending a RTS. Terminal B sends a CTS which is successfully received by terminals A and C, initiating the data transmission from A to B, but is not received by terminal D due to its distance from B exceeding 50 meters. In this scenario, terminal D is unaware of the transmission from A to B and may begin a transmission to some other terminal within its range (but beyond the range of A or B). This transmission will cause destructive interference at terminal B unless it is attenuated by at least 10 dB (or whatever the capture ratio is) more than A's transmission.

Fig. 2 shows the faded and unfaded (99.9% coverage, 2 level switched diversity) signal strengths and path losses at distances from 10 to 200 meters assuming transmitter power of 20 dBm and no antenna gain.

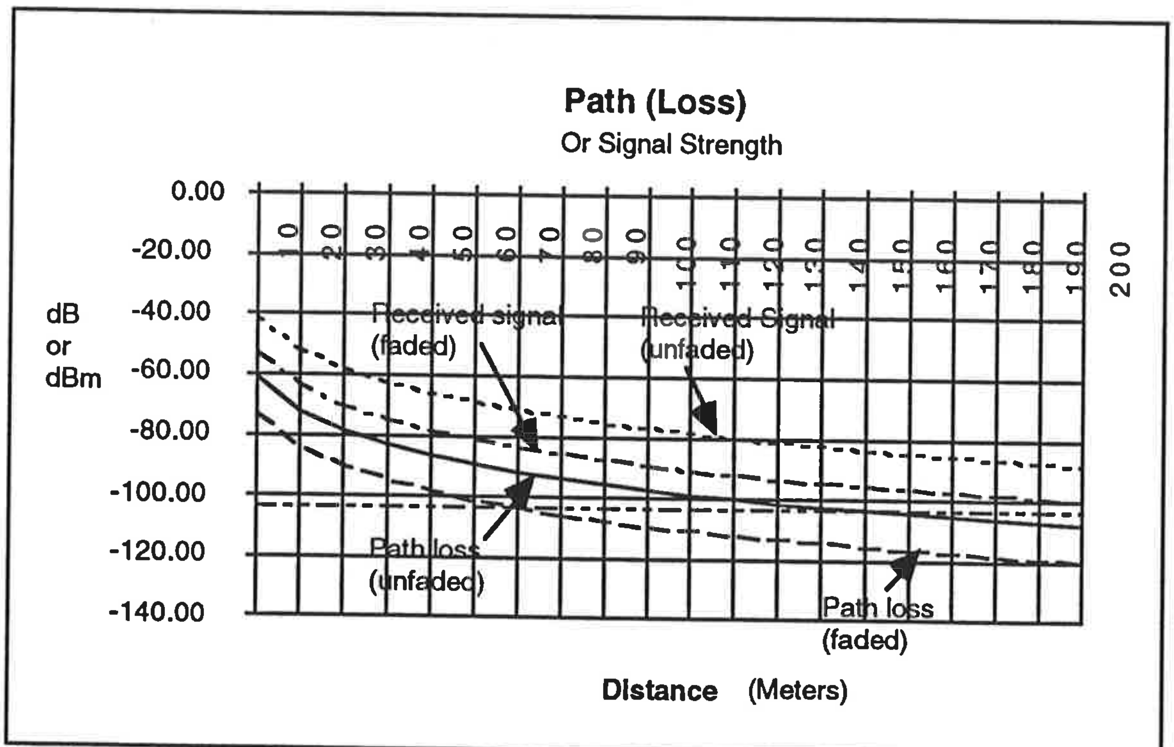

Fig. 2 Path Loss or Signal Strength vs. Distance from transmitter

Scenario 1 (Faded desired signal, unfaded interferer):
At 50 meters, terminal A produces a faded signal strength at terminal B of -78 dBm. An interferer 200 meters away from terminal B will produce a signal strength at terminal B of -88 dBm providing 10 dB of capture margin and allowing terminal B to successfully receive terminal A's transmission despite the interference from terminal D. In this worst case scenario, all terminals at distances less than 200 meters from terminal B can destructively interfere. While A and B can protect an area described by two overlapping circles of 50 meter radius, D can interfere over an area described by a circle of 200 meter radius. This is a ratio of areas of about 10:1.

Scenario 2 (Unfaded desired signal, unfaded interferer):

At 50 meters, terminal A produces an unfaded signal strength at terminal B of -66 dBm. An unfaded interferer 95 meters away from terminal B will produce a signal strength at terminal B of -76 dBm providing 10 dB of capture margin and allowing terminal B to successfully receive terminal A's transmission despite the interference from terminal D. In this scenario, all terminals at distances less than 95 meters from terminal B can destructively interfere. While A and B can protect an area described by two overlapping circles of 50 meter radius, D can interfere over an area described by a circle of 95 meter radius. This is a ratio of areas of about 2.24:1.

Discussion:

With or without considering fading, the RTS-CTS-ACK and similar protocols are vulnerable to interference from a large number of terminals which cannot be made aware of the potential for interference. The ratio of protected to unprotected terminals is somewhere between 2:1 and 10:1. and Some additional form of robustness must be included in any wireless LAN system which must coexist with large numbers of like systems. This interference potential is in addition to the interference from other dissimilar radiators in the same spectrum. Likely candidates for providing this robustness is frequency hopping combined with powerful error correction.