IEEE 802.11

802 LAN Access Method for Wireless Physical Medium

Engineering Choices for Portable Wireless LAN Adapters

November 6th, 1991

Peter Cripps
20 Carrera Court
Redwood City, CA 94062
415 364 4413

Abstract

This contribution describes spread spectrum wireless LAN technology currently under development at Texas Microsystems' Cupertino labs. The objective is to explore engineering tradeoffs which apply to products meeting one particular group of market requirements, and the technical parameters set out are not intended as completed MAC and PHY proposals.

The primary focus of the Texas Microsystems program is wireless LAN adapters for laptop and portable computers. Typical range must be at least 150 feet in an office building, with 1 Mbps transmission speed. Important design constraints are size, power consumption, and cost. Products should not require FCC licensing.

These requirements are met using a Part 15.247 2.4 GHz frequency hopping system which offers robustness, low power, and up to 82 Mbps total wireless capacity.

Wireless protocols are tuned to the requirements of the FH radio channel. Medium access is by an enhanced listen-before-talk algorithm, and an automatic repeat request procedure is used for error control.

1.   Requirements

The primary focus of Texas Microsystems' program is wireless LAN adapters for laptop and portable computers. Important design constraints are as follows:

|	
Size	The adapter must be small enough to fit in a typical laptop modem slot, or to be packaged as a self-contained external parallel port adapter. Future development to PCMCIA memory card format is desirable.
Power consumption	Adapter power consumption when not transmitting should be less than 50 mA at 5V
Cost	End user list price must be less than $500.
Speed	Must be at least 1 Mbps. Faster speeds are desirable, but not at the expense of higher power consumption, size, or cost.
Range	Should be at least 100 feet in a single network, with 200 feet desirable. Penetration of normal office partitions and walls is required.
Channels	At least 16, and preferably 64, independent channels should be possible, allowing many networks to operate in the same neighborhood without interference or throughput degradation.
Microcells	Must allow coverage of arbitrarily large areas using microcells.
Compatibility	Must work with de-facto and de-jure industry standards. NetWare on MS-DOS machines is a minimum.
Topology	Support for peer to peer communications, with no external hubs or relay stations, is essential.
Regulatory	Unlicensed operation under current FCC rules is required.

2.   Radio Channel

2.1.   Propagation

Attenuation

Indoor propagation varies considerably from building to building. A useful assumption for typical offices, with some sheetrock walls, is square law power fall-off for the first 3 meters, with 4th law fall-off thereafter. In more open environments, the ultimate fall-off may be closer to 3rd law, while in buildings with internal masonry or brick walls it may be as high as 5th or 6th law.

To a first approximation, these figures are independent of frequency. However, because the capture area of an omnidirectional receive antenna is proportional to its physical size, actual received signal power goes down with the square of the operating frequency.

Examples of received signal strength with various overall system parameters are shown below:
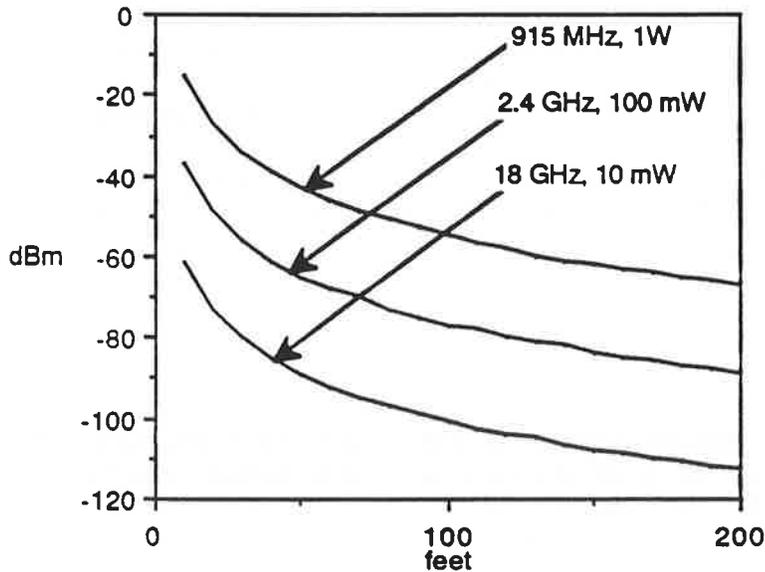
Depending on bandwidth, noise figure, and type of modulation, typical receiver thresholds will be between -80 dBm to -100 dBm. Clearly, to achieve 200 feet range, transmit powers approaching 100 mW are needed.

