

**UNIVERSITY OF TECHNOLOGY
SYDNEY**

**SCHOOL
OF
ELECTRICAL ENGINEERING**

THESIS 2

Report submitted in Partial Fulfilment
of the Requirements for the Degree of
Bachelor of Engineering (UTS) in
Electrical Engineering

A Spread Spectrum Packet Radio Network.

Student Name: Darryl Robert Smith

Academic Supervisor: A/Prof. Sam Reisenfeld

Autumn, 1995

Synopsis

This final year thesis project is the culmination of work done as a result of discussions between A/Prof Sam Reisenfeld and myself in May 1994. He convinced me that there was still a lot of work to be done with spread spectrum technologies, as well as emphasising how important spread spectrum is to the expansion of telecommunications in the global environment.

This thesis report looks at the interaction between spread spectrum technologies and the equally as new packet radio technologies. It has only been in the last 15 years with increased computerisation that either of these technologies have seen significant work.

This thesis also looks at some of the hardware required to implement a spread spectrum packet transmission system. During the design process I incorrectly assumed that PSK modems could be operated successfully at the chip-rate. Due to factors outside my control this assumption was not discovered until after the circuit boards had been produced.

A re-design implemented an early-late tracking loop which operates successfully at baseband, but not with RF signals as intended. The circuit should work with RF signals with the inclusion of ample amplification throughout the circuit.

Therefore I am presenting a circuit which demonstrates the circuits ability to lock to an incoming spread digital base band signal.

Most of the work on this project was done at home where I have a reasonably well stocked workshop. However I am grateful to those on level 23 in the school of Electrical Engineering for the use of the various labs. However I must thank here the numerous people who I have borrowed parts and equipment from enabling me to complete this project.

Acknowledgments

Special Acknowledgment should be made to the following people who have made this thesis possible.

Jack Heath, VK2DVH
Steve Bible, N7HPR
Clive Pickup, VK2DND
Sam Reisenfeld, VK2FPJ
Terry Behan, VK2TDQ

This is not a complete list but contains those who have contributed in significant ways. In addition I should thank Pacific Power for their help throughout the 5 1/2 years that I have been a Cadet with them. Their support has enabled me to complete my degree 6 months early despite early teething problems.

Also the members of Fisher's Ghost Amateur Radio Club (Inc) have given me great support. Some members names appear above but these are only a few of the many that have helped in some way.

Lastly I wish to thank all my family for all their support and guidance.

Table of Contents

Chapter 0 : Summary and Introduction	1
Summary Of Work.....	1
Introduction and Relevance to Pacific Power	2
 Chapter 1: Packet Radio Technology Overview	 4
The Present Packet Radio System	4
Protocols for Radio Transmission	5
Changes required to upgrade AX.25 to Version 2.1	5
Improving Channel Utilisation	6
Cleaning up Bugs and Ambiguities	6
Longer Callsigns. 6	
Parameter Negotiation and Longer Frame Sizes.....	7
High Speed Operation 7	
Limitations of AX.25 7	
Hidden Transmitters.....	7
On Packet Networks.....	9
The TAPR TNC-2.....	11
Kiss 12	
Options to a traditional TNC.....	13
 Chapter 2: Spread Spectrum Network Design	 14
Introduction 14	
Network Topology	15
Advantages of the Near-Far Problem to packet network routing.....	18
Power Control 19	
The state of the art.....	20
The UNISYS PA-100 Spread Spectrum Demodulator	21
Costing and Export Restrictions	22
Internal ASIC functions	23
FIR Filter and DC Removal. 23	
Digital Phase Shifter 23	
Automatic Gain Control 23	
Preaccumulator 23	
Despreaders 23	
Timing Error Detector 23	
Timing Error Processor 23	
Phase/Level Processor 23	
Timing Loop Filter 24	
PN Sequential Detector 24	
Phase Loop Filter 24	
Timing Strobe Generator 24	
PN code generator 24	
Phase Frequency Detector 24	
Frequency Hopped Spread Spectrum - Data Transfer	25
The Antenna System.....	26
Choice of Pseudo-Random Noise Sequence	26

Patents and CDMA	28
Auto-Correlation Functions	29
 Chapter 3: Hardware	 30
Spread Spectrum using PSK modems	32
Intermediate Frequency Delay Locked Loop	33
Full-time Early-Late Non-Coherent Tracking Loop	34
Increasing the search speed of an Early-Late synchroniser	35
Phase Reversal Keying (PRK) and the Spread Spectrum Modulator....	36
Modulator-Spreader	36
The RF implementation	39
Modulator 40	
Demodulator 40	
Filtering 40	
Mathematical realisation	41
IF Considerations	42
The Demodulator and Despreader.	45
Simple Despreader	45
The VCO 48	
Tuning the Circuit	49
Testing.... 51	
Tunable Parameters of the circuit.	53
 Chapter 4: References	 54
 Chapter 5 : Packet Radio in Professional Journals.....	 57
 Chapter 6: Literature Review	 65
 Appendix 1 : Thesis 1 Report	 71
Introduction 71	
Scope of Thesis 2	73
Licencing 74	
Required Resources.....	75
List of Thesis 2 Deliverables	76
Proposed development cycle.	77
Parts of the Final Report	78
Assumptions 79	

Table of Abbreviations

AFSK	Audio Frequency Shift Frequency
AGC	Automatic Gain Control
ASIC	Application Specific Integrated Circuit
BPSK	Binary Phase Shift Keying
CDMA	Code Division Multiple Access
DSSS	Direct Sequence Spread Spectrum
FEC	Forward Error Correction
GPS	Global Positioning System
IF	Intermediate Frequency
KISS	Keep It Simple, Stupid
NBFM	Narrow Band Frequency Modulation
PLL	Phase Locked Loop
PN	Pseudo Noise
PSK	Phase Shift Keying
RSPF	Radio Short Path First

Chapter 0 : Summary and Introduction

"Ye didnae tell him how long it was really going to take?..."

*Laddie, Laddie, Laddie. Ye've got a lot to learn if ye
want them to think of ye as a miracle worker"*
Scotty, Star Trek: The Next Generation, Relics

Summary Of Work.

1 Investigated the problems with networks using conventional radio packet technologies.

2 Investigated spread spectrum packet technologies applicable to a network.

3 Built a Synchroniser/De-spreader for eventual use on such a network.

I have made the following decisions when it comes to a Spread Spectrum Packet network.

- AX.25 is probably the protocol to use at this stage at least for level 2 although modifications for Forward Error Correction (FEC) would be quite required.
- The network should operate on a single frequency with transmitter power control for each packet.
- Automated routing such as RSPF should be used to reduce the Near-Far problem, but needs work to tailor it to the needs of Spread Spectrum.
- The [7,1] spreading code provides a long enough sequence and short enough synchronisation time.
- Binary Phase Shift Keying is the modulation scheme is simple and cheap to implement. Bit-rate may be doubled by also transmitting a quadrature signal with an additional BPSK signal although this is not investigated.
- A lot more work is required before a packet network based on topologies other than dedicated point-to-point links would be feasible.

Introduction and Relevance to Pacific Power

Inside any substation or power station there is a huge investment in copper cables. Each sensor and transducer is connected to a controller with hundreds of kilometres of wire in a site that might spread over several square kilometres.

The cost of these cables is huge. Not only are the capital costs involved with purchase and installation of the cables high, but also the maintenance costs both due to aging and transients picked up on the cables causing equipment failure.

Substations are designed with cheaper PVC cables in the switch-yard rather than silicon. However if a transformer explodes causing hot or burning oil to enter cable ducts it is known that all the cables will need to be replaced, and that the substation will be out of service until this happens.

In the case of Pacific Power Western the area where Wallerawang and Mount Piper are in close vicinity much environmental data is used by both power stations. Even more environmental data is not collected because of the remoteness of the sites.

Radio based telemetry is a solution to many of the situations just posed. A radio transmitter may be placed in a sub-station yard to send telemetry to the controller. Environmental sensors may do the same. In the case of a power station, telemetry may go to a marshalling kiosk and then be transmitted to the controller.

However standard radio techniques will not be reliable in an environment such as a power or sub-station where there is a large amount of electrical noise. This noise would cause important control information to be lost or delayed.

But all is not lost. Once solely a military technology, Code Division Multiple Access (CDMA) or Direct Sequence Spread Spectrum (DSSS) has been gaining prominence as a radio transmission technique allowing high traffic volumes to be transferred with a great immunity to interference.

Direct Sequence Spread Spectrum modulation does not make it possible to overcome wide band thermal noise. However it does overcome narrow band interference with ease as well as the effects of multi-path interference. In the power station environment there noise of all types. Switching are a large problem although they tend to be wide bandwidth with little auto-correlation. Modern control systems like most computerised equipment create a large amount of highly correlated noise as do mobile communication devices.

Throughout this thesis there is constant reference to Amateur Packet Radio. As amateur radio operators have done much of the work on packet technologies this is inescapable. They are also doing much of the work on Spread Spectrum Packet Technologies because they are permitted to experiment without the need for a special licence.

Chapter 1: Packet Radio Technology Overview

"The present packet radio networks in use are a combination of radios based on 1930's technologies with modems based on 1970's technologies"

Author Unknown

The Present Packet Radio System

Packet Radio Networks are currently being used quite extensively although their penetration is nowhere near that of other mobile services such as cellular telephone communications, point to point microwave connections and satellites.

Packet Radio is being used together with the normal voice communications by taxi and courier companies allowing bookings to be electronically transmitted to each vehicle. During the Gulf War, Packet Radio was used by the United States Military to transfer commands to field officers with Terminal Node Controller's (TNC's) connected to their secure SatComm satellite radio's.

Except for some subtle differences with addressing in most cases the system used by these organisations an X.25 variant known as AX.25. AX.25, however does not make any reference to the actual physical hardware. Provided the data is transferred end to end in packet form the physical medium is of little concern.

The most common method used is a modified random Aloha where a Carrier Sense is used on receivers. Commonly Narrow Band FM (NBFM) is used with 1200 BPS FSK modulation.

The system of carrier detect is similar to that used by ethernet. However there are some major differences. With ethernet the transmitted signal is constantly monitored for corruption denoted as Collision Detect or CD. There is no such facility in standard packet radio communications.

The exception is operating packet radio through a full duplex repeater. In this case it is possible to monitor the transmitted signal. Unfortunately even when using a full duplex repeater, the transmitted signals are seldom monitored.

Protocols for Radio Transmission

Of course there are options to AX.25 although they exhibit some problems in terms of usage as well as standardisation. As we speak all commercial packet radio (eg RDLAP, MOBITEK etc) uses some form of strong Forward Error Correction (FEC).

The lack of a Forward Error Correcting code in AX.25 is one great deficiency. The other being that it uses a 'Go Back N' retry algorithm rather than a selective repeat algorithm. The selective repeat algorithm would be far better in a radio environment due to the increases in spectral efficiency.

Phil Karn has implemented TCP-IP operation over the AX.25 protocol using the Un-numbered Information (UI) frames of AX.25. If AX.25 was chosen as a basis for Spread Spectrum transmission it would only be useful to encapsulate an additional protocol. Such a protocol would have FEC, selective repeat amongst other factors.

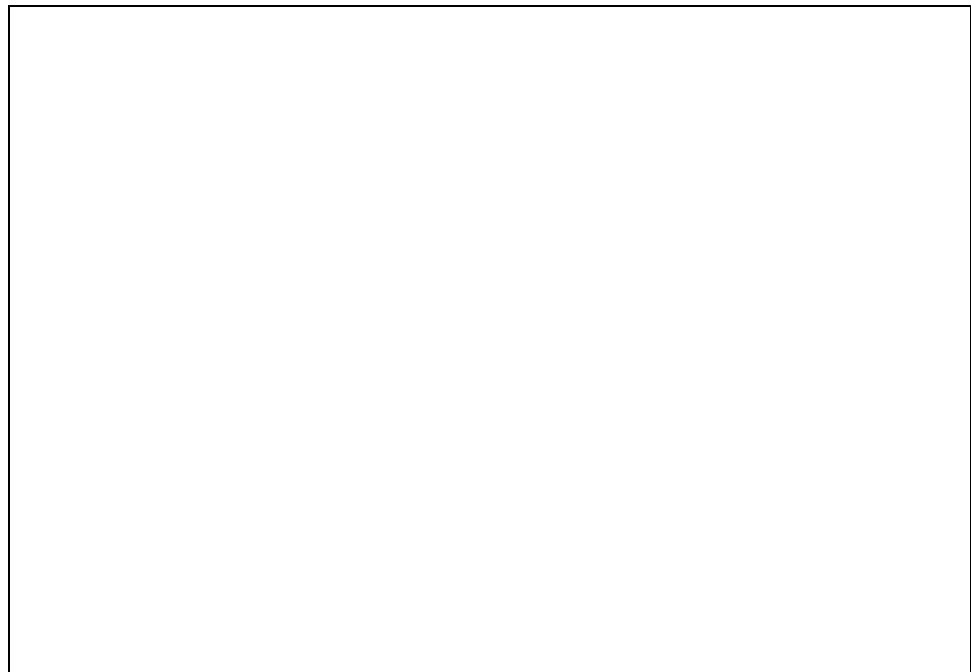


Figure 1: AX.25 frame structure

Changes required to upgrade AX.25 to Version 2.1

In looking at the upgrade of AX.25, the ARRL Digital Committee highlighted some problems and proposed solutions [17g][17h]. These problems can be divided into a number of main areas such as:

- Improving channel utilisation
- Removing bugs and ambiguities
- Suppressing the connection which never dies.
- Longer Callsigns
- Parameter negotiation
- Longer frame sizes
- High speed operation, other types of links and packaging

Improving Channel Utilisation

Where many links co-exist on the one frequency there is the tendency for one transmitter to seize the link. For a simplex channel the p-persist has been added. The retry timer has also been modified to allow for exponential increase in interference and high channel usage and automatic retuning when the link improves.

Cleaning up Bugs and Ambiguities

Various ambiguities occur in the existing specification which need to be removed in version 2.1. These fixes also repair the problem of some links re-establishing themselves after a disconnect on a marginal channel.

Longer Callsigns.

Not only was this the hardest problem facing the digital committee it was also the most important. A six character callsign is a problem requiring many users to operate illegally under reciprocal agreements where various extensions must be added to the callsign. In the commercial world the use of six letter is somewhat limiting. Longer callsign fields would be a great improvement in the commercial world. At least in Australia, many commercial callsigns are longer than six letters.

Although in many cases there is no legal need to use the callsign it's use is preferred. The Committee was unable to come up with a 100% backward compatible system, but was able to come up with a fallback to the old system when required.

Parameter Negotiation and Longer Frame Sizes.

In association with longer frame sizes it was decided to implement a means of negotiating various parameters such as the length of the frame. The frame would then be able to be larger than 256 Octets long.

High Speed Operation

AX.25 has quite small frame sizes and supports a limited number of outstanding frames. Ideally the number of frames needs to be increased with improvement for selective repeating packets lost.

Limitations of AX.25

In addition AX.25 Version 2 has some limitations. It is quite suitable for data communications however it has some limitations with respect to error correction. It uses a C.R.C. and it is fairly reliable. However it contains no facility for error correction.

Because of this lack of error correction on receive it is proposed that a FEC be added to the standard AX.25 packet.



Figure 2: Differences between a telephone-line BBS and a Packet BBS

Hidden Transmitters

Any interference caused by two stations transmitting at the same time causes both packets to be lost in most cases. However, if one of the signals is received at a strength much higher than the other, the signal with highest signal level would be correctly demodulated due to the FM capture effect, presuming that Narrow Band FM (NBFM) is used of course.

It is possible to use a full duplex repeater to listen for corrupted packets however this becomes expensive and reduces the versatility of packetised communications. To do this a transmitter and receiver would require a large amount of filtering to remove the transmit signal from bleeding straight into the receiver. Where the transmit and receive frequencies are close this equipment is quite bulky.

In packet situations the case of a hidden transmitter is quite common. The hidden transmitter is one which not all users can hear and are, therefore, likely to transmit over. In rugged terrain the problem is increased.

Taking this problem of 'hidden transmitters' to a logical extension the channel throughput approaches that of standard Aloha with just under 20% maximum throughput. Where there are no hidden transmitters the channel is almost constantly utilised with almost no collisions.

Due to hidden transmitters, packet networks tend to be concentrated about hubs in each geographical area on each frequency. If they were not grouped, stations would tend to hear only a fraction of the total number of stations. The challenge therefore is to maintain the use of a single frequency packet radio system while removing the limitations caused by frequency usage.