Multipath

For most indoor environments, multipath delays are generally less than 100 ns. For transmission rates less than about 1 Mbps, the principal effect of multipath will therefore be signal fading.

If median signal strength for any particular range is defined as the level where half the sampled locations are above median, then the following statistics apply:

Signal strength vs median	*Percentage probability*
less than 0 dB	50%
less than -10 dB	10%
less than -20 dB	1%
less than -30 dB	0.1%

At higher transmission rates, waveform distortion caused by multipath intersymbol interference becomes increasingly important. Measures such as adaptive equalization can deal with this problem, but only with significant penalties in cost, size and power consumption.

This suggests that a transmission rate no higher than 1 Mbps is preferable for portable products. As will be seen later, this data rate also matches well with regulatory requirements and low cost modulation techniques.

## 2.2. Spread Spectrum

Part 15.247 rules

The only provision for unlicensed operation at the power levels needed for this product is Part 15.247, which governs spread spectrum operation in the Industrial, Scientific and Medical (ISM) bands at 915 MHz, 2400 MHz, and 5725 MHz. Up to 1 W of RF power is allowed, and either direct sequence (DS) or frequency hopping (FH) can be used.

With DS, a processing gain of at least 10 dB must be demonstrated, with a minimum occupied bandwidth of 500 kHz. FH must use at least 75 hops (50 in the 915 MHz band), dwelling for no more than 400 ms on each hop, with no more than 1 MHz per-hop bandwidth (500 kHz at 915 MHz).

Almost all Part 15 spread spectrum LANs announced so far have used DS. This is largely because the original 1985 FCC rules allowed only 25 kHz hop bandwidth, forcing the use of DS for high speed digital transmission. This constraint was relaxed in 1989, making FH a viable option for wireless LAN products.

DS and FH interference characteristics

One of the most important differences between DS and FH in this application is performance in the presence of one or more narrow band interferers:

1 DS channel, 10 MHz wide   10 FH slots, each 1 MHz wide
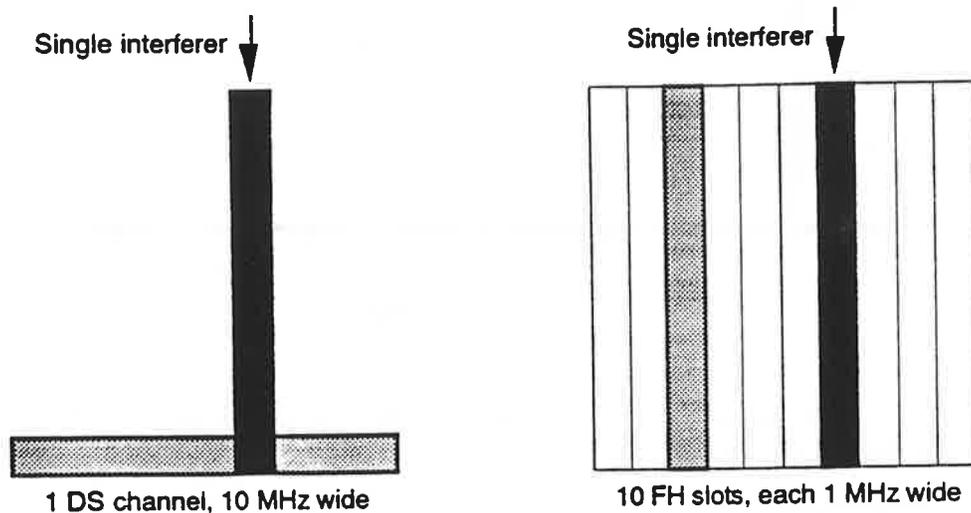
In this example, a DS system with 10:1 spreading ratio is compared to a FH system with 10 hops. Narrow band interference with the same total power as the wanted signal is assumed, so that the pre-processing signal-to-interference ratio is 0 dB in both cases.

The DS receiver de-spreader concentrates all the 10 MHz wide signal power into a 1 MHz post-processing bandwidth. Narrow band interference power is spread over 10 MHz, so that only 10% of the interference appears in the post processing bandwidth.This gives a 10 dB output signal-to-interference ratio, for a processing gain of 10 dB. If the required demodulator threshold is 15 dB, then the minimum input signal-to-interference ratio is 5 dB. Interference anywhere in the receiver input bandwidth which causes the signal-to-interference ratio to fall below this level will result in collapse of the transmission link.

With FH, narrow band interference affects just one frequency slot, resulting in a signal-to-interference ratio of 0 dB in that slot, for the example illustrated above. To obtain 15 dB signal-to-interference ratio at the receiver output, the input signal-to-interference ratio must also be 15 dB - but only in that slot. All other slots will be unaffected by interference, and will remain usable even at very high interference levels. With a suitable error control protocol, this will allow 90% of peak data throughput in the remaining 9 frequency slots.

To summarize, both DS and FH give equivalent performance at high signal-to-interference ratios. When there is strong narrow band interference, DS performance collapses completely, while FH continues to operate, albeit with reduced throughput. Only over a relatively narrow region, defined by the DS processing gain, does DS give better performance than FH. Increasing the spreading ratio for DS will give more processing gain, and allow DS to perform better than FH over a wider range of input signal-to-interference ratios. However, the scope for doing this at useful data rates within the ISM bands is strictly limited.
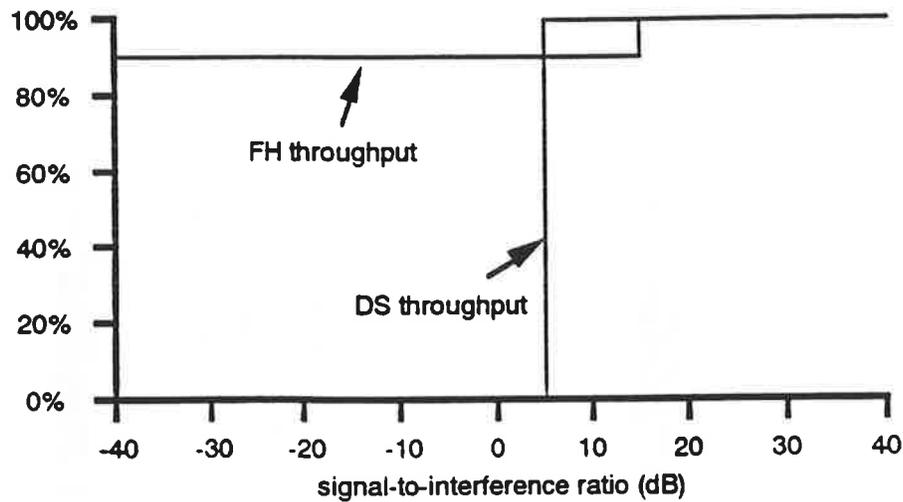
Since ISM band products have to withstand strong external interference, FH is strongly preferred to DS for wireless LAN adapters.

Multiple channels

For small networks, all nodes will be within wireless range of each other, and only a single shared communications channel is required. To cover larger areas, or deal with higher capacity requirements, multiple independent channels are needed:
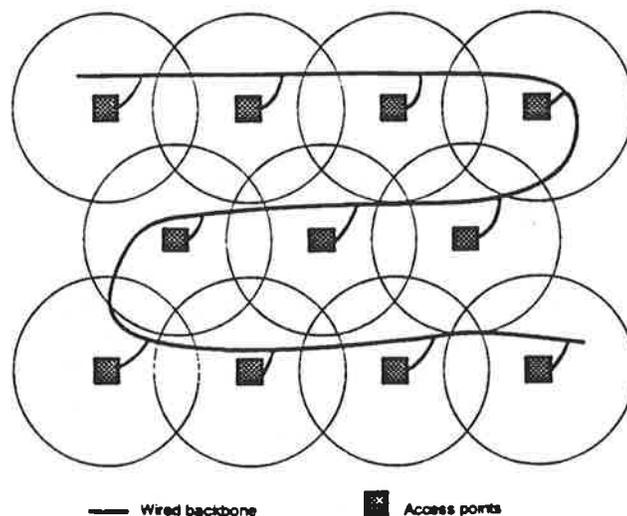

Here, each microcell would use a different channel, so that total wireless throughput is equal to the per channel data rate multiplied by the number of cells.