Unfortunately having all stations in separate receive frequencies would allow stations to independently communicate but would not solve the problem of two users attempting to send to a station when they cannot hear themselves.

Therefore, what would be ideal is for all transmissions to all receivers to be totally orthogonal. However we still require a reasonable bandwidth and to use the spectrum responsibly. By making all the transmitted signals orthogonal we are also able to receive more than one signal detectable and identifiable at the receiver.

On Packet Networks

In the Ham-Radio Digest[34], January 1993 C.E. Piggot comments

One of the potential strengths of packet is as a distributed, redundant system.

Adding a repeater greatly reduces collisions, but at a significant expense:

- the repeater is a single point-of-failure, and many people will not be able to or know how to operate without it when the repeater dies*
- repeater coverage rarely stays localised. After while, a better antenna, more power, etc. and you wind up with a wide-coverage packet repeater that is jammed up.*

In response Phil Karn of Qualcomm made the following comment also in the Ham-Radio Digest

*I happen to agree with this. Using repeaters to reduce collisions **does** involve a significant opportunity cost. Unfortunately, the alternative techniques to "do it right" are still not yet known in the amateur service. These include:*

- Spread spectrum, which creates a channel that degrades more gracefully with multiple simultaneous transmitters than does a narrow band channel.*
- Strong forward error correction coding. By decreasing the required signal-to-noise(interference) ratio, this enhances the ability of spread spectrum to tolerate multiple simultaneous transmitters on a channel. And by reducing the necessary transmitter power to sustain a link, it also reduces interference to other receivers.*
- Automatic transmitter power control so you never use more power than is actually necessary to reach a particular node.*
- Automatic routing algorithms with link metrics based on power/interference estimates so that paths are chosen on the basis of their minimum impact on overall system capacity. That is, you would choose a path of many closely spaced nodes over a few widely spaced nodes because the much lower power required at each hop would more than make up for the increased number of hops.*

As Phil Karn works with cellular CDMA at Qualcomm and also has a lot of the major work on packet radio in the last 15 years I suspect that he has a greater grasp of the issues involved.

Taking his points individually. Firstly CDMA is a modulation technique which degrades gracefully as is seen in the CDMA cellular telephone system. In it the received signal may be 14 db under the interference from another user. Additional users just add to this interference. However since the additional users are transmitting a mainly orthogonal signal very little of the transmitted signal causes interference.

With power control the whole packet system is not being overloaded by those who feel that more transmit power is the answer to a busy channel. Again taking the example of the Qualcomm CDMA cellular telephone system, the voice is sent as packets of data. There are also cases where the transmit power of the telephone is only 100 nW, or the received energy is higher than the transmitted energy.

With power control all users are given equal access regardless of the distance of the transmitter. Unfortunately in my thesis I have been unable to implement this.

Routing is quite important to overcome the NEAR-FAR problem. Short links must be used. To this end a protocol such as RSPF could be used. Craig Small, VK2XLZ is completing a thesis on this at the moment. An indication of the distance of a transmitter from the receiver can be obtained by monitoring the BER at the receiver. The protocol needs to be modified to channel network traffic into low BER channels if possible. The present RSPF protocol is designed for standard packet radio networks and their specific problems.

The TAPR TNC-2

In the early 1980's the Tuscon Amateur Packet Radio Group in the USA designed a series of PAD's (Packet Assembler/Disassembler) known as a Terminal Node Controllers. To aid future expansion this TNC had an expansion port for connecting external modems and radios.

This port contains all the clock signals a modem designer could ever want. For this reason the author decided that the TAPR TNC should be the basis of any packet system. This therefore really dictates the use of AX.25 as a Level 2 Protocol.

This does not affect the ability of the system to operate with experimental protocols which require unconnected information transfer. The UI frame in AX.25 allows for broadcasts. Phil Karn, KA9Q has used these frames to transfer IP datagrams.

Unfortunately the TAPR TNC-2 is getting quite old, being designed in the mid 1980's using Zilog Z80 microprocessors. Although the Z80 was mandatory for the CP/M operating system used on most computers of the era, CP/M has since died and thus the Z80 family is not as popular as it one was.

With increasing power available the traditional job done by the TNC is often being done by the computer the TNC is connected to. The KISS protocol (Described on the next page) is a useful machine independent protocol for transfer between PAD (TNC) and computer.

Kiss

Synchronous protocols are the most efficient to be used over radio networks. The stop and start bits in the asynchronous data communications would reduce the throughput of the link by at least 25% depending on the number of stop bits used.

A version of X.25 known as AX.25 has been formulated for use on radio networks by the American Radio Relay League (ARRL) and the Amateur Satellite Company (Amsat). It contains a certain amount of overhead but in most cases it is more efficient than asynchronous transmissions.

An interface from asynchronous to synchronous and back is required as modems usually require a synchronous signal. In the 9th Computer Networking Conference, Phil Karn proposed a standard for such an interface and called it KISS.

KISS is based on the SLIP with special bytes for start and end of a packet. A kiss controller simply takes asynchronous input from a computer and converts it to synchronous transmissions and back. It also deals with setting the speeds of transmission on the synchronous side as well as the transmit Push to Talk (PTT) on radio links.

Options to a traditional TNC

For many years the only options have been to use either an expensive SCC card on your computer or a full external microcomputer known as a TNC. In the proceedings of the 1989 ARRL computer networking conference, Henk Peek, PA0HZP presented a universal medium speed packet interface for the IBM-PC. It is largely based on the 8530 SCC chip from Zilog. The circuit presented has been modified and even redesigned by others including DRSI in their PC*PA.

The use of a programmable timer within a TNC is to control the key-up delay of the system. In systems such as the PI card this timer is able to be set down to 5 mSec. Relatively few radios can cope with such a short key-up delay. In fact the author would contest that such a short period in a Spread Spectrum situation would be almost impossible to obtain without PN cycle times of under 2 msec. A programmable timer allows a key up delay that is not CPU intensive which is important for DMA control.

In the past it was said that the Z-80 rules and CP/M would live forever because of it. In the last 10 CP/M has effectively been killed off but the Z-80 family continues to be used in many applications where cost is a primary concern.

Standard KISS does not have the ability to route transmissions going through it to the specific port. In this situation it is more important to have one KISS line to each port than to multiplex both signals onto the one line. In fact the serial links are often the slowest element in the system so by using one port per radio there is a speed advantage.

Unfortunately there is a great problem with the IBM-PC which is prevalent at the time of writing. The PC allows only four serial ports. In fact the situation in most cases is that two serial ports is the limit. This provides a problem for users.

The current state of the art in terms of interfaces is combined DSP modems and TNC's. As would be expected with any new product in a limited market these prices are quite high. Most TNC's are still only designed to handle a single radio at a time, with the exception of a few top-end TNC's catering usually to 2 radios.

Cards exist to plug into an IBM-PC although these obviously are limited by the constraints of the computer bus, processor as well as peripherals.

Chapter 2: Spread Spectrum Network Design

"Beware of programmers carrying screwdrivers"

Leonard Bradwein

Introduction

In 1989 at the ARRL's 8th Computer Networking Conference in Colorado Springs, Colorado, Roy Gould presented a study of high speed packet radio[17]. In this article he touches on spread spectrum techniques for packet radio operation.

He listed some of the advantages of Spread Spectrum packetised radio as:

- Immunity to man-made interference.
- Security of information within the channel.
- Immediate random access to the channel by a number of simultaneous users.
- Graceful degradation of the signal with overload.

He added however that a great deal of research would be needed to determine if this was actually practical.

Network Topology

The network topology in relation to a Spread Spectrum Packet Radio Network directly relates to the assignment of spreading codes. As spreading codes are orthogonal, just as frequencies are orthogonal with Narrow Band FM different spreading codes create different virtual links.

Several authors have provided a basis for assignments of spreading codes within a system [22][24][30]. The three assignments suggested are random orthogonal codes, common spreading codes and distributed assignment of spreading codes. A last option on which I could find no references during a detailed literature review was on individual permanent assignment of a unique spreading code per receiver.

Where the spreading codes are anything but common to all users the spreading code becomes an effective address where the only users receiving the packet are those whose receiver shares the spreading code of the transmitter. Qualcomm's CDMA system uses a common spreading code for all users with time offsets giving addressing using the spreading code (See Appendix 2).

Cartographers have long known that no more than 4 colours are needed to differentiate different areas of a map. A translation may be made to Spread Spectrum Packet Radio where very few spreading codes are required for individual addressing using spreading codes. However assignment of these codes is not so simple and would need some way for a new link to become part of a

changing system.

The easiest way to do this would be to broadcast using each spreading code waiting for a response. Another option would be to have a standard Narrow Band FM channel for assignments although this would be wasteful.

In GPS, units are transferred spreading codes via a very slow spread spectrum link with a short sequence length [11]. It would be easy to build a transmitter and receiver for this type of synchronisation into each unit. Transmission of this PN sequence by the station already a part of the network need not cause interference as the signal can be randomly interspersed with the network traffic such as transmitting a slow speed signal with the Qualcomm CDMA cellular telephone (See Appendix 2).

In effect, distributed code assignment creates a network of short orthogonal links. As stated in the section on code assignment however the choice of PN sequences is somewhat limited by the FCC in the USA.

A solution has therefore been posed whereby all users share a common spreading code [22]. In this situation each packet effectively becomes a broadcast just as in the present packet systems in use. However it is likely that simultaneous transmissions will be orthogonal. This can be enforced by time offsetting the PN codes from all users, although this adds considerable complexity.

Kim [22] states that at the link level there are two key design parameters in common spreading code systems to be evaluated. They are:

- The expected number of packets captured at the receiver.
- The allowable number of simultaneous transmission that are supported at a specific data bit error rate and probability of packet capture.

The author of this paper has shown that for the multiple capture model it is possible to improve significantly system performance by using the capture property existing in a spread-spectrum receiver.

In other words if Spread Spectrum networks are designed with common spreading codes the receiver architecture should acknowledge this and offer the ability to receive multiple Spread Spectrum signals at once. In fact this is also true in the other cases of code assignment as there will often be the case that two stations are attempting to transmit to a third station.

If the receiver has multiple capture characteristics care should be taken during the design so that signals are not multiply captured in the receiver. The logic of the receiver should be able to skip over signals that are already being tracked.

Comparing all the models available for code assignment it is the author's opinion that the optimum for a packet network would be using a common spreading code.

The advantages are:

- All users know the spreading code in use.
- All nodes can be heard without changing spreading codes.
- Receiver complexity is not increased as duplication is required anyway.
- Broadcasts are really broadcasting to all nodes that can hear the packet.
- Signals are usually orthogonal due to Auto-Correlation properties.

There are some disadvantages. They include

- Signals are not non-orthogonal at all times causing collisions.
- Security of information of the link is reduced because all users can listen in.

Alternative Topologies

The ideal topology for a Spread Spectrum Packet Radio network is in the author's opinion one where there is no central hub. However there are occasions where a central hub would be an advantage.

One example of this would be the case of a Bulletin Board System where users are usually downloading messages and files. In this case the speed of the down-link is most important. However the industrial environment is getting increasingly decentralised with remote sites requiring and generating data.

It is suggested that the spreading code on this topology be hard coded to simplify the receiver cost.

Advantages of the Near-Far Problem to packet network routing

Classical Spread Spectrum suffers when there are two transmitters in close proximity attempting to receive a signal from a transmitter much further away.

Aloha systems with Carrier Detect often suffer from a hidden transmitter problem where stations on the same frequency cannot hear each other but both transmit to a third station at the same time colliding causing packet loss.

The Near-Far problem, if dealt with properly can actually increase the performance of a communications system. To counter the problem of Near/Far the systems must be designed for many small hops rather than few large hops. Provided that each hop is acknowledged in turn, there is likely to be less problems caused by spread spectrum packet than with conventional modulation techniques.

But for this to work all the users on the frequency using the same coding must accept the responsibility to re-transmit packets as required. Failing to do this would create a situation similar to that of NBFM packet but much worse.

In their cellular telephone systems Qualcomm overcomes the Near-Far problem by ensuring that all nodes transmit only to the base station where the signal is strongest. Although this adds complexity it overcomes this problem.

In a spread spectrum packet network the protocol should contain information allowing closed loop power control.

Power Control

Qualcomm has done some pioneering work on power control of spread spectrum signals with open and closed loop feedback. Much of this work is covered by various patents.

In a packet network situation power control is important but more difficult as transmissions are required to more than a single base station if the versatility of packet protocols and topology are to be realised.

Each transmitter should only transmit as much power as it needs to close a link. It is assumed that each node will wish to communicate to more than one other neighbouring node. Whilst transmitting to the nearest of these two nodes the furthest node will not be affected, but when the furthest of the nodes is being transmitted to the nearest will be swamped by the signal possibly losing any other signals that are being transmitted to it at that time.

The KISS protocol discussed elsewhere allows for transmitter power control information transferral in band along with the data. The case of transferring the received power levels are more of a problem though. Several options exist. The first option is to use the upper nibble of the KISS address/packet identifier to transfer the level. However this only contains 4 useable bits, and these may also be needed by multi-drop kiss.

A more viable alternative is to transmit the level as an 8 or 16 bit number just before the end of frame synchronisation of the KISS packet. This would be ignored by software that was not looking for this information, gaining transparency to the user.

The last option would be to transfer the data as a special packet via the KISS control packet although there is no guarantee that the correct level would line up with the correct packet.

The state of the art...

The following edited comment came on of the Ham-Radio[34] mailing lists on Mon, 18 January and 8 July 1993 from Glenn Elmore, N6GN.

" I'm implementing DS spreading in my second phase of higher speed radios which are to be part of the "layer 3 TNC" we're working on for user access to a higher speed wide area amateur digital network. This is being done to help combat multi-path on less than optimum paths. I haven't yet found the limitation of spreading codes; the particular 7,13 and 19 bit sequences specified by the FCC, to be too much of a problem. Since I'm already using a moderately wide information bandwidth, pushing 1 Mhz, I run out of spectrum within the band before I run out of code length.

" I've had good luck using differential ECL logic (10116 variety) to drive DBMs directly. They have adequate current capability along with good balance and speed. I've used this to direct sequence modulate a variety of Schottkey diode mixers. I am interested if you have a good and simple discrete transistor design though.

" My spreading sequence operates synchronously with the carrier/pilot and data clocks. Therefor, once I have acquired PN synchronisation (by software rather than a hardware loop) and have locked onto the pilot tone, everything stays locked and synchronous and I also have all data clocks recovered.

" I'm generating the carrier, at 1265 Mhz, in one half of a dual PLL chip. The second half is used to phase lock the master VCXO (at 31.47 Mhz) to the received pilot tone. The carrier oscillator uses a coaxial line resonator and results in very low phase noise. See my 1988 Ham Radio Magazine microwave series for a similar design.

" The goal of the radio is 250 Kbps data to the user. See our paper in the 9th ARRL CNC for a description of the Hubmaster protocol which supports this. The addition of spread spectrum and fully synchronous and coherent radios will require some additions to this protocol but the fundamental operation is similar. "

Glenn Elmore n6gn

glenne@sr.hp.com

The UNISYS PA-100 Spread Spectrum Demodulator

In the past few months, Unisys of Salt Lake City, Utah, has released an Application Specific Integrated Circuit (ASIC) described as a "Spread Spectrum Demodulator" [31]. This Integrated Circuit has the capability for data rates up to 64 Mbps, chipping rates up to 32 Mcps, soft and hard decisions, AGC and up to 48 Db processing gain. Availability of the PA-100 integrated circuits along with the EB-100 and EB-200 development boards is unknown. The documentation, electronically obtained, is dated March 1995.

Put simply this integrated circuit has made the author's work on hardware redundant except for it's educational value. The device can operate at either RF provided the centre frequency is relatively low or at an I.F. using a down converter. It operates by digitising the incoming waveform, tracking it and despreading it.

According to the Technical Data Sheet and User's Guide common applications would be Satellite modems, Personal Communications systems, Wireless Networks and Cellular radio system. From the preliminary documentation it appears that the development system is designed to be used in association with microsoft windows software provided.

Interestingly the data from the manuals contains information on an epoch for the spreading code. That is the spreading code must start on a bit boundary, and the spreading code may be truncated to ensure this. Unfortunately this would be equivalent to resetting the sequence making. The epoch detection would limit the case of a symbol being transmitted with all 1's. The author must assume that the epoch function can be over-ridden.