Code division multiplexing

In a FH system, code division multiplexing is implemented by assigning distinct hopping sequences to each channel. In this way, several asynchronous networks, located in the same physical area, can share common frequency space. From time to time, two hopping sequences my hit the same frequency slot at the same time. This will cause some throughput degradation, although not to a serious extent if only a few channels are in use.

Better CDMA efficiency is possible if all channels use the same hopping sequence, but with time shifts so that frequency hits never occur. The number of channels can then equal the number of frequency slots, allowing, for example, 82 Mbps total wireless capacity in the 2.4 GHz ISM band.
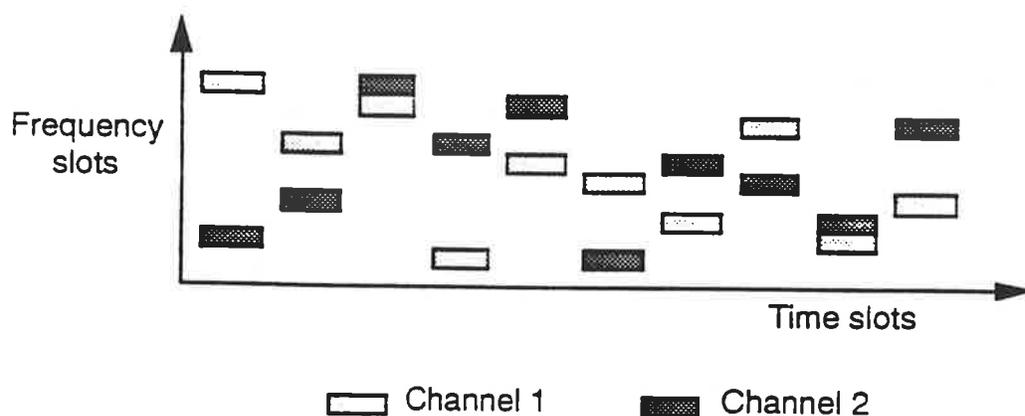
Under these conditions, FH offers equal spectral efficiency to conventional FDMA. DS can approach this level of performance only by using stringent power control and/or time synchronization, neither of which is realistically feasible in a peer-to-peer network.

Processing requirements

Typically, DS requires a substantial amount of signal processing at the receiver. If this is implemented digitally, there will be power consumption, space, and cost penalties. While passive correlators such as SAW devices overcome the power problem, their lack of programmability is a disadvantage for CDMA.

Overall comparison

For ISM band portable wireless LAN adapters, FH is superior to DS. It is more robust, has higher overall capacity, and uses less power. The only significant penalty is that under current FCC rules, per-channel throughput is limited to 1 Mbps. However, overall wireless throughput can be much higher than this figure if multiple simultaneous CDMA channels are used.

2.3.   Operating Frequency

Bandwidth

FH per-hop bandwidth at 915 MHz band is only 500 kHz, compared with 1 MHz at 2.4 GHz and 5.8 GHz. In addition, the 915 MHz band is only 26 MHz wide compared with 83.5 MHz and 125 MHz for the higher frequency bands. Use of either 2.4 GHz or 5.8 GHz is therefore preferred.

RF parts cost

Low cost bipolar parts for both transmit and receive RF circuitry are available at 2.4 GHz. In addition, standard 0805 and 0603 chip passive components give acceptable performance at this frequency. At 5.8 GHz, the situation is not nearly as good - transmitters and receivers can of course be built, but with significant cost and current consumption penalties compared with 2.4 GHz.

This suggests that 2.4 GHz is the best choice of operating frequency. However, the 2.4 GHz ISM band is also used by consumer microwave ovens, so the question of interference must be carefully considered.

Microwave oven interference

Consumer microwave ovens use a magnetron tube with 60 Hz AC applied between anode and cathode. On alternate half cycles, the tube does not conduct, and no energy is generated. When the tube is conducting, RF is generated at a frequency determined broadly by the physical properties of the magnetron cavity. Short term spectral purity of the output is quite good; measurements made at Texas Microsystems indicate that most of the short term spectral energy is contained within a 100 kHz bandwidth. However, there are some second order effects which must be considered:

Frequency modulation	Variation of magnetron anode voltage over the active half cycle	Sweeps up and down over ~10 MHz during a 9 ms half cycle
Long term drift	Dimensional changes in the magnetron cavity as it warms up	Moves ~25 MHz over tens of seconds
Mode hopping	Jumps in preferred operating frequency	Sudden jumps of 25 MHz to 50 MHz, apparently linked to thermal effects
Power control	Pulsing during the active half cycle	Produces AM sidebands within ~10 MHz of carrier

Results presented in a previous contribution (IEEE P802.11/91-52, Interference Characteristics of Microwave Ovens in Indoor Radio Communications, Dr J.Y.C. Cheah) are generally consistent with this physical description. From a practical point of view, interference will only occur when the magnetron is active, and then only when it happens to sweep through the receiver passband. Even when a receiver is located close to an operating microwave oven, there is no interference for several ms at a time on any particular 1 MHz wide frequency slot, a pattern of interference which can readily be handled with a packet repeat request protocol.

Conclusion

The preferred operating frequency is 2.4 GHz. Current FCC rules provide sufficient bandwidth, low cost RF parts are available, and interference from microwave ovens is a tractable problem.

2.4. Carrier Modulation

Binary

In order to meet performance requirements and FCC Part 15.247 specifications, a carrier modulation technique capable of providing 1 Mbps in a 1 MHz bandwidth is needed. Multilevel modulation techniques such 4-level PSK or FSK are one possibility, but binary modulation would be desirable for a low cost, low power consumption product.

Non-coherent

Non-coherent demodulation is also desirable for cost and power consumption reasons. Particularly for indoor communications, the relatively small performance advantage of coherent demodulation does not appear to be worthwhile.

Constant envelope

Constant envelope modulation allows the use of efficient, easy to tolerance, low cost transmitters using saturated amplifiers. This is the main reason why GMSK was selected for standards such as GSM and DECT. Unfortunately, in this case GMSK is not suitable - its spectral occupancy does not quite meet the 1 bps/Hz requirement.

FSK

Binary FSK with 0.175/T peak deviation (T = bit period) and linear phase 0.75/T premodulation filtering yields a 99% RF power bandwidth of approximately 950 kHz at a 1 Mbps data rate, comfortably meeting FCC specifications. Use of such a low deviation level does carry a penalty in signal-to-noise threshold, but this is acceptable in view of the advantages of binary, non-coherent, constant envelope modulation.

2.5. Performance Projections

Radio parameters

With an overall receiver noise figure of 6 dB, a noise bandwidth of 1 MHz, and a demodulator C/N requirement of 18 dB for $P_e = 10^{-6}$, the minimum receiver threshold will be -90 dBm. Assuming a transmitter power output of +17 dBm, and a unity gain antenna, EIRP will be +17 dBm.

Margin

While FH does provide many of the benefits of frequency diversity, some operating margin must still be provided to deal with multipath fades. A 10 dB margin over median signal level will result in approximately 10% raw packet failure rate, which is an acceptable minimum performance level.

The effective receiver threshold is therefore -80 dBm.

Link budgets

Case 1 - normal office

Frequency	2450	MHz	0.12 m
TX Power	17	dBm	0.05 W
RX NF	6	dB	
RX Bandwidth	1000	kHz	
Demod threshold	18	dB	
Margin	10	dB	
Fall-off coefficient	4		
Range corner	3	m	4.43E-04 PF at corner
TX ant gain	0	dB	1 power gain
RX ant gain	0	dB	1 power gain
RX ant aperture	1.19E-03	sqm	
RX threshold	-80	dBm	1.00E-11 W
RX Power Flux	8.38E-09	W/sqm	
Range	**45 m**		**149 feet**