Another strange detail about this ASIC is that it allows for chip-rates equal to that of the bit-rate. In that case, the gain by using spread spectrum technologies is certainly not as high as with a higher chip-rate.

For operation as a spread spectrum receiver a down-converter is required to reduce the frequency of the received signal. The down-converter [32] is able to convert the centre frequency low enough for the ADC but still high enough to so that information is not lost in the conversion process.

Unlike the Qualcomm CDMA phone system, the PA-100 does not have multiple fingers enabling the chip to simultaneously track multiple signals. The PA-100 may be able to track two BPSK signals independently but is certainly unable to track two QPSK signals independently. The lack of multiple fingers leaves it more sensitive to multi-path interference as well as increasing the difficulty level associated with inter-cell handoff's as required to decrease near-far problems.

The circuit as described in the next section implements the early-late synchroniser by delaying the incoming DAC signal and then despreading rather than using two despreaders. The circuitry required for a despreaders is somewhat more complex

and therefore probably more expensive than the delay line.

Costing and Export Restrictions

The cost of the PA-100 is approximately \$US165 with the price dropping to about \$US65 for quantities of 100 at the time of writing. The development boards are worth about US\$5000 each.

An export restriction has been placed on some of the software associated with this integrated circuit. At the time of writing it is unsure if the integrated circuits themselves may be exported from the USA. These export restrictions are based on a treaty aimed at slowing the flow of technology behind the Iron Curtain. Whilst the Iron Curtain has collapsed the munitions export regulations have not, leaving many products with zero export market.

It should be noted here that the same regulations apply to Australian exports of 'munitions' such as codes, ciphers and decipherers.

Internal ASIC functions

FIR Filter and DC Removal.

Removes inter-sample interference caused by resistor/capacitor pre-sampling filters and remove the DC component for processing.

Digital Phase Shifter

Output from the phase loop filter varies the complex rotation inside the digital phase shifter.

Automatic Gain Control

The AGC monitors the amplitude of the incoming data yielding a 12 bit output in proportion to the required gain of the input amplifier.

Preaccumulator

Used to perform an accumulate and dump operation at the sample rate for over a sub-chip interval allowing for systems with chipping rates varying up to an octave with a constant data rate.

Despreaders

The preaccumulator is processed by two complex despreaders, removing the PN code from the received stream before further processing.

Timing Error Detector

The preaccumulator is also processed with slightly early and slightly late PN codes. These codes are exactly one sub-chip early and late. In practice the incoming data from the de-spreader is subtracted from the data delayed by two sub-chips. This can then be put through the despreader with a PN code one sub-chip ahead of the desired tracking point. The output has a zero-mean output in lock conditions.

Timing Error Processor

The timing error processor accumulates the timing error over a symbol time, scales the results and removes the data modulation.

Phase/Level Processor

The phase/level processor accumulates the outputs of the despreader over symbol times, scales the results, makes data decisions, and provides outputs for use by the PN sequential detector and the phase locked loop. In addition the inputs to the phase accumulators are inverted during the last half of the symbol time to produce a frequency discriminator function.

Internal ASIC Functions (cont.)

Timing Loop Filter

This is a 1st order digital filter that may be used to form a 2nd order timing recovery loop. The output of the filter is a sample rate command that can be used to control an external clock generator for generating the system clock.

PN Sequential Detector

The PN sequential detector is used to acquire the PN code and monitor the signal level after code acquisition. It consists of data removal circuitry, bias subtractor, coherent accumulator and an acquisition/tracking controller. This circuit operates by attempting to lock onto a signal, with the PN rate as close as possible to the transmitted rate, and then adding slip pulses rather than modifying the frequency of the PN signal in out of lock conditions. If the frequency of the regenerating PN and the transmitting PN are not similar the tracking loop can handle that.

Phase Loop Filter

This filter controls the digital phase shifter forming a 2nd order carrier recovery loop.

Timing Strobe Generator

This generates sub-chip, chip and data symbol strobes, as well as full and half chip slips of the various timing strobes to accommodate pn acquisition.

PN code generator

The PA-100 chip contains dual 16-stage PN generators of variable length, with programmable feedback taps and initial values.

Phase Frequency Detector

The Phase/Frequency Detector processes the phase/level processor outputs.

Put simply this chip does everything that the author's thesis does, and does it better and much faster. However it does verify that many design decisions by the author will work in practice. The use of the slip generator added to a PN sequence which is not locked to a carrier.

Frequency Hopped Spread Spectrum - Data Transfer

At the beginning of work on this work it was thought that Frequency Hopping would not really be suitable for work with data communications.

Although a Frequency Hopping system might be useful in voice communications it is less useful for data communications. In a system without protection against multiple sequential error bits a Frequency Hopped system would not be viable.

Frequency Hopped Spread Spectrum works on the assumption that although some of the message is destroyed there is usually enough redundancy to determine the message. This is certainly true for voice communications.

When Frequency Hopped Systems are phototyped they are usually done with a single transmitter and a single receiver with Phased Locked Loop (PLL) frequency synthesis. Due to locking characteristics of PLL synthesisers there is often a large period of time when the transmitted signal's frequency is stable. On the receiver a similar problem exists where the frequency it is attempting to receive is highly unstable.

To reduce the dead zone between frequency hops at least two PLL's are required. One holding the present frequency and another holding the next frequency in the hop sequence. This would reduce dead zones to the vicinity of 1 mSec.

For low data speeds with error, correction data communications should be possible using a Frequency Hopped Spread Spectrum system. In fact during the Gulf War the allied forces used AFSK.

Frequency Hopping systems should become more popular in the next few years. GSM mobile digital telephones gaining acceptance in Australia uses a form of frequency hopping.

According to a Manager of AWA in their Military Products Division, it should be possible in the next decade to perform digital Signal Processing on radio frequency signals. When this happens, Frequency Hopped Spread Spectrum for digital communications should develop beyond our wildest dreams.

The Antenna System.

The antenna is the one component of the system where a small cost increase can reduce the bit error rate significantly. However the antenna system is a tradeoff between directivity, size and gain.

The directivity of the antenna system is an important factor in dimensioning the network. Cellular Telephone systems are designed around uni-directional base station antennas to allow maximum frequency re-use.

The gain of a transmitting antenna is only a function of the efficiency and the directivity of the antenna. As gain of an antenna increases in one direction, it decreases in another direction. High gain transmission antennas will not necessarily give better results. High gain antennas will only have this gain in a particular direction, with a very poor signal in other areas.

Receiving antennas however do not follow this rule, and can have high gains without the resultant minima. It therefore remains to be seen on what type of antenna array would be required.

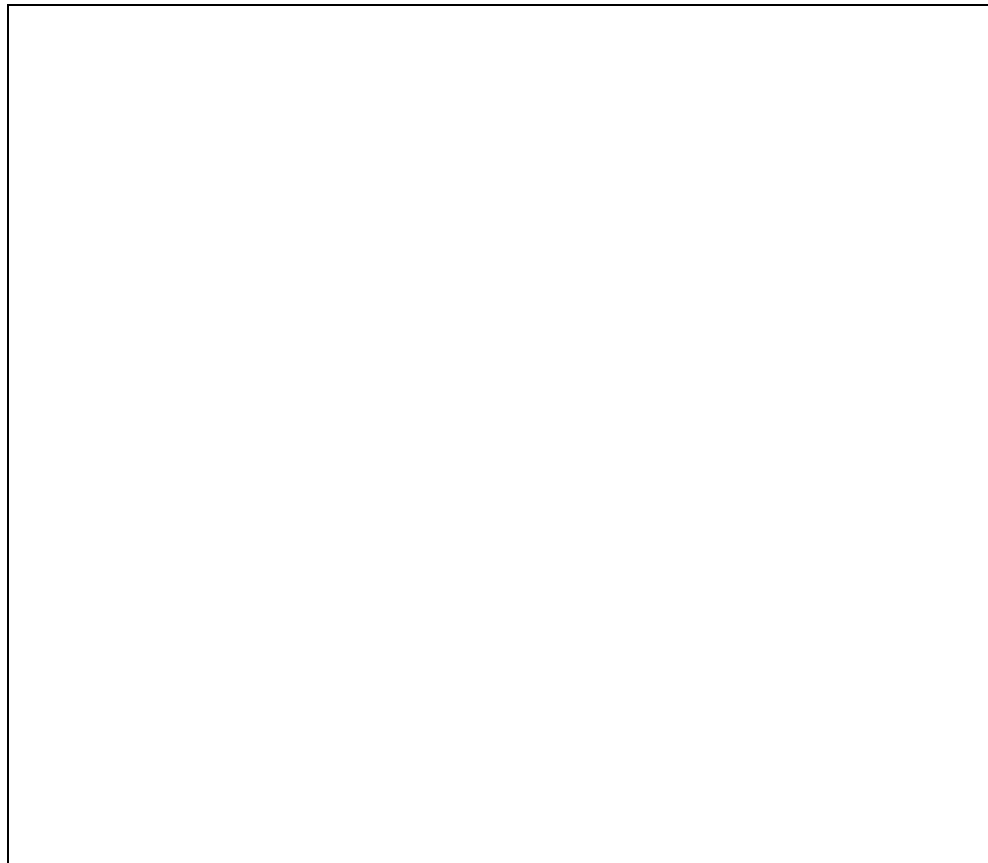


Figure 3: Examples of antenna radiation patterns

Choice of Pseudo-Random Noise Sequence

Whilst looking at the PN sequences available legislation must be taken into account. It is not always possible to choose the ideal sequence or set of sequences because of legislation.

There is some common notation for PN sequence identification. The sequences are often generated by a shift-register using feedback. The PN identification notation indicates which bits are modulo-2 added and fed back to the input of the shift-register.

As an example the [7,1] sequence is generated by modulo-2 adding register bits 1 and 7, inverting this and applying this to the input of the shift register.

The United States has the largest English speaking Amateur Radio population in the world. It also needs to be understood that they, as a group, have the ability to bring spread spectrum technology to the user. At the moment they are limited to only three sequences, [7,1], [13,4,3,1] & [19,5,2,1]. These sequences are also suitable for the FCC Part 15 requirements for Spread Spectrum transmitters operating in ISM bands.

This makes any form of variable assignment of sequences impossible. It is possible to assign each station a destination address which is a time offset from a reference sequence. In this case it would be possible to have a GPS time code provide synchronisation information at lower bit-rates. However this adds complexity and cost.

Under Australian **law** any spreading code is permitted, although there is little use in designing a transmitting system where the use outside Australia is limited.

The author has therefore chosen the [7,1] sequence as it is only 127 bits long requiring a short synchronisation time. This comes to about 8 bits per epoch, which reduces synchronisation time but has disadvantages with interference from other users.

The following message appeared in the Packet-Radio Digest[34] list on 16 Jan 1993

I arrived at more or less the same conclusion that SS was a good avenue for future packet development, primarily because direct sequence spread spectrum is probably one of the cheaper ways to 'fix' the multipath problem in high bit rate packet systems.

Rick Spanbauer, WB2CFV
SUNY/Stony Brook

Long codes are unfortunately vary difficult to synchronise to. This is especially true in a Packet Switched Network where connections are made when packets are needed to be sent.

Short codes are relatively easy to synchronise to but they suffer from a problem similar to jamming. When a CDMA receiver is in search mode it will usually lock onto the first signal it finds that has the correct signature. It may be one of many signals transmitting at the same instant.

Patents and CDMA

The following statement was made by Phil Karn of Qualcomm in early 1993 being asked on the TCP Group[34] mailing list of the patent situation with CDMA

Generic, basic CDMA (i.e., multiple spread spectrum transmitters sharing the spectrum) has been around for a long time -- since World War 2 -- so any patents on it have long since expired. Qualcomm's patents cover only some very specific implementation details on applying CDMA to cellular telephony, particularly the closed-loop power control scheme.

Phil Karn KA9Q, 18 January 1993

Auto-Correlation Functions

Graphically analysing a PN sequence of 7 bits I came to the following conclusions

- The number of agreements one or more chips from perfect correlation is equal to 3, and the disagreements are equal to 4.
- The number of agreements when perfectly synchronised is equal to 7, with no disagreements.
- The following equation was derived for the case where signals are within one chip of being synchronised.

$$D = \Delta * 4$$

Where

D = number of disagreements

Δ = fraction of a chip from agreement

The correlation function can be graphed as a function of the number of agreements, or as a function of the number of agreements minus the number of disagreements

The closest approximation to the hardware is using the A - D since it gives results closer to zero. The hardware does not go negative, but does go down to 0 volts for no correlation.

If the PN sequence is inverted but synchronised, both A and A-D will give results that indicate that no lock is close. In fact this is to be expected. Before we can use a delay locked loop we must remove the phase information leaving only magnitude.

Unfortunately there is no easy way to remove the phase information on a digital baseband signal. One option is to take a digital derivative of the difference between the incoming signal and the PN sequence. This function will tend towards a minima under synchronisation, inverted giving a correlation function that has phase removed.

This however requires a quite accurate local clock for the delay elements to acquire and maintain lock. It also makes the synchronisation much more susceptible to noise.