Case 2 - open hall

Frequency	2450	MHz	0.12 m
TX Power	17	dBm	0.05 W
RX NF	6	dB	
RX Bandwidth	1000	kHz	
Demod threshold	18	dB	
Margin	10	dB	
Fall-off coefficient	3		
Range corner	3	m	4.43E-04 PF at corner
TX ant gain	0	dB	1 power gain
RX ant gain	0	dB	1 power gain
RX ant aperture	1.19E-03	sqm	
RX threshold	-80	dBm	1.00E-11 W
RX Power Flux	8.38E-09	W/sqm	
Range	**113 m**		**369 feet**

Case 3 - brick walls

Frequency	2450	MHz	0.12 m
TX Power	17	dBm	0.05 W
RX NF	6	dB	
RX Bandwidth	1000	kHz	
Demod threshold	18	dB	
Margin	10	dB	
Fall-off coefficient	5		
Range corner	3	m	4.43E-04 PF at corner
TX ant gain	0	dB	1 power gain
RX ant gain	0	dB	1 power gain
RX ant aperture	1.19E-03	sqm	
RX threshold	-80	dBm	1.00E-11 W
RX Power Flux	8.38E-09	W/sqm	
Range	**26 m**		**87 feet**

3.   Protocols

3.1.   Special Requirements

Many protocol techniques developed for wired networks can be applied to wireless LANs. In this contribution, attention will be focussed on some key areas where wireless connectivity introduces special requirements:

Packet length	Should be less than half the worst-case gap between microwave oven interference events
Retries during one hop	Should be spaced to catch the worst-case interference gap
Retries from hop to hop	Should be spaced to accommodate frequency slots in multipath nulls
Error rate distribution	Should recognize that error rates are typically either very good, or rather poor
Dynamic range	Transmit and receive signal levels may differ by 110 dB or more, making direct collision detection virtually impossible
Hidden stations	There may not be full connectivity between all network members
Non-reciprocity	Interference may mean that A can hear B, but not the reverse
Variability	Path quality between two stations may vary with time

3.2.   Medium Access

Channel sense mechanism

Correct operation of the Texas Microsystems medium access protocol relies on the ability of each station in a network to sense reliably that the channel is in use. This process starts with detection of a transmitted packet, which requires error free reception of at least 16 bits of 101010.... preamble, followed by an 8 bit unique word.

Packets may be RTS (request to send), CTS (clear to send), DATA (containing the data payload), or ACK (acknowledgment), which normally appear in the following packet dialog:
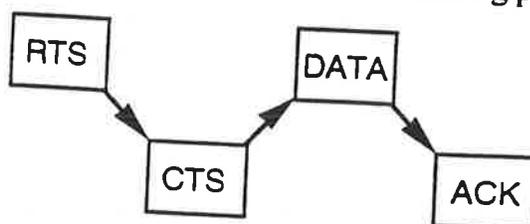
Both RTS and CTS packets include information on the length of the following data packet. Reception of either CTS or RTS by a station not participating in the dialog will cause that station's "channel in use" flag to be set. Reset of this flag occurs either on the final ACK, or after the time allotted for the dialog has expired.

This approach has the advantage of providing double protection against unwanted channel accesses, substantially reducing 'hidden station' collisions caused by one of the dialog participants being inaudible. It follows the procedure set out in a previous contribution (IEEE P802.11/91-92, A Hybrid Wireless MAC Supporting Synchronous and Asynchronous MSDU Delivery Services, Ken Biba).

Access control

A station wishing to send a packet determines from the channel sense mechanism whether a transmission is in progress. If it is, the station defers. If it is not, the station waits for a backoff period, and, if the channel is still free, sends an RTS packet addressed to the destination station, which replies with a CTS (clear to send). The originating station sends its data packet, and, if it is received correctly, the destination acknowledges with an ACK. CTS, DATA, and ACK packets are transmitted without deferral.

The backoff period is determined by an algorithm which substantially ensures different backoffs for each station at any one time, without giving any particular station priority over an extended period.

The advantage of this procedure is that data packet collisions should not occur. RTS/CTS collisions are minimized by the backoff process, and any that do occur will only have a small effect on overall throughput since RTS and CTS packets are quite short. The RTS/CTS exchange also ensures that connectivity does exist between the two participating stations, even under changing propagation conditions.