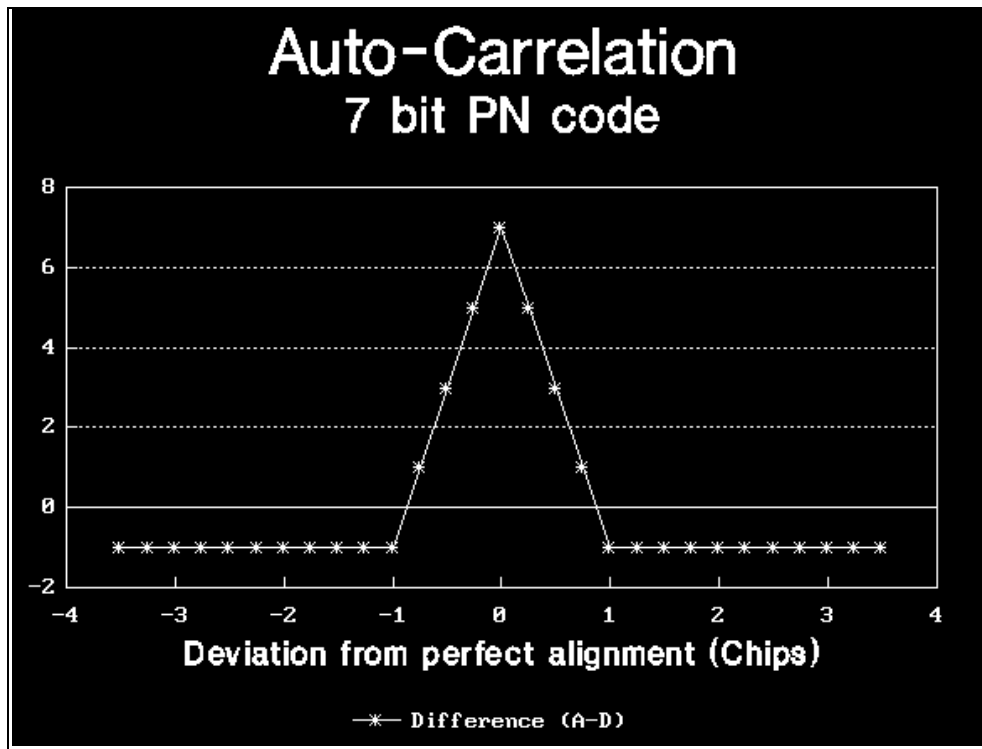


Figure 4: Auto-Correlation - Agreements Vs Deviation

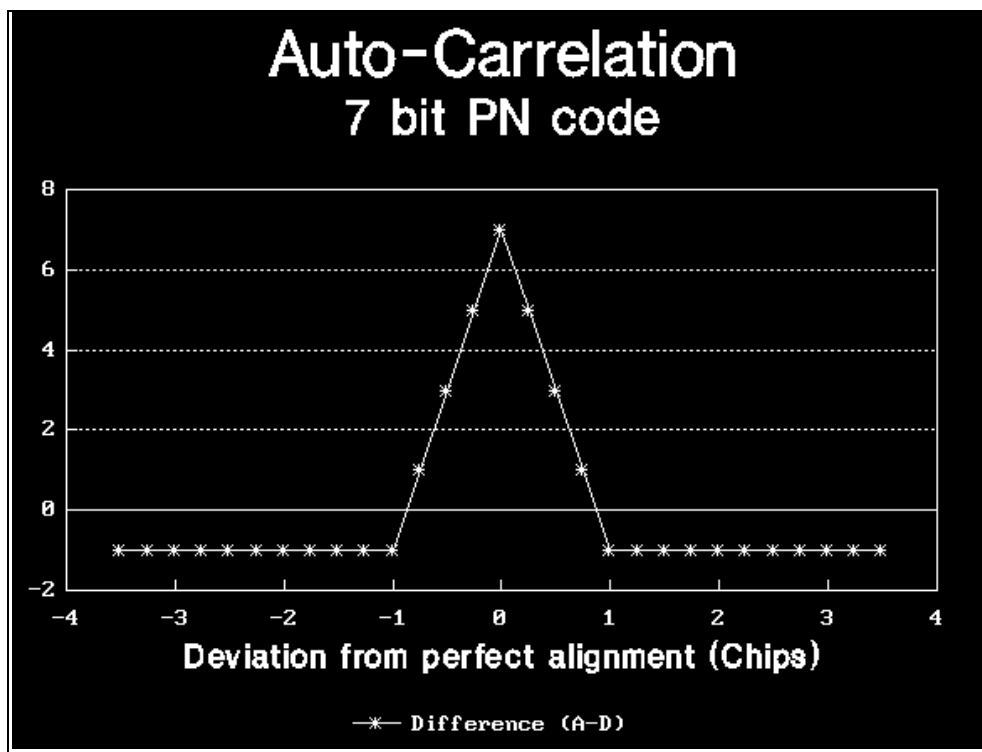


Figure 5: Auto-Correlation - Difference Vs Deviation

Chapter 3: Hardware

*"A sine curve goes off to infinity or at
least to the end of the blackboard"*

Prof. Steiner

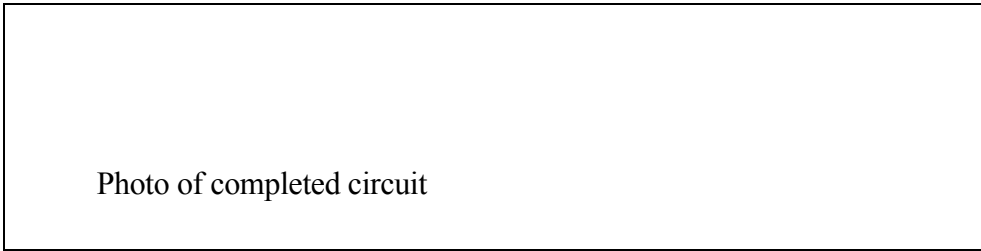


Photo of completed circuit

Photo of the completed hardware.

Before coming up with a final design for the thesis many designs were investigated. Although it is not intended to present the complete failures, the author feels that he should indicate where mistakes were made.

The three main steps were

- Spread Spectrum using PSK modems
- Spread Spectrum with RF signals
- Spread Spectrum with digital baseband signals.

Spread Spectrum using PSK modems.

The spreader and modulator simply modulo-2 added a generated PN sequence with the incoming data, and then sent the output to an off the shelf PSK modulator. This circuit should have worked if it had been built.

It was intended to use an off the shelf PSK demodulator to demodulate the modulated PN sequence. The output was then modulo-2 added with a reconstructed PN sequence and sent to a state machine for lock detect and data recovery. If the despreader was not locked, a 'SLIP' pulse was added to the PN generators clock at set intervals until lock was obtained.

There were two major problems with this design. First is that generation of the PN sequence relied on a clock from the demodulator at the bit-rate. In addition the PSK demodulator are not intended to operate in high noise environments which is where spread spectrum excels. PSK modems need to find a clock to synchronise to, which would be difficult with high interference levels. Therefore the PN generator also has a highly unstable clock leading to more synchronisation problems.

This design might work if a transmitted reference were used such as from a radio or television station so that a stable clock could be obtained.

Although this would have been spread spectrum, we are in fact transmitting symbols at a rate sixteen times greater than the bit-rate. It could be shown that there are many channel codes that could exhibit far better bit error rates for a given signal to noise ratio.

Intermediate Frequency Delay Locked Loop

After realising that the first design would not work, a circuit was developed that on paper would work, using mixers and filters. Although this circuit did not work in the lab, the reasons for this not working are not difficult to rectify given time.

Specifically the power level to the spreading mixer is limited to 0 dBm. Thus after the passing through mixers, splitters, pads and filters the level is in the vicinity of -60 dBm. This level is un-suitable for the diode detector used. To increase the level microwave amplifier circuits need to be used throughout the RF signal paths.

The diode also appeared too insensitive to the signal level. Increasing the level at the diode using distributed amplification should improve matters. Should that fail, an Op-Amp configured as a precision rectifier could be used subject to gain-bandwidth constraints.

Due to earlier problems and lead times on the production of Printed Circuit Boards, updated design needed to be completed over a single weekend, with no time for full circuit evaluation. Information on the losses exhibited in the mixers and filters did not come available until after the design had been completed

The signal level at the input to the diode detector needs to be 0.6 volts for an un-correlated signal to about 3 volts for a correlated one.

In addition a Voltage Controlled Oscillator was implemented using an Exar 2206 VCO after the circuit was designed. During testing it was found that the time constant of this circuit was quite large, making the VCO less than ideal for this application. To improve this situation, the low pass filter needed to be removed from the circuit.

This circuit also has problems with the use of a capacitor to provide ± 25 mVolts on the I.F. input of the mixer to change the phase of the output. Unfortunately this design was taken from another circuit with a much higher chip rate. Unfortunately the 3db pad to ensure a correct level and impedance limits the energy stored in the capacitor. That in turn causes problems with the circuits operation.

A solution would be to bias one of the I.F. pins to 2.5 volts and a series resistor between the other pin and the digital modulated PN signal.

It is interesting to note that although the author has seen no actual circuits using the crystal filters, Ziemler[6] provides a theoretical model of the this situation. Unfortunately the mathematics involved are quite complex.

Another circuit was developed. It relies on a TTL signal and uses early-late correlator to synchronise to the signal. It has a slight modification in the level detecting circuit with a 10K resistor placed in series with the diode to improve signal levels in the digital circuitry.

This circuit only works with a received PN code that contains no data on it. However it does prove that the delay locked loop circuit will operate correctly given amplification.

Full-time Early-Late Non-Coherent Tracking Loop.

Generating a coherent reference for demodulation of a DSSS signal is inherently difficult due to the extremely poor signal to noise ratios. In addition coherent early-late synchronisers have difficulty synchronising with modulation data. Neither of these difficulties is present in non-coherent early-late tracking loops.

Firstly the non-coherent tracker contains two energy detectors which are not sensitive to carrier modulation or phase. With minor modifications this loop may be used on any direct-sequence modulation scheme.

Increasing the search speed of an Early-Late synchroniser.

The Early-Late Tracker or Delay-Locked Loop operates by comparing a PN sequence $1/2$ a chip before and after the PN sequence of the demodulated channel. By comparing the input signal with these two time offset PN sequences it is possible to maintain lock on the main signal even in case of oscillator instability and multi-path interference.

However the normal model for the Early-Late synchroniser may be unable to lock under certain cases of oscillator frequency because the composite early-late signal has an output of zero under lock conditions, but also at points more than $1/2$ a chip from lock.

The composite output is useful in maintaining synchronisation but less useful in initial synchronisation. Therefore the lock condition occurs when the correlation outputs of the early and late paths are both non-zero.

To search for a signal it is possible to use a single correlator to determine the location of the signal. As three correlators are used in the Early-Late synchroniser it would be trivial to use all three separately searching for the signal drastically decreasing the search time. Once the approximate position of the signal was located with a correlation greater than zero it would then be possible to use all the correlators to lock the signal and maintain synchronisation.

What is proposed is partitioning the receiver into two distinct modes, hunt and track. During HUNT the early and late receivers are given a code that are equidistant from each other. When one of these receivers indicate a lock the mode changes to TRACK where the central receiver changes mode to the code of the signal that was locked and the Early and Late receivers return to their normal value.

This would be in effect be three tau-dither circuits searching for a signal. When a candidate was found it would be possible to use either two correlators in an early-late configuration in attempting to lock on or attempt to lock using a single correlator still in tau-dither mode. This would allow the other two correlators to look for another signal in case the one found turns out just to be temporary noise.

However a dual mode synchroniser was not implemented due to time constraints. A dual mode synchroniser would ideally require some intelligent form of control circuitry such as a microcontroller.

Phase Reversal Keying (PRK) and the Spread Spectrum Modulator

Phase Reversal Keying (PRK) or Bi-Phase Shift Keying (BPSK) is a simple modulation technique which involves transmitting a 0 phase shift for a 1 and a 180 phase shift for a 0. When used in conjunction with NRZI the encoding transmission of 1 and 0 may be arbitrarily swapped.

The modulation technique involves multiplying the NRZI signal by the modulating waveform. Thus the transmitted signal becomes

$$g_{PRK}(t) = A_c d(t) \cos(2\pi f_c t)$$

in the case where the incoming NRZI signal $d(t)$ has a value of ± 1 . (Reference [6])

The modulator circuit is also the realisation of the following equation

$$S_{tx}(t) = A * PN(t) * \cos(2\pi f_0 t + \Theta(t))$$

where

$$\Theta(t) = + \frac{\pi}{2}$$

$$- \frac{\pi}{2}$$

There is no reason to modulate the carrier with the data and then with the PN sequence rather than modulate the PN sequence with the data and then modulate them with the carrier such as

$$S_{tx}(t) = A * [m(t) \oplus PN(t)] \cos(2\pi f_0 t)$$

To simplify matters the data is simply modulo-2 added to the PN sequence before being applied to the modulator. This is possible in the case of Phase Reversal Keying.

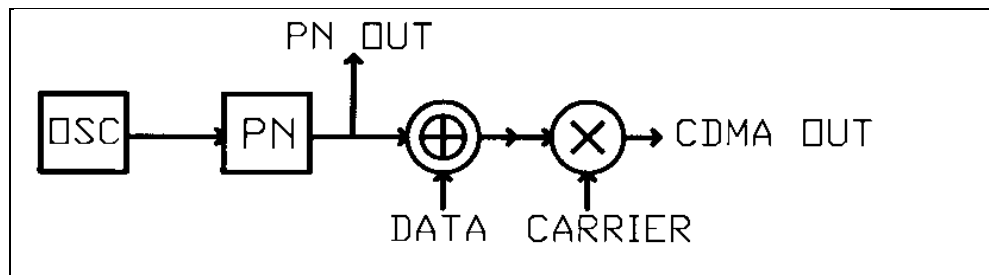
Modulator-Spreader

Figure 6: Spread Spectrum Modulator for baseband and RF applications

This diagram shows all the parts of the modulator. An oscillator provides a clock signal for the PN generator at. This PN signal is then mixed with the carrier as well the data. In the case of transmitting this signal at RF, the PN sequence is modulo-2 added to the data and then mixed with the carrier.

When operating at base band, the mixer involved with the oscillator is simply removed.

In accordance with FCC regulations in the United States of America there is no facility in the PN generator of the modulator to reset the PN sequence. The PN sequence is derived from a simple digital feedback loop and is clocked at a rate of sixteen times the base clock frequency.

The sixteen times clock signal is applied to the PN. This circuit assumes that the data only changes on the transitions of the unity clock signal.

In the circuit that I am presenting here as a working circuit the transmitted waveform can be given by the following equation.

$$S_{tx}(t) = M(t) \oplus PN(t)$$

It should be noted that there is no data modulation being placed onto the PN signal due to design simplification in the demodulator. Therefore the actual transmitted signal become

$$S_{tx} = PN(t)$$

The Spread Spectrum Despreader and Demodulator

Assuming that there is an accurate PN signal at the receiver, the signal becomes

$$R_{prompt} = m(t) \oplus PN(t) \oplus PN(t) = m(t)$$

The received signal is modulo-2 added with two PN signals. These PN signals correspond to early and late PN lock limits. The waveforms after mixing become

$$R_{early} = m(t) \oplus PN(t) \oplus PN\left(t - \frac{\Delta T_c}{2} + T_e\right)$$

$$R_{late} = m(t) \oplus PN(t) \oplus PN\left(t + \frac{\Delta T_c}{2} + T_e\right)$$

where

T_c is the chip time

T_e is the timing error

After filtering and differencing, the time averaged signals become

$$E_{VCO} = m(t) \oplus \left(\frac{PN(t) \oplus PN\left(t - \frac{\Delta T_c}{2} + T_e\right) - PN(t) \oplus PN\left(t + \frac{\Delta T_c}{2} + T_e\right)}{2} \right)$$

It can be seen from this equation that the error voltage to the VCO is still dependant on the incoming modulated data. However this is what I have implemented in hardware.

To extend this it is necessary to remove the data from the recieved waveform. This can only be done on a digital signal by actually demodulating the data. This involves a delay of one bit time, T_b , to make a decision on the data. We therefore gain the modulation data one bit time too late to be able to apply it directly to the early-late synchroniser. The block diagram appears on the next page.

Therefore we must delay the signals going to the early and late detectors by one bit time, modulo-2 add the data and then perform the same processes as before. This extension however has not been implemented in hardware.

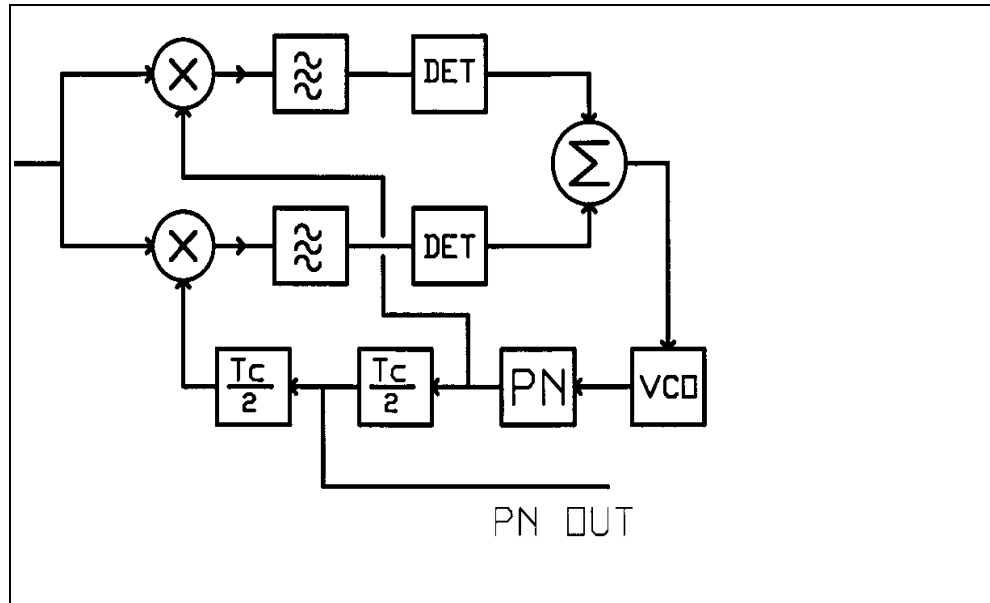


Figure 7: Spread Spectrum Despreader as implemented for both baseband and RF.

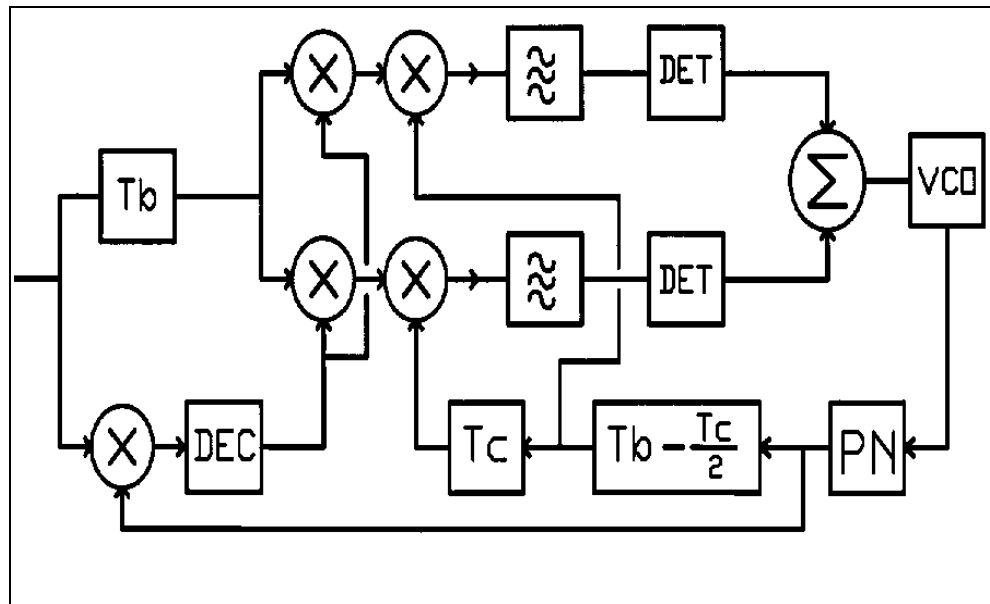


Figure 7: Baseband Despreader with phase removal

The RF implementation**Modulator**

The mathematical representation can be shown to give

$$S_{TX} = \text{COS}\left[2\pi f_0 t + (m(t) \oplus PN(t))\pi \right]$$

where PN(t) and m(t) are both 1 or 0. To simplify matters let us assume that they are ± 1 . The equation would then become

$$S_{tx} = m(t) PN(t) \cos\left[2\pi f_0 t \right]$$

Demodulator

The received waveform is received. It is assumed that it has been down-converted to the correct frequency. This signal gets mixed with the recovered PN signal.

$$R_{early} = m(t) * PN(t) * PN\left(t - \frac{\Delta T_c}{2} + T_e\right) * \cos\left[2\pi f_0 t\right]$$

$$R_{late} = m(t) * PN(t) * PN\left(t + \frac{\Delta T_c}{2} + T_e\right) * \cos\left[2\pi f_0 t\right]$$

These signals then get passed through band pass filters with a bandwidth sufficient so that 95% of the energy from m(t) is passed through. The loss of the filter is being totally ignored here as it produces a proportionality constant.

After going through the filter, the signal out will either have a large amplitude indicating close to synchronisation, or a low amplitude signal indicating that the signal is completely out of lock.

This signal still has the phase (or data) information. The phase information can be removed most easily by envelope detection of the signal. After envelope detection this yields

$$E_{vco} =$$

$$\left(\overline{PN(t - T_b) \oplus PN\left(t - T_b - \frac{\Delta T_c}{2} + T_e\right) - PN(t - T_b) \oplus PN\left(t - T_b + \frac{\Delta T_c}{2} + T_e\right)} \right)$$

Filtering

In practice the BW_{3dB} of the filters was about 2660 Hz. At ± 600 Hz we can assume that the signal is no more than 1dB down from that at the centre frequency.

The equation for PSK data transmission is given as

$$S_{\phi}(\omega) = \frac{1}{2} A^2 T \text{Sa}^2 [(\omega + \omega_c)T/2] + \frac{1}{2} A^2 T \text{Sa}^2 [(\omega - \omega_c)T/2]$$

where

$$\omega_c \text{ is the carrier frequency} = 10.7 \text{ MHz}$$

$$\text{Sa}(x) = \frac{\sin(x)}{x}$$

It can be seen that there are two lobes with symmetry. The lobes are centred at ± 600 Hz from the carrier frequency with the receive filter filtering at ± 1330 Hz. Thus about 94% of the transmitted energy is contained in the pass-band of the filter.

It can also be shown that only about 27% of a spread PN transmission would occur within ± 1330 Hz. (The 27 becomes 13.8% if the spreading makes $\pm 19\text{K}2\text{Hz}$).

Thus the detected power of the data is about 5.3 dB higher than the detected noise level assuming an equal reception power before the filter. If the filter was approximately 1300 Hz wide rather than 2660 Hz the detected power would have been about 8 dB higher than the power of the spread data.

However a tighter filter would have been more expensive and resulted in greater losses in the pass-band. The filters chosen were once sold by Dick Smith Electronics and were on loan from Clive Pickup VK2DND. His experiments at the CSIRO department of Applied Physics resulted in the following results as to their characteristics

3 dB band edges 10.69483 MHz and 10.69217 MHz
yielding 2660 Hz BW
7 dB insertion loss at centre frequency.

The filter is model 10622E1 KDS 6B, with a centre frequency of 10.6935 Mhz and is an 8 pole filter. This would translate to a lower sideband normally. However in the circuit the filter is used at its centre frequency.

Mathematical realisation

The input signal received is

$$r(t) = m(t) \oplus PN(t)$$

This is then mixed with a prompt PN sequence yielding

$$m(t) \oplus PN(t) \oplus PN(t + T_e)$$

After making a decision, assuming that the timing error, T_e , is small then gives us

$$m(t - 1)$$

Relating back to the incoming signal we delay it by one decision time yielding

$$m(t - 1) \oplus PN(t - 1)$$

Assuming that data is correctly demodulated with little timing error, we can then show that modulo-2 adding these two signals gives us

$$m(t - 1) \oplus PN(t - 1) \oplus m(t - 1) = PN(t - 1)$$

Thus we have removed the modulation, although the signal is now slightly delayed. Note that the delay is indicated as T_b , being a bit period

$$E_{VCO} =$$

$$\left(\overline{PN(t - T_b) \oplus PN(t - T_b - \frac{\Delta T_c}{2} + T_e)} - \overline{PN(t - T_b) \oplus PN(t - T_b + \frac{\Delta T_c}{2} + T_e)} \right)$$

IF Considerations

Due to mass production the cost of hardware involved with television reception is quite cheap considering the amount of circuitry involved. It therefore makes sense to base any designs on building blocks normally incorporated into television receiver design. Given that these transmissions are vestigial side band, they would be ideal for spread spectrum.

A possible building block is the Dick Smith Electronics Television Field Strength Meter. What makes this project ideal for spread spectrum communications work is the IF output from the first tuner module. This would enable a single tuner to be used with several IF modules. It would also allow for a phase inverter to be placed after the tuner and before the demodulator.

The circuit is fairly simple due to the high level of integration in the tuner modules. A large portion of the circuit as presented is redundant in this case as it will not be used as a field strength meter. I have modified the circuit given to include IF in and out connections which should be connected for normal operations. I have also modified the circuit for connections to the AGC and the AFC.

One disappointment was the frequency range of the receiver. With a lower limit of the UHF TV band at about 470 Mhz the receiver does not operate in the Amateur 70 CM band. It does operate in the 50 CM band although there is a somewhat limited life for this band.

The circuit includes a Switchmode Power Supply for generation of 36 volts required for the tuner. This power supply appears to be well shielded and causes no problems to the circuit.

Disappointingly the whole construction of the case is plastic. It therefore would show little resistance to interference from nearby electric fields.

On the IF module there is an Automatic Gain Control (AGC) input that might need to be connected. It would be relatively simple to place a mixer before the antenna input allowing spread spectrum demodulation.

To maintain control accurately 3 tuners would be required increasing the cost. Alternately the early and late signals could be derived using mixers and filters exclusively much as in the prototype design.

Modulator Circuit Diagram
SS Modulator
THESIS21.S01

The Demodulator and Despreader.

The demodulator is probably the most important part of the spread spectrum system. It certainly contains the most complexity. It may be helpful to read this description of the demodulator with reference to the block diagram.

When a signal is received at baseband it has most of the signal about 40 kHz removed as there is little information content within this band. This signal is then fed through a comparator for clock recovery and an amplifier for the information recovery.

Demodulation is relatively straight forward involving the use of a Carrier Recovery circuit and multiplying its output with the incoming signal. Then the sum is integrated over a bit period before a decision is made at DC where positive signals represent 1 and negative represent a 0.

Simple Despreader

This circuit does not actually recover data, although recovery of the data is relatively simple. Again this diagram is common between both the RF configuration and the baseband digital configuration. In the case of the RF configuration, the mixers are balanced mixers, the filters are band pass filters, and the detector is an envelope detector.

In the digital baseband case, the mixers are modulo-2 adders, the filters are low pass filters as are the detectors.

The $T_c/2$ elements are delays of $1/2$ the chip time, with the prompt PN output between the two delay elements.

Include RF Circuit Diagram

Digital Baseband Circuit Diagram

The VCO

The receiver requires a 19.2 KHz signal for the PN generator clock. Further the digital delay line for the PN output requires a clock frequency of 8 times this. That is we require a clock of

$$F_c = 153.600 \text{ KHz}$$

This clock frequency is generated by a Monolithic Function Generator integrated circuit from EXAR, driven by a filtered signal from the early and late level detectors.

The XR-2206 is a 16 pin IC commonly used in analogue modems, although it was more popular before modem chips such as the 7910 was released. The design calculations following are based on the equations from the appropriate Exar Data Book. Unfortunately the exact date of publication is not known as only an extract was available.

$$F_{osc} = \frac{1}{RC} \text{ Hz}$$

The data sheets also give us an appropriate value for the resistance R.

$$R = 5.6 \text{ K } \Omega$$

$$C = 1.162 * 10^9 \text{ F}$$

$$= 1.163 \text{ nF}$$

The following equation was incorrect in the data sheet, with misplaced brackets. Now, including an offset the frequency is given by

$$F_{osc} = \frac{1}{RC} \left[1 + \frac{R}{R_c} \left(1 - \frac{V_c}{3} \right) \right] \text{ Hz}$$

We require about $\pm 10\%$ frequency variation. This happens when $V_c = 0$ and 6 Volts for maximum and minimum frequencies respectively.

$$\therefore \frac{R}{R_C} \left(1 - \frac{V_c}{3}\right) = + - \frac{1}{10} \quad \text{for } V_c = 0,6$$

Since $R = 5.6 \text{ K}\Omega$ then $R_C = 56 \text{ K}\Omega$

The sensitivity then becomes

5120 Hz/V or 5.12 Hz/mV

Tuning the Circuit

There are three discrete conditions found in the delay locked loop after the modulo-2 adder despreaders. They are when

- Both outputs are equal; Found when either in perfect lock or out of lock.
- One the late output is high and early output is low; and visa versa.

Of course when the signal is perfectly in lock we would like the VCO frequency to be as close as possible to the generation frequency minimising jitter on the PN signal. Out of lock we need the frequency to be close to the transmission frequency, with a small amount of frequency offset.

Without this small offset, the system would never lock as the loop relies on the principle of beat frequencies. An option is to change the frequency of the VCO by adding slip pulses when the system is out of lock.

With this in mind it should be possible to set up the system so that the free running frequency of the system with no input is equal to the anticipated frequency of the incoming signal. However there are two tuning adjustments that may be made, and these are not orthogonal.

Thus we need to set the frequency of the VCO with the early output high and the late output low. This is the condition to tell the oscillator to slow down. Thus we should adjust the frequency under these conditions to be slightly lower than the centre frequency. And exchanging inputs should return a VCO frequency slightly higher than the centre frequency.

These two frequencies are the upper and lower limits of the lock range. Therefore they should be set wide enough to lock to the signal, and narrow enough to minimise capture time.

Testing....

Two major criterion are used to verify the operation of this circuit. They are

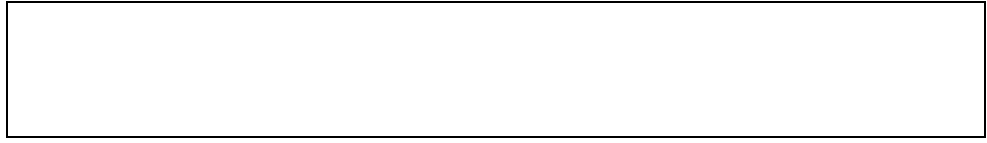
- Lock condition after parameter tuning
- Ability to re-lock after interruption in the signal.

The second of these is the most important. If a signal can be locked by an operator manually adjusting the parameters this does not mean that the tracking loop is operational. But if the circuit can re-lock after being interrupted, the circuit must therefore be working correctly.

It has not been possible to verify the lock range of the circuit because of the lack of stable test equipment. In the laboratory it has been possible to establish lock after loss of the signal. Unfortunately the most common reason for loss of lock appear to be transients caused by power supply problems.



Transmitted PN waveform (Top) prior to synchronisation to the regenerated PN sequence (Bottom)



Transmitted PN waveform (Top) synchronised to the regenerated PN waveform (Bottom).

Tunable Parameters of the circuit.

There are a number of adjustable parameters in the circuit design. First of all there is the DC offset added for centre frequency control as a bias. The next parameter is the frequency of the loop filter. Then comes the natural frequency of the VFO as well as the DC reference level. Further on there are the Tap Points for the PN code.

Not all these parameters are orthogonal. Changing either the DC offsets will change the oscillation frequency where no signal is present. Changing the tap points may require adjusting the frequency of the feedback loop filter.

Chapter 4: References

Sattigner's Law: It works better if you plug it in.

- [1] Cook, Charles E., "Spread-spectrum communications" IEEE Press, New York c1983.
- [2] Dillard, George M., "Delectability of spread-spectrum signals" Artech House, Norwood, Ma, c1989
- [3] Dixon, Robert C. "Spread spectrum systems with commercial applications: Third ed." J.Wiley New York 1994.
- [4] Prescott, Glenn e. "Spread spectrum communications [videorecording] : fundamentals and applications" IEEE Piscataway, N.J. 1989
- [5] Skaug, R. (Reidar), "Spread spectrum in communication" Peregrinus, London 1985.
- [6] Ziemler, Rodger E. "Digital communications and spread spectrum systems" Collier Macmillan, New York c1985
- [7] Simon, Marvin, "Spread spectrum communications" Computer Science Press Rockville, Md 1985.
- [8] Qualcomm 1992 "Specification for CDMA cellular telephones" ftp.qualcomm.com/pub/cdma, Qualcomm
- [9] American Radio Relay League, "Spread Spectrum Compendium" American Radio Relay League, 1991
- [10] Vincent, James (G1PVZ), "Voice link over Spread Spectrum radio" Electronics World and Wireless World, September and October 1993.
- [11] Mattos, Phillip, "Global Positioning System" Electronics World and Wireless World, December 1992, January-May 1993.
- [12] McArdle, Brian, "Wideband Wireless Data Systems" Elektor April 1993, pp40-43
- [13] Black, Uyles D. "Data Communications and Distributed Networks" Prentice Hall, New Jersey.
- [14] Lee, William C. Y. "Mobile Cellular Telecommunication Systems" McGraw
-

Hill 1992

[15] American Radio Relay League "10th Computer Networking Conference, San Jose, California September 27-29, 1991" American Radio Relay League 1991.

[16] American Radio Relay League "11th Computer Networking Conference, California September 27-29, 1992" American Radio Relay League 1992.

[17] American Radio Relay League "8th Computer Networking Conference, Jose, California September 27-29, 1991" American Radio Relay League 1991.

[18] American Radio Relay League "7th Computer Networking Conference, San Jose, California September 27-29, 1991" American Radio Relay League 1991.

[19] Mano, Moris "Computer Engineering: Hardware design" Prentice Hall, 1988.

[20] Davidovici, Sorin "On the Radio: Wireless LAN's give new meaning to the term *ethernet*" Byte Magazine June 1990, pp224A-228.

[21] James Vincent, "Spread Spectrum in Action" Electronics World and Wireless World August - September 1993.

[22] Kim, D. I. "Multiple Capture performance of DS-SS packet radio systems with common spreading codes" IEE Proceedings I [Communications, Speech and Vision] Vol 140, Issue 6. December 1993.

[23] Song, M. K., Sakong, S. C. and Tchah, K. H., "Realisation of power line modem using direct sequence spread spectrum techniques." IEEE Transactions on Consumer Electronics, Volume 39, Issue 3, August 1993.

[24] Hu, Limin "Distributed Code assignments for CDMA packet radio networks" IEEE/ACM Transactions on Networking, Volume 1, Issue 6, December 1993.

[25] Stephens, J. P., Norman D. M. "Direct Sequence Spread Spectrum System" Proceedings of the 1991 National Aerospace and Electronics Conference NAECON 1991.

[26] Dill, J. C., Silvester, J. A. "On throughput of random multi-hop packet radio networks using receiver directed CDMA" IEEE International Conference on Communications '88: Digital technology - Spanning the Universe. Conference Record.

[27] Morrow, R.K.; Lehnert, J.S. "Packet Radio Throughput in Slotted ALOHA DS/SSMA Radio Systems with Random Signature Sequences" IEEE Transactions on Communications, Vol 40, Issue 7 July 1992.

[28] Hung, Kwok-Wah; Yum, Tak-Shing, "The coded tone sense protocol for

multi-hop spread spectrum packet radio networks" GLOBECOM '89. IEEE Global Telecommunications Conference and Exhibition.