Retries

If 4 successive RTS packets have failed, further attempts are delayed for 4 ms, in case there is interference from microwave ovens. This procedure is repeated a further 3 times, and if there is still no RTS response, further attempts are delayed until the next hop, in case the particular frequency slot in use is in a multipath null. This whole procedure is then repeated for 3 more hops. If there is still no response, the station concludes that the destination address cannot be reached.

3.3.   Error Recovery

Strategy

If the only source of transmission errors was thermal noise, forward error correction (FEC) would give an improvement in transmission quality when the received signal level was marginal. Depending on the code chosen, an overall gain of 1 dB to 3 dB might be expected. While this would give some improvement in average range (about 20%), error-free data could not be guaranteed using FEC alone, since packets may contain long bursts of errors which could not be corrected with any reasonable level of FEC.

The primary strategy for radio link error control is therefore a protocol which causes lost and errored packets to be retransmitted.

Transmission procedure

A data packet for transmission is transferred from the host to the wireless adapter, together with information on packet length, destination address, and miscellaneous control information. A 16 bit CRC is calculated for the complete radio packet.

If the destination receiver detects an incorrect CRC, the packet is discarded and no further action is taken. If the packet is correctly received, the station sends an ACK. If the ACK is not received by the originating station the data is re-sent after first establishing radio channel access using the RTS/CTS procedure described above. The originating station does not send any new data until an ACK is received for the current packet.

If, after 3 retries, an ACK is still not received, the originating station assumes that the packet cannot be delivered, and informs its host.
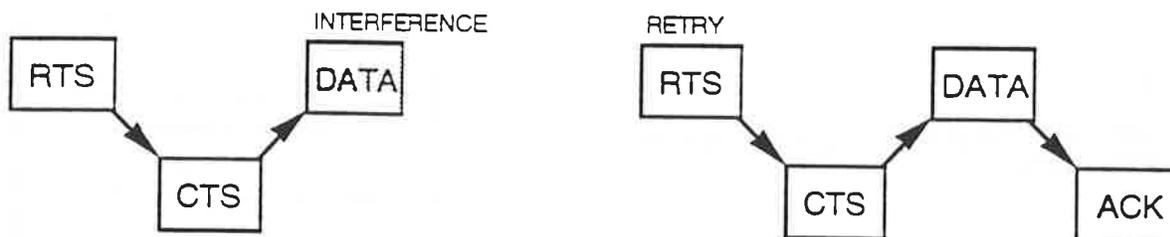
Packets include a transaction number so that duplicate packets resulting from lost ACKs can be detected and discarded by the destination station:
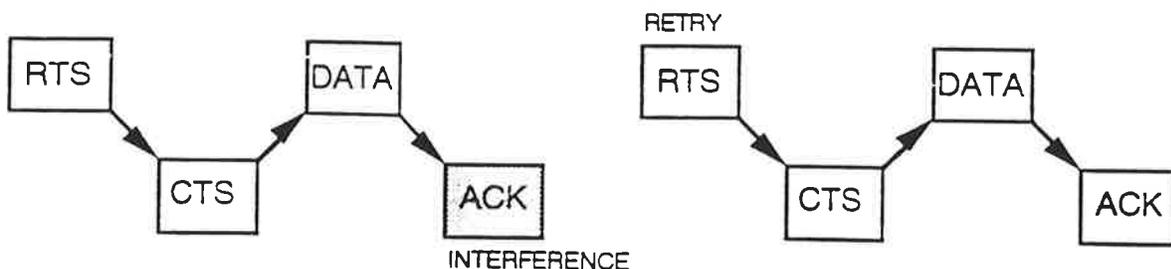
3.4. Packet Structure

Preamble

A 64 bit 101010....preamble is transmitted before the start of each radio packet. Its purpose is to ensure accurate clock recovery at the receiver.

Unique word

An 8-bit unique word allows correct packet alignment. Packet detection requires correct reception of 16 preamble bits followed by the unique word.

Network number

This 8-bit number allows up to 256 networks to coexist with each other in the same physical area.

Tick clock

This byte allows accurate FH synchronization.

Addresses

Physical radio network addressing is by 48-bit universally administered addresses.

Type, status

This 8-bit number defines packet type, used for several detailed protocol functions.