[29] Conner, Doug "EDA tools help fine tune system design" EDN, April 28, 1994, pp31-34

[30] Chase, M; Pahalvan, K. "Performance of DS-CDMA over measured indoor radio channels using random orthogonal codes" IEEE Transactions on Vehicular Technology Vol 42, Issue 4 November 1993.

[31] Unisys Corporation "PA-100 Help System Version 1.0 1st March 1995; Including PA-100 Spread Spectrum Demodulator Application Specific Integrated Circuit Technical Data Sheet and User's Guide" Unisys Corporation, Government Systems Group, Salt Lake City, Utah, USA. Published Electronically, obtained from the USA Navy Postgraduate School in California, USA.

[32] Gallant, John "Handheld receiver front ends integrate assorted components" EDN Magazine January 6, 1994, Page 49.

[33] Gallany, John "IC's and modules for digital wireless communications" EDN Magazine, August 19, 1994, Page 77.

[34] Ham-Digital, Ham-Homebrew and TCP-GROUP digests are all available on ftp.ucsd.edu. Subscriptions are available by sending email to LISTSERV@UCSD.EDU.

Chapter 5 : Packet Radio in Professional Journals

*"A good engineer is always a wee bit
conservative, Commander. At least on Paper."
Scotty, Star Trek : The Next Generation, Relics*

TCP-Group Digest[34] Packet Radio Topics in Professional Journals

by S. R. Bible, N7HPR - March 26, 1995
srbible@cs.nps.navy.mil
Naval Postgraduate School, Monterey, CA 93943

_____, IEEE Journal on Selected Areas in Communications, Vol. 11, No. 7, Sep. 1993.

_____, "Special Issue on Packet Communication Networks," Proceedings of the IEEE, Vol. 66, No. 11, Nov. 1978.

_____, IEEE Journal on Selected Areas in Communications, Vol. 11, No. 6, Aug. 1993.

_____, "Special Issue on Packet Radio Networks," Proceedings of the IEEE, Vol. 75, No. 1, Jan. 1987.

Abramson, N. "Multiple Access in Wireless Digital Networks," Proceedings of the IEEE, Vol. 82, No. 9, pp. 1360-1370, Sep. 1994.

Acampora, A. S. and Zhensheng, Z. "A Throughput/Delay Comparison: Narrowband verse Broadband Wireless LAN's," IEEE Transactions on Vehicular Technology, Vol. 42, No. 3, pp. 266-274, Aug. 1993.

Adams, S. et. al., "A Unified Network approach to the Control of Survivable Multimedia Communication Networks," MILCOM 90, pp. 323-329, Sep./Oct. 1990.

Bantz, D. F. and Bauchot, F. J. "Wireless LAN Design Alternatives," IEEE Network, pp. 43-53, Mar./Apr. 1994.

Bausbacher, P. E. and Kearns J. L. , "Transmission Parameter Selection in an Adaptive Packet-Radio Network," Proceedings of the Tactical Communications Conference, Vol. 1, Tactical Communications, Challenges of the 1990's, pp.51-68, Apr. 1990.

Bertoni, H. L. et. al., "UHF Propagation Prediction for Wireless Personal

Communications," Proceedings of the IEEE, Vol. 82, No. 9, pp. 1333-1359, Sep. 1994.

Bradley, B. D. et. al., "Simulation Issues for Future Wireless Modems," IEEE Communications Magazine, Vol. 32, No. 7, pp. 42-53, Jul. 1994.

Buchholz, D. et. al., "Wireless In-Building Network Architecture and Protocols," IEEE Network, pp. 31-38, Nov. 1991.

Caceres, R and Iftode, L, "The effects of Mobility on Reliable Transport Protocols," Proceedings of the 14th International Conference on Distributed Computing Systems, pp. 12-20, Jun. 1994.

Chang, J. J. C., et. al., "Wireless Systems and Technologies: An Overview," AT&T Technical Journal, Vol. 72, No. 4, pp. 11-19, Jul./Aug. 1993.

Chase, M. and Pahlavan, K. "Performance of DS-CDMA Over Measured Indoor Radio Channels Using Random Orthogonal Codes," IEEE Transactions on Vehicular Technology, Vol. 42, No. 4, pp. 617-624, Nov. 1993.

Cheah, J. Y. C. "A Proposed Access Method for the Wireless LAN Standard," The Third IEEE International Symposium on Personal Indoor and Mobile Radio Communications Proceedings, pp. 145-148, Oct. 1992.

Chen, K. C. and Lee, C. H., "RAP -- A Novel Medium Access Control Protocol for Wireless Data Networks," GLOBECOM '93 - IEEE Global Telecommunications Conference, pp. 1713-1717, Nov./Dec. 1993.

Chlamtac, I. and Farago, A. "Making Transmission Schedules Immune to Topology Changes in Multi-Hop Packet Radio Networks," IEEE/ACM Transactions on Networking, Vol. 2, No. 1, pp. 23- 29, Feb. 1994.

Chen, K. C. , "Medium Access Control of Wireless LANs for Mobile Computing," IEEE Network, pp. 50-63, Sep./Oct. 1994.

Cohe, D. et. al., "IP Addressing and Routing in a Local Wireless Network," IEEE INFOCOM '92, pp. 626-632, May 1992.

DeSimone, A. et. al., "Throughput Performance of Transport-Layer Protocols over Wireless LANs," GLOBECOM '93 - IEEE Global Telecommunications Conference, pp. 542-549, Nov./Dec. 1993.

Demers, A. et. al., "MACAW: A Media Access Protocol for Wireless LAN's," SIGCOMM 94, pp. 212-225

Duchamp, D. "Issues in Wireless Mobile Computing," Proceedings Third Workshop on Workstation Operating Systems, pp. 2-10, Apr. 1992.

El-Tanany, M. et. al., "Performance Analysis and Design Guidelines of a Mobitex Modem at 8 kb/s," Vehicular Technology Society 42nd VTS Conference, pp. 110-113, May 1992.

Esmailzadeh, R. et. al., "Power Control in Packet Switched Time Division Duplex Direct Sequence Spread Spectrum Communications," Vehicular Technology Society 42nd VTS Conference, pp. 989-992, May 1992.

Foschini, G. J. and Miljanic, Z. "A Simple Distributed Autonomous Power Control Algorithm and its Convergence," IEEE Transactions on Vehicular Technology, Vol. 42, No. 4, pp. 641-646, Nov. 1993.

Hashemi, H. et. al., "Measurements and Modelling of Temporal Variations of the Indoor Radio Propagation Channel," IEEE Transactions on Vehicular Technology, Vol. 43, No. 3, pp. 733-737, Aug. 1994.

Hamilton, R. L. and Yu, H. C. , "Optimal Routing in Multihop Packet Radio Networks," Proceedings IEEE INFOCOM '90, pp. 389-396, Jun. 1990.

Hendricks, D. "Wireless Off-Ramps from the Information Highways," Spring COMPCOM 94, pp. 182-184, Feb./Mar. 1994.

Hou, T. C. and Li, V. O. K. "Transmission Range Control in Multihop Packet Radio Networks," IEEE Transactions on Communications, Vol. COM-34, No. 1, pp. 38-44, Oct. 1986.

Hu, L., "Topology Control for Multihop Packet Radio Networks," IEEE Transactions on Communications, Vol. 41, No. 10, pp. 1482-1493, Oct. 1993.

Hubner, D. et. al., "A Multihop Protocol for Contacting a Stationary Infrastructure," 41st IEEE Vehicular Technology Conference, pp. 414-419, May 1991.

Jangi, S. and Merakos, L. F. "Performance Analysis of Reservation Random Access Protocols for Wireless Access Networks," IEEE Transactions on Communications, Vol. 42, No. 2/3/4, pp. 1223-1234, Feb./Mar./Apr. 1994.

Johnson, D.B. "Routing in Ad Hoc Networks of Mobile Host," 1994 Workshop on Mobile Computing System and Applications, ???, 1994.

Jubin, J. and Tornow, J. D. , "The DARPA Packet Radio Network Protocols," Proceedings of the IEEE, Vol. 75, No. 1, pp. 21-32, Jan. 1987.

Kahn, R.E. "The Organisation of Computer Resources into a Packet Radio Network," IEEE Transactions on Communications, Vol. COM-25, No. 1, pp.

169-178, Jan. 1977.

Kahn R. E. , et. al., "Advances in Packet Radio Technology," Proceedings of the IEEE, Vol. 66, No. 11, pp. 1468-1496, Nov. 1978.

Karn, P. R. et. al., "Packet Radio in the Amateur Service," IEEE Journal on Selected Areas in Communications, Vol. SAC-3, No. 3, pp. 431-439, May 1985.

Katz,R. H. "Adaption and Mobility in Wireless Information Systems," IEEE Personal Communications, pp. 6-17, First Quarter 1994.

Khayata R. and Huang, C. C. "Characterising Wireless Indoor Communications: Measurements in the ISM Bands with a Directional Antenna," The Third IEEE International Symposium on Personal, Indoor and Mobile Radio Communications Proceedings, pp. 315-319, Oct. 1992.

Kleinrock, L and Tobagi, F. A., "Packet Switching in Radio Channels: Part I -- Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics," IEEE Transactions on Communications, Vol. COM-23, No. 12, pp. 1400-1416, Dec. 1975.

Kleinrock, L. "Principles and Lessons in Packet Communications," Proceedings of the IEEE, Vol. 66, No. 11, pp. 1320-1329, Nov. 1978.

Kleinrock, L and Tobagi, F. A. , "Packet Switching in Radio Channels: Part II -- The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution," IEEE Transactions on Communications, Vol. COM-23, No. 12, pp. 1417-1433, Dec. 1975.

Kleinrock, L. and Silvester, John "Spatial Reuse in Multihop Packet Radio Networks," Proceedings of the IEEE, Vol. 75, No. 1, pp. 156-166, Jan. 1987.

Kwok, T. C. "Wireless Networking Requirements of Multimedia Applications," 1st International Conference in Universal Personal Communications, pp. 15.01.1-15.01.5, Sep./Oct. 1992.

LaMaire, R. O. et. al., "Analysis of a wireless MAC protocol with Client-Server Traffic," IEEE INFOCOM '93, pp. 429-438, Mar./Apr. 1993.

Lansdowne, Z. F. "A Stopping Rule for Link Failure Detection," IEEE Transactions on Communications, Vol. 41, No. 4, pp. 528-530, Apr. 1993.

Leiner, B. M. et. al, "Issues in Packet Radio Network Design," Proceedings of the IEEE, Vol. 75, No. 1, pp. 6-20, Jan. 1987.

Leung, V. C. M. "Internetworking Wireless Terminals to Local Area Networks via Radio Bridges," 1992 IEEE International Conference on Selected Topics in Wireless Communications, pp. 126-129, Jun. 1992.

Liu, M. K. "Base Station Networking in Personal Communications," IEEE Transactions on Communications, Vol. 41, No. 6, pp. 932-939, Jun. 1993.

McQuillan, J. M. et. al., "The New Routing Algorithm for the ARPANET," IEEE Transactions on Communications, Vol. COM-28, No. 5, pp. 711-719 , May 1980.

Magill, D. T. et. al., "Spread-Spectrum Technology for Commercial Applications," Proceedings of the IEEE, Vol. 82, No. 4, pp. 572-584, Apr. 1994.

Meier-Hellstern, K. S. et. al., "Network Protocols for the Cellular Packet Switch," IEEE Transactions on Communications, Vol. 42, No. 2/3/4, pp. 1235-1244, Feb./Mar./Apr. 1994.

Myles, A. and Skellern, D. "Comparing Four IP-based Mobile Host Protocols," Computer Networks and ISDN Systems, Vol. 26, No. 3, pp. 349-355, Nov. 1993.

Nanda, S., et. al., "A Retransmission Scheme for Circuit-Mode Data on Wireless Links," IEEE Journal on Selected Areas in Communications, Vol. 12, No. 8, pp. 1338-1352, Oct. 1994.

Pahlavan, K. and Levesque, A. H., "Wireless Data Communications," Proceedings of the IEEE, Vol. 82, No. 9, pp. 1398-1430, Sep. 1994.

Perkins, C. E. "Simplified Routing for Mobile Computers Using TCP/IP," Proceedings IEEE Conference on Wireless LAN Implementation, pp. 7-13, Sep. 1992.

Perkins, C. E. and Bhagwat, P. "A Mobile Networking System based on Internet Protocol," IEEE Personal Communications, pp. 32-41, First Quarter 1994.

Pouzin, L and H. Zimmermann, H., "A Tutorial on Protocols," Proceedings of the IEEE, Vol. 66, No. 11, pp. 1346-1370, Nov. 1978.

Roberts, L. G. "The Evolution of Packet Switching," Proceedings of the IEEE, Vol. 66, No. 11, pp. 1307-1313, Nov. 1978.

Ross, I. M. "Wireless Network Directions," IEEE Communications Magazine, pp. 40-42, Feb. 1991.

Sobrinho, J. L. and Brazio, J. M. "D-MCMA: A New Multiple Access Protocol for Distributed Wireless Local Networks," GLOBECOM '93 - IEEE Global Telecommunications Conference, pp 70-75, Nov./Dec. 1993.

Seshadri, N. et. al., "Advanced Techniques for Modulation, Error Correction, Channel Equalisation, and Diversity," AT&T Technical Journal, Vol. 72, No. 4, pp. 48-64, Jul./Aug. 1993.

Shacham, N. and Westcott, J. , "Future Directions in Packet Radio Architectures and Protocols." Proceedings of the IEEE, Vol. 75, No. 1, pp. 83-98, Jan. 1987.

Steele, R. "The Evolution of Personal Communications," IEEE Personal Communications, pp. 6-11, Second Quarter 1994.

Suzuki, T. and Tasaka, S., "A Performance Comparison of ALOHA-Reservation and PRMA in Integrated Voice and Data Wireless Local Area Networks," TENCON '92 - Technology Enabling Tomorrow, pp. 754-758, Nov. 1992.

Tanaka, R. and Tsukamoto, M., "A CLNP-based Protocol for Mobile End Systems within an Area," Proceedings 1993 International Conference on Networking Protocols, pp 64-71, Oct. 1993.

Tobagi, T. A., et. al., "Modelling and Measurements Techniques in Packet Communication Networks," Proceedings of the IEEE, Vol. 66, No. 11, pp. 1423-1447, Nov. 1978.

Tobagi, T. A. "Modelling and Performance Analysis of Multihop Packet Radio Networks," Proceedings of the IEEE, Vol. 75, No. 1, pp. 135-155, Jan. 1987.

Tsai, Y. R. and Chang, J. F. , "Using Spread Spectrum Techniques to Combat Multipath Interference in Mobile Random Accessed Networks," 1992 IEEE International Conference on Selected Topics in Wireless Communications, pp. 429-432, Jun. 1992.

Van Der Jagt, L., "A Framework for Specifying a Physical Layer and Medium for Wireless Local Area Networks," The Third IEEE International Symposium on Personal Indoor and Mobile Radio Communications Proceedings, pp. 149-152, Oct. 1992.

Vannucci, G. and Roman, R. S. "Measurement Results On Indoor Radio Frequency Re-use at 900 Mhz and 18 Ghz," The Third IEEE International Symposium on Personal, Indoor and Mobile Radio Communications Proceedings, pp. 308-314, Oct. 1992.

Ward J. and Compton, R. T., "High Throughput Slotted ALOHA Packet Radio with Adaptive Arrays," IEEE Transactions on Communications, Vol. 41, No. 3, pp. 460-469, Mar. 1993.

Wang, J. L. and Silvester, J. A. "Maximum Number of Independent Paths and Radio Connectivity," IEEE Transactions on Communications, Vol. 41, No. 10, pp. 1482-1493, Oct. 1993.

Weiser, M., "Some Computer Science Issues in Ubiquitous Computing," Communications of the ACM, Vol. 36, No. 7, pp. 75-84, Jul. 1993.

Yum, T. S. and Hung, K. W. "Design Algorithms for Multihop Packet Radio networks with Multiple Directional Antennas Stations," IEEE Transactions on Communications, Vol. 40, No. 11, pp. 1716-1724, Nov. 1992.

Vitalpur, S. V. "Evaluation of Adaptive Routing Protocols for Packet Radio Networks," Proceedings of the Tactical Communications Conference, Vol. 1, Tactical Communications, Challenges of the 1990's, pp. 105-115, Apr. 1990.

Yee, J. R. and Shiao, F. M. , "On Calculating High Throughputs in Multi-Hop Slotted ALOHA Packet Radio Networks, Proceedings IEEE INFOCOM '90, pp. 382-388, Jun. 1990.

Yee, J. R. and Shiao, F. M. , "An Algorithm to find Global Optimal Routing Assignments for a Class of PRNS," ICC 91 - International Conference on Communications, pp. 1604-1608, Jun. 1991.

Chapter 6: Literature Review

"A Hypothetical Paradox: What would happen in a battle between an Enterprise security team who always get killed soon after appearing and a squad of imperial storm troopers who can't kit the broad side of a planet?"

Tom Galloway

Voice Link over Spread Spectrum radio (Reference [10])

James presents both theory and detailed circuitry for a voice link using spread spectrum in the UHF Amateur band. The design is in a modular approach allowing working circuits to be re-used modularly in other designs. To transfer voice he digitises the voice using delta modulation obtaining a bit stream at 32k bps which is then di-phase modulated and spread. To obtain initial synchronisation the incoming BPSK signal is squared. If there is a signal present and it is in synchronisation then a signal at half the exactly carrier frequency will be generated.

This article in fact forms the basis for the hardware presented in this thesis.

Spread Spectrum in Action (reference [21])

An easy to read article on spread spectrum systems. It has a good diagram showing the interference noise added by various interfering signals to a spread spectrum signal. This article provides a more theoretical view than that presented in Electronics World and Wireless World.

Multiple Capture performance of DS-SS packet radio systems with common spreading cods (Reference [22])

The author looks at a Spread Spectrum Packet Radio Network where all users share a common spreading code deriving the performance of the system. The determination on desirability Single over Multiple spreading codes is not raised.

Realisation of power line modem using direct sequence spread spectrum techniques. (Reference [23])

Packet Radio Networks share many things in common with the highly interconnected power grid. Using some of the ideas raised in this article it should be possible to move a radio based system onto power lines bringing advantages in communication costs for distribution authorities.

Distributed Code assignments for CDMA packet radio networks (Reference [24])

Looks at Packet Radio CDMA in terms of throughput versus offered load. Parallels this with Aloha and talks about optimal assignments of spreading

codes.

Direct Sequence Spread Spectrum System (Reference [25])

Although the spread spectrum system in this article is based on those in publications of the ARRL this provides a number of interesting changes. The first is that the despreading was done at UHF frequency after a pre-amp rather than at an IF. The article also looks at BER measurement.

On throughput of random multi-hop packet radio networks using receiver directed CDMA (Reference [26])

This paper provides an alternate view to that of providing a packet network with all stations sharing the same spreading code. It looks at modelling random networks, routing, throughput and derivation of a slotted Aloha system for packet radio networks.

Packet Radio Throughput in Slotted ALOHA DS/SSMA Radio Systems with Random Signature Sequences. (Reference [27])

Yet another look at a slotted Aloha system. However it looks at error probabilities.

The coded tone sense protocol for multi-hop spread spectrum packet radio networks. (Reference [28])

Looks at the idea of using coded tones to maximise reuse of codes.

7th ARRL Computer network Conference (Reference [18])

[18a] A duplex Packet Radio repeater approach to Layer One efficiency

Scot Avent, N6BGW and Robert Finch, N6CXB investigate full duplex packet radio repeaters and why they are more both bandwidth and throughput efficient than standard simplex CSMA. Timing diagrams are included to show why they are a solution to collisions. This technology is possibly superior to CDMA due to its simplicity.

[18b] Digital Networks and Spectrum Management

Paul Flaherty N9FZX of Stanford University looks at Spectrum Management in Amateur radio. He looks at issues including frequency and space division multiplexing and their relation to CSMA packet radio.

[18c] Cellular area coverage transport networks

Here a proposal is for a cellular type network with nodes being on at intersection points of the hexagonal cellular diagram with 3 connections to nodes adjoining. Users are kept from these link frequencies with each node providing network access out of band. Frequencies may be reused with an algorithm. about 10 different frequencies are required for the network links to avoid interference.

[18d] 9600 baud packet radio modem design

James Miller produces a well designed modem using some novel techniques which I have gone on to use in my modem. James has relied on EPROMS to store transmit waveforms as well as the state machine for clock recovery. This design includes a scrambler circuit. Although the scrambler is useful for Satellite work this modem has since become a standard with the scrambler adding complexity ultimately stunting growth. In most cases it has been found that the scrambler is not required The computer models of waveforms are a trademark of any article of James Miller.

8th ARRL Computer Network Conference (Reference [17])**[17a] A packet broadcast protocol**

The author managed to write a paper with few specifics but did include useful event diagrams showing the flow of information in a network where most of the information was being transmitted on a common high bandwidth channel. The protocol suggested was a selective retransmittal one.

[17b] Licence Free Spread Spectrum Packet Radio

This article was based on the USA regulations including FCC regulations part 15 and 97 with recommendations for changes. The conclusion of the article was important as it highlighted applications for Spread Spectrum in the Packet Arena. If this document is an indication to the packet work being done in the real world on Spread Spectrum then my thesis is really needed.

[17c] Design of a next generation packet network.

The author points out that 1200 AFSK is quite good for quick growth of a packet network however the growth might slow due to saturation.

[17d] Local Distribution in the Amateur Radio Environment

The Italian authors point out that packet radio as implemented is often done in a semi-centralised environment with most activity centred on a few high usage systems. This paper therefore looks at alternatives to the CSMA commonly used and introduces the R-ISA access scheme as a solution. It looks of limited use for my applications.

[17e] Design of a Next-Generation Packet Network

Bdale Garbee, N3EUA attempts to design an upgrade for a large packet type network and make proposals based on high speed microwave links between regional nodes.

[17f] A study of High Speed packet radio

The author makes the case for a specialised high speed packet radio rather than the modified voice radios commonly in use. The article addresses many of the issues facing conventional packet radio although these comments are only valid in showing why Spread Spectrum radio communications would be useful.

[17g] Proposed AX.25 Level 2 Version 2.0 Changes" Terry Fox, WB4JFI

A technical look into the issues of upgrading the AX.25 specification.

[17h] "Overview of the ARRL Digital Committee Proposals for enhancing the AX.25 Protocols into Revision 2.1" Eric Scac, K3NA.

The official recommendations on an upgrade of the AX.25 protocol which still had not been adopted.

[17i] "DAMA - A new method of handling packets? Detlef J. Schmidt, DK4EG, Tr. Mark Bitterlich, WA3JPY.

The author makes the case for a modification of AX.25 to permit DAMA access with very little in the way of software patching. Looking at the evidence it seems that DAMA is good in a situation where there is a master where most traffic is destined. It would probably need a lot more effort to get the system working in a multiple master anarchaic network.

IC's and modules for digital wireless communications (Reference [33])

An overview of IC's and modules especially designed for digital wireless telecommunications is presented.

The ARRL Spread Spectrum Sourcebook (Reference [15])

[18a] Spread Spectrum Applications in Amateur Radio

William E Sabin W0IYH. QST July 1983.

Sabin gives a wide overview of spread spectrum communications. Simple block diagrams are used to show many different structures for transmitters and receivers, of both Direct Sequence and Frequency Hopping.

[18b] Spread Spectrum Theory and Projects

From the 1991 ARRL Handbook for radio amateurs.

Broad overview of the entire subject of spread spectrum including a baseband transceiver. Worthy of further investigation.

[18c] Experimenting with Direct Sequence Spread Spectrum

Andre Kesteloot, N4ICK

The author presents a practical Morse Code transmitter and receiver operating at baseband using spread spectrum.

[18d] Extracting Stable Clock Signals from AM broadcast Carriers for Amateur Spread Spectrum applications.

The author presents an alternative to the transmitted reference architecture by using broadcast stations as the synchronisation source. Since it is unlikely that the broadcast station will drop out or be jammed this enables the system to be resynchronised faster and maintain synchronisation longer. A circuit diagram is given.

[18e] Practical Spread Spectrum: Achieving Synchronisation with Slip-Pulse Generator.

It appears that the slip pulse generator is a 'dumb' synchroniser reducing the cost of receivers. Periodically whenever the system is out of sync the slip pulse generator adds a pulse to shift the sequence.

[18f] A practical Direct Sequence Spread-Spectrum UHF Link Andre Kesteloot.

Further extending previous articles, Kesteloot adds transmitter and receiver modules to the system.

[18g] Practical Spread Spectrum: Clock recovery with the Synchronous Oscillator.

The synchronous oscillator is presented as the saviour to all the problems of clock recovery from a bursty signal.

[18h] Practical Spread Spectrum: An experimental Transmitted Reference Data modem.

In this design two carriers are transmitted. One with the PN sequence encoded onto it and one with the PN and Data encoded onto it. It is relatively simple to maintain synchronisation to the PN Only carrier and apply this to the joint carrier.

Handheld-receiver front ends integrate assorted components (Reference [32])

This article presents not only a theoretical primer on the Low Noise Amplifier's (LNA's), Power Amplifier's and mixers required for the emerging wireless technologies but provides an overview of suppliers with suitable products.

Appendix 1 : Thesis 1 Report

Introduction

With the increasing computerisation of process control systems distributed over a wide area there have been increasing demands placed on the communication system connecting these systems.

The industrial environment holds certain challenges to those wishing to implement such a distributed control system. In many cases the system may be distributed over many hundreds of square kilometres with diverse terrain and accessibility.

Ideally wired communications would be used in a control system, although in an environment such as a power station there are places where it is not feasible for technical or economic reasons to install a cable for control system telemetry.

Even where a cable is installed there are often cases where cables fail due to age or a number of external factors such as explosion or a cable being broken by machinery. Many cables which fail cannot be economically repaired or replaced.

In many processes inside a Power Station such a failure of telemetry would cause significant problems. For instance should a cable to the coal conveyor fail there is only a window of about 30 minutes where the cable can be repaired without having the whole power station fail.

The current trend is to install dual FDDI fibre optic links although it has been known for these to fail. Ideally some type of backup for these types of links are required. FDDI does reconnect itself back into a loop but there are times when a single accident can split the network.

Also around power stations there are often environmental logging equipment which can supply data at a slow data rate but can be quite useful in reducing the possibility of environmental damage. That is they could if they could be monitored.

Another problem in substations incoming lines are required to be isolated from the substation itself in case of faults. An external radio link has no such need of isolation from incoming earth potential

My thesis is based on the Telecommunications Strand and as such contains a great deal of work specific to telecommunications. However I am endeavouring during this project to make the project potentially useful to Pacific Power in the future as a way for Power and Machines as well as Instrumentation and Control Engineers to transfer the information that they require efficiently and reliably.

Because it this project is designed to operate in a high electrical noise environment

like a power station I will need to use many cutting edge technologies. These are technologies such as Code Division Multiple Access (CDMA) communications using Spread Spectrum. In order to facilitate its use in over a large terrain I will need to implement the system as a Packet radio Network.

The prototype of this project is being designed to operate in one of the bands used by Amateur radio Operators. However it is envisaged that the project could easily be modified to operate in an ISM (Industrial, Scientific, Medical) band and could operate there without a licence.

The technology that I am basing my thesis on is fairly new. The technology is currently being used for military communications as well as civilian systems such as the Digital Advanced Mobile Phone System used in North America as well as other locations around the globe. With the end of the cold war this technology can be used to maximise throughput in the presence of interference rather than jamming.

A further extension to this work would be to extend the concepts worked on to operate over a Power Line Carrier system. By using spread spectrum communications on PLC's we can reduce interference problems that cause degradation to the signals sent over PLC as well as reducing the problems caused by limiting the bandwidth we are required to use over high voltage power lines.

Some pioneering work on this concept is being done by California Edison in the United States. In fact by using a CDMA system for metering it would be almost impossible for jamming or alteration of data through the system. It would also be possible (assuming that switching paths didn't change) to determine if even a few feet of wire has been added to rewire a meter.

The classic problem with the PLC system in the past has been the noise on the lines rather than the bandwidth available. However by using CDMA techniques the bandwidth may be increased and the noise decreased.

In my thesis I hope to use my time to bring all that I have learnt in the course together to the advantage of Pacific Power and myself.

Scope of Thesis 2

The broad aim of this project is develop software and hardware such that it is possible transmit data over radio links in the presence of interference.

I am not interested in keeping the data secret. I am more concerned that no interference from others operating spread spectrum interfere with my communications.

I will be investigating the ways that a land based Spread Spectrum Packet Radio Network might operate in relation to more conventional techniques. I will also be investigating code assignments for optimal throughput and ease of implementation.

I will be investigating the possibility that it may be worthwhile also using a channel with standard modulation techniques for link set up. I will also investigate alternate channel access and theoretical channel throughput.

I will be investigating cheap receiver and transmitter architecture with emphasis on commercial television modulators and tuners.

I will be investigating the properties of existing Packet Radio Networks. Where they fail I will attempt to show that in many cases Spread Spectrum can offer distinct advantages.

It is my intention to assist an associate over the summer 1994-5 period in a design for a cheap Asynchronous to Synchronous converter. However if this fails I will still be able to use more expensive converters.

I will not be greatly concerned about initial synchronisation time but I will attempt to minimise it where possible.

I will be attempting to implement the system using conventional analogue and digital electronics without the use of Digital Signal Processing processors. I feel that implementation using digital signal processors would however be a good extension for another undergraduate thesis or as part of the requirements for a masters thesis in addition with improvements in other parts of the system.

Licenceing

The Spectrum Manager on behalf of the Spectrum Management Agency (SMA) has determined that I am fit to hold an Amateur Operator's Limited Certificate of Proficiency (AOLCP). Under the terms of this licence I am permitted to operate a transmitter with a power output of up to 150 Watts (P.E.P.) in various bands above 52 Mhz.

I am intending that my design will be in the range of either the 70 or 50 cm amateur bands where wide-band pulse modes are permitted to be transmitted. There has however been no declaration on the use of Spread Spectrum by Amateurs in Australia by the SMA. In private electronic communication several SMA employees have informed me that Spread Spectrum is quite legally able to be transmitted so long as all other regulations are obeyed.

In addition I will be operating during testing on such a power that if the transmissions were in an ISM (Industrial, Scientific and Medical) band they would be allowable without licensing.

Should during my work I find that the transmission of general spread spectrum is not permitted my experiments would still be permitted with the superposition of a Television Synchronisation Signal over my spread spectrum signal. Although this would cause time domain distortions it is possible in a worse case scenario.

Required Resources

One of the most important resources required during a project such as this is access to test equipment. Such test equipment would include a spectrum analyser, wide-band noise source, attenuators, Signal generators, power supplies, an oscilloscope and passably a soldering iron. Weekend access to these resources would be an advantage, especially over the christmas break.

As I have my own laptop computer it may be used to generate sequences required for experimentation and link analysis although access to a personal computer specifically for BER measurement would be useful.

For modelling of systems I will require access to a computer system such as the Sparc workstations owned by the School of Electrical Engineering and also the SPW program running on them. Access to the BOSS package might be useful.

One other important resource that I will be requiring is a microprocessor of some type to help with synchronisation and generation of spreading codes. One of my associates from the local amateur radio club has offered to provide a suitable controller. Should that development effort fail I have access to several commercial units suitable for this purpose.

As this is a project based on Hardware and Software rather than just on the software or the theory it is hard to determine with absolute certainty the resources required.

To assist with my experiments and design I have outlines a number of projects from electronics magazines that would be useful. They are

TV Field Strength Meter

Low cost spectrum analyser

Wideband noise signal generator

Techno-Whizzy transceiver

An Asynchronous to Synchronous converter will be required. An associate is working on this. If my associates project doesn't get finished in time or perform properly I have access to some more expensive converters.

List of Thesis 2 Deliverables

At the completion of Thesis 2 I will have submitted a number of items for evaluation. The first of these is the Thesis 2 dissertation containing all the information required to reconstruct the work I will be doing during the course of the thesis.

The Thesis 2 report will contain all circuit diagrams and all code on either a machine read form or on paper.

Also deliverable will be Spread Spectrum modems for transmit and receive. These modems will convert a serial bitstream to an appropriate I.F. and back. At this stage it has not been determined what the I.F. will be or the specific modulation technique.

Subject to the availability of time hardware suitable for use of the modems over a Radio Frequency link may be submitted.

With correct planning at the end of this project I hope to be able to place the transmit and receive modems several kilometres spatially diverse and transmit data with a high immunity to noise. While testing this system with 2 transmitters and one receiver would be ideal that may not be possible due to time and resource limitations.

Proposed development cycle.