Length

This specifies total packet length, not including the 64-bit preamble.

Data

Maximum packet length is 600 bytes, or 4.8 ms, allowing transmissions between gaps in microwave oven interference.

CRC

A 16-bit cyclic redundancy checksum is used for error detection.

Byte	Field
Byte 0	
	PREAMBLE
Byte7	
Byte 8	UNIQUE WORD
Byte 9	NET NUMBER
Byte 10	SOURCE TICK
Byte 11	
	DEST ADDRESS
Byte 16	
Byte 17	
	SOURCE ADDRESS
Byte 22	
Byte 23	TYPE, STATUS
Byte 24	LENGTH
Byte 25	
Byte 26	
	DATA
Byte xxxx	
Byte xxxx+1	CRC
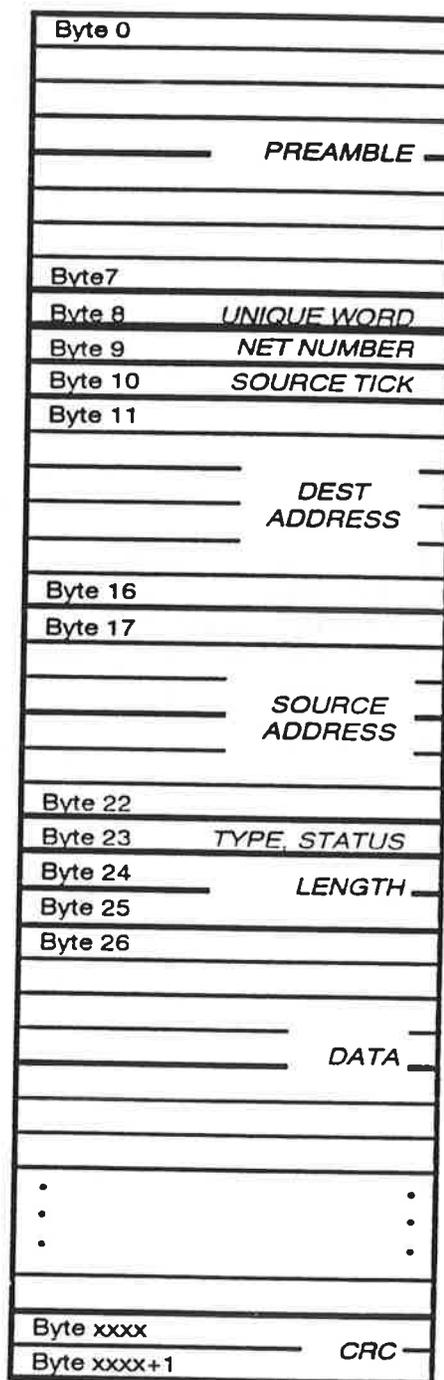
3.5.   Additional Protocol Requirements

The protocols under development by Texas Microsystems provide several additional network functions:

Synchronization	Allows new stations to join an existing network.
New network set-up	Allows automatic determination of correct hopping sequence for new networks. Applies both to independent networks and sub-networks in a large wireless installation.
Switching	Allows mobile or portable station to choose the correct cell in a large network.
Encryption	Provides protection against casual data theft.
Network management	Provides hooks needed to manage wireless network sectors. Also provides data on the quality of all wireless paths on the network.

Further discussion of these protocol services will be provided in a future contribution.

4. Conclusions

4.1. Regulatory

For unlicensed wireless network adapters operating under current FCC rules, Part 15.247 spread spectrum is the best option for range and speed.

4.2. Frequency Hopping

For portable products, a 1 Mbps frequency hopping spread spectrum system operating in the 2.4 GHz ISM band offers advantages of robustness, low power, and multiple communication channels giving 82 Mbps total capacity.

4.3. Direct Sequence

With current FCC rules, direct sequence spread spectrum is not a good choice for ISM band LAN adapters.

4.4. Medium Access

An enhanced listen-before-talk medium access algorithm allows distributed control, with good performance and reasonable protection against hidden station collisions.

4.5. Error Control

Link level error control by means of an automatic repeat request protocol is efficient and easy to implement.

4.6. Optimization

Both medium access and error control characteristics must be optimized for the FH ISM band channel.