During Thesis 2 I intend to implement the system in the following way.

Design and implement a system of modems and links suitable for transferring data at a rate suitable to fill the channel being used. This link is to have a reasonable BER on completion of this stage. It is not to be transmitting using spread spectrum techniques.

Add a PN generator to the transmitter with the option of being able to change the tap points to generate different sequences. Synchronise this to the bit-rate using a PLL. Ensure that the output looks significantly like noise with minimal peaks.

De-modulate and de-spread the Spread Spectrum signal. However with the use of reset and clock pulses maintain the two in synchronisation.

Add a Early-Late synchronisation loop to enable lock to be maintained if the clock pulses are removed and the clock frequency changes slightly.

Add a synchronisation loop to lock an incoming signal regardless of its phase in relation to a reset pulse.

Investigate methods of identifying users of the channel if we choose assignment of multiple spreading codes.

Parts of the Final Report

Bit Error Rate. Theoretical and practical results at each stage of development. Methods of determining the Bit Error Rate. Also looking at the sensitivity to noise of the signal.

Circuit description. Features of the circuit allowing the project to be re-constructed at each step.

Present usage. What are the problems with traditional Packet Radio Networks and traditional Spread Spectrum links.

Code Assignment. What is my view of code assignment in a packet radio network.

Routing and I.D. Who is out there? How do I know they are there? What is the best way to get through the network? Will a Radio Short Path First protocol work? If it will not how can it be modified? Is Short Path First more appropriate?

Modelling. What is the theoretical throughput of this system? How does it achieve this? What can I do better? Can a packet network using these elements work?

Modelling

- 1 - Model the proposed system at each stage of development
- 2 - Model different methods of setting up the packet network.

Software

- 1 - Setup the loops for the two synchronisation.

Questions to be Answered.

- 1 - What channel coding should I use?
- 2 - How can i decrease the acquisition time of the receiver?
- 3 - What protocol should be used over a SS packet radio network?
- 4 - What needs to be done to make this work over PLC?

Assumptions

In packet radio networks each station needs to transmit and receive data packets. Where the network is highly distributed there can be no central node acting as a hub or repeater. In this case the decision must be made as to how frequencies are assigned. Separate transmit and receive frequencies work well with a centralised repeater but not in a highly distributed system.

Therefore I am proposing that the system that I am working on operate on a single frequency only. This will allow any station within hearing distance to hear the transmitting station even if other stations stop working.

In a packet system there are also times where high power is required for long links. In this case there will be high transmit power level and in the case of a full duplex system a still weak receive level.

It has been shown that up to 26 db separation may be obtained using orthogonal transmit and receive codes. Where low power levels are being used this in addition with the process gain would allow full duplex operation. However under higher power levels half duplex operation is required.

To reduce the cost and complexity I will be working on a half duplex system only.

Appendix 2: Phil Karn Qualcomm CDMA.

The following appeared in the TCP-GROUP mailing list [34], and is written by Phil Karn, KA9Q. He is a vice president of Qualcomm. It is included here as it is quite a good description of the Qualcomm CDMA cellular telephone system

I promised some details on Qualcomm's CDMA system, so here they are.

*The gory technical details will soon be publicly released when we submit our system to the new TIA committee that was recently formed to accept proposals for wideband (i.e., spread spectrum) cellular telephone systems. I don't know what the procedure will be to get copies, and in any event the spec is *quite* thick. So your best bet for getting a general technical overview is to look up any of several papers that have already been published about the system in the past year or so.*

Probably the best reference is the paper "On the System Design Aspects of Code Division Multiple Access (CDMA) Applied to Digital Cellular and Personal Communications Networks" by Allen Salmasi and Klein S. Gilhousen [WT6G], from the Proceedings of the 41st IEEE Vehicular Technology Conference, St Louis MO May 19-22 1991.

There are also several papers on Qualcomm's CDMA system in the May 1991 IEEE Transactions on Vehicular Technology, including one on the capacity of CDMA.

Just to summarise the system:

- The Qualcomm CDMA cellular system uses direct sequence spread spectrum. The chip rate is 1.2288 megachips/sec.*
- The RF channel spacing is 1.23 Mhz (the first spectral nulls occur at the chip rate, and digital filtering essentially eliminates the extra sidelobes).*

There are actually two spreading sequences

- a "short" sequence of 32768 chips*
- a "long" sequence of $2^{42}-1$ chips*

The short sequence is generated by a pair of 15-stage PN generators (one polynomial for I, a different one for Q) and is applied in offset quadrature to all signals, both forward (cell-to-mobile) and reverse (mobile-to-cell) links. The reason for using two (I and Q) sequences is to reduce the peak-to-average ratio of the resulting signal to make it more friendly to

RF power amplifiers. The polynomials are the same for all cell sites and mobiles.

Note that the short code is one chip longer than the 32767 chip sequence that would be generated by a 15 stage LFSR. An extra chip is added to round the total out to 32768 (2^{15}). This simplifies system timing.

A "long code" PN sequence of length $2^{42}-1$ is applied in addition to the short code on traffic channels, i.e., those channels carrying user voice and/or data. Different phases of this sequence are assigned to different mobiles to preclude the possibility of them "colliding" by transmitting correlated spreading sequences. (Again, the polynomial is the same for all mobiles and cell sites).

The cell transmits the sum of the forward link spread spectrum signals to all the mobiles in its territory. The composite forward link signal always includes a "pilot", a carrier modulated only by the short PN sequence. At power-up a mobile acquires this pilot's timing, locks an oscillator to it and uses it for all system timing. Finding the pilot takes only a few seconds because the sequence is so short.

The forward link consists of 64 orthogonally multiplexed channels, with each channel covered by one of 64 Walsh code sequences. Three channels are used for overhead (pilot, sync and paging) so 61 are left for user traffic. The reason for using orthogonal coding on the forward link is to allow the cell to vary the power allocated to each channel over a modest range without the inter-channel interference that would otherwise result from the "near-far" problem. This is possible only because all of the signals leaving the cell are synchronised to a common clock.

By the way, each cell site derives its PN clocks and carrier frequencies from a rubidium oscillator in a GPS timing receiver. This keeps the relative timing errors between cell sites down below a microsecond, which is important for the "soft handoff" feature I'll describe later. (Actually, each cell's PN sequences are "offset" by a specified amount from each other to ensure that they can always be resolved separately by a mobile, no matter where that mobile is in the system.)

The reverse (mobile-to-cell) link from a given mobile only has one channel, so it uses Walsh functions in a different way to provide 64-ary encoding. That is, each group of 6 data bits is transformed into one of the 64 sixtyfour-chip Walsh codes. This spreads the energy of a given bit out over time to make it more resistant to very short fades.

On top of the spread spectrum modems in both the cell and the mobile, some fairly strong interleaving and Forward Error Correction (FEC) is used: K=9 rate= $\frac{1}{2}$ convolutional coding for the forward link and K=9 rate= $\frac{1}{2}$ coding

for the reverse link. Viterbi decoding is used at each end. FEC significantly reduces the power required to maintain communications; we typically run at somewhat less than 7 dB E_b/N_0 .

User voice is encoded and decoded with a variable rate vocoder that currently runs on an AT&T DSP-16 chip. It operates at data rates of 1200, 2400, 4800 and 9600 bps. When a user talks, the 9600 bps data rate is generally used. When the user stops talking, the vocoder generally idles at 1200 bps so you still hear background noise; the phone doesn't just "go dead". The vocoder works with 20 millisecond frames, so each frame can be 3, 6, 12 or 24 bytes long, including overhead. The rate can be changed arbitrarily from frame to frame under control of the vocoder.

The RF modem varies its average transmit power automatically depending on the vocoder frame rate to keep the received E_b/N_0 ratio constant. E.g., when going from 9600 bps to 4800 bps, the transmitter drops its average output power by 3 dB; when going from 9600 bps to 1200 bps, average power drops by 9 dB. I say "average" because the peak power remains constant; average power is actually adjusted by pseudo-randomly "muting" the transmitter during some fraction of the transmitted symbols in the frame. Because of the strong FEC and interleaving, this has the same net effect as leaving in all of the transmitted symbols and reducing the average transmit power, but it was easier to implement.

The variable rate vocoder/variable power transmitter combination helps increase overall system capacity by assigning full resources to users only while they are actually talking. Since on average only 40% of the users in a large system will be talking at any one instant, this results in roughly a 2:1 system capacity increase.

One of the biggest problems with traditional spread spectrum (especially the direct sequence kind used in Qualcomm CDMA) is the "near/far" problem. In CDMA, you have many mobiles all transmitting to the same cell at the same time, and some of those mobiles may be much closer to the cell than others. Something that adjusts the transmit powers of those mobiles so that they all arrive at the cell with roughly equal signal strengths is necessary.

Qualcomm CDMA does this with a two-part automatic power control system. An "open loop" power control system in the mobile simply measures the total received signal energy and varies its transmitter power in inverse proportion; the actual formula is

$$P_{tx} = 73 \text{ dBm}^2 - P_{rx} + \text{adjust} + \text{system constraints}$$

where P_{tx} and P_{rx} are transmit and receive powers in dBm, respectively. (I'll talk about the "adjust" term shortly.)

The open loop system does almost all of the work. Because it's a broadband spread spectrum system, the highly frequency selective, deep Rayleigh fading you see in narrowband systems ("mobile flutter") just don't occur in our system. I.e., the forward and reverse links are much more closely correlated in a spread spectrum system than they are in a narrowband system, so this scheme works well.

It's not perfect, however, so there's an additional closed-loop power control system that makes fine adjustments. The cell measures the instantaneous E_b/N_0 ratio for each mobile and compares it to a threshold (e.g., 7dB). If the measured ratio is higher than the threshold, the cell sends a "go down" command to the mobile. If the measured ratio is lower than the threshold, it sends a "go up" command. The mobile adjusts its power up or down by typically 0.5 dB for each such command and keeps the total in the "adjust" term shown in the formula above.

The commands are actually sent as a 800 bit/sec bit stream that is "punctured" out of the convolutionally encoded data stream going to the cell's transmitter. That is, when it's time to send a power control bit the transmitter simply substitutes the power control bit in place of the data symbol that would normally be transmitted. Again, because of the very strong FEC and interleaving that is used, the receiver has no trouble decoding the correct user data bits despite this intentional source of "errors". If the cell is happy with the mobile's power level, it simply sends an alternating up/down/up/down sequence. Think of it as a servo loop with a delta-modulated error signal channel. The power control bits are not error protected because the additional delay would be intolerable, but they are highly resistant to errors because of the self-correcting nature of the feedback loop. Errors in the power control bits only slow down the response of the power control loop; they generally don't introduce biases.

In load tests, the E_b/N_0 ratio differences (actual - desired E_b/N_0) as measured at the cell sites typically average to 0 dB with a standard deviation of about 1 dB. You see somewhat lower standard deviations for close-in mobiles and larger deviations for mobiles at the hairy edges of the cell. You also have higher deviations for the lower data rates since the power control bits are being punctured out by the power adjustment mechanism.

We found that in practice, adjusting the power control thresholds as a function of the observed error rate on the link is better overall than picking arbitrary E_b/N_0 set points. I.e., you can run below 7 dB with good results for the guys who are nearby (and who have tighter power control), give some of this extra margin to the guys on the edge who need it, and use the rest to increase overall system capacity.

The power control mechanism is probably the single most impressive part of CDMA. You don't have to run the usual 10-20 dB or more of margin required by mobile FM systems to carry you through those brief but deep and annoying fades. You use only the exact amount of power you need at any instant. (The resistance of spread spectrum to multipath fading also helps considerably).

There are three separate mechanisms that control transmitter power. One is the open loop component that responds to receiver AGC. This responds very quickly, within microseconds. Another is the closed loop component driven by the cell's transmitted up/down bits. These first two components are summed and together they control the gain of the analog transmitter stages. (I'm not sure of the actual mechanism, it's probably done by summing the AGC voltage with the output of a DAC and using the result to control an analog voltage-controlled attenuator.) This mechanism has no effect on the peak-to-average power ratio.

The third component of power control is the pseudo-random transmitter muting mechanism that does lower the average power while leaving the peak unaffected. This is only used when transmitting at rates less than 9600 bps, and there are only four settings: full power (no muting) for full rate 9600 bps frames, half power (half the symbols muted) for half rate 4800 bps frames, quarter power (three quarters of the symbols muted) for quarter rate 2400 bps frames, and eighth power (7/8 of the symbols muted) for eighth rate 1200 bps frames.

The idea is that the power level as set by the closed and open loop mechanisms is a function only of the RF link; it doesn't have to track the variations caused by the vocoder switching data rates.

I routinely see the mobile's transmit power go below 1 milliwatt while driving around San Diego, even when I'm a mile or so from the cell site. If you're directly adjacent or underneath a cell site, the total received RF energy from the cell can actually exceed the transmit power you're putting back into the antenna! (I've seen transmit power go below 100 nanowatts a few hundred feet from the cell). These exceptionally low power levels obviously have some strong implications for solving RFI and biohazard problems.

The low power levels and the inherent resistance of spread spectrum to interference (either from narrowband signals or from other, uncorrelated spread spectrum signals) are what makes CDMA so spectrally efficient. A typical analog FM cellular system can use only $1/7$ th of the total number of channels in each cell, due to the need to protect adjacent cells against interference. In CDMA, however, every cell can use the same frequency even if their coverage areas overlap. Since the processing gain in our system is

$$10 * \log_{10} \left(\frac{1.2288 \text{ Mc/ Sec}}{9600 \text{ bits per sec}} \right) = 21 \text{ dB}$$

The required receiver E_b/N_0 ratio is 7 dB. Therefore it is possible to receive a signal even when it is $21 - 7 = 14$ dB below the interference from another cell! So if you're on the border between two cells on the same frequency and you're receiving them with equal strengths, you can easily demodulate one, the other or both.

This is the principle behind "soft handoff". In CDMA, when you drive from one cell to another, you send a message back to the system reporting the reception of the new cell's pilot. The system responds by setting up another traffic channel through the new cell, in addition to the one you already had on the old cell. Now you can combine the signals from both cells before decoding, so if the signal from one cell fades, you are likely to still have the other. Similarly, both cells receive your reverse link signals, funnelling them to the MTSO for combining into a single data stream.

As you move further into the new cell, eventually the mobile will lose the signal from the old cell and report this to the system, which will deallocate your original traffic channel. All this happens transparently and automatically, with no audible effects (unlike FM). I get a real kick out of demonstrating CDMA soft handoffs to people who are familiar with FM cellular, especially when they ask "when do we do the handoff?" and I explain that we have been doing them several times per second for the past full minute!

To do soft handoff, you need multiple spread spectrum receiver channels. Our mobiles have three such channels ("fingers"), all on a single ASIC. They can be allocated by the control CPU to track multipath signals from the same cell separated by at least a chip time (814 ns or 244 meters differential path length), signals from different cells during a soft handoff, or any combination thereof.

For example, one finger might be tracking a direct signal from cell site #1, a second tracking a reflected signal from the same site, and the third finger could be tracking a signal from cell #2 once a soft handoff has been set up.

The mobile continuously searches for and locks onto the three best signals it can find. (The more fingers the better, but returns diminish rapidly above 3 fingers.)

The heart of the CDMA system is 5 full custom ASICs. Two are for the mobile, two for the cell, and one is for both (a Viterbi decoder). In San Diego we have a demonstration/qualification system consisting of 5 cells co-located with conventional FM cellular equipment in PacTel cell sites. It operates in the B' segment (the extended wireline carrier band). All are on the same RF channel. The forward links are centred on 892.74 Mhz and the reverse links 45 Mhz lower, on 847.74 Mhz. PacTel has cleared out conventional FM cellular operations in San Diego for this segment, although it is heavily used for FM up in Los Angeles (we can occasionally see them on the spectrum analyser, but they don't normally bother us because of the isolation afforded by the spread spectrum processing gain.)

The MTSO (we call ours a "QTSO") is at Qualcomm. We have almost a hundred prototype mobiles, most of which were used in the formal capacity field tests last November. Somebody counted up the total miles driven, mostly in circles, during that test; I think it amounted to the tens of thousands. We proved that CDMA can support 10-20x the capacity of a conventional analog FM cellular system using the same bandwidth. We are now in the interesting position of having a digital cellular system with considerably more practical experience behind it than the so-called "standard" TDMA digital cellular system!

If any of you are attending the TAPR meeting in Tucson this weekend, I plan on bringing my CDMA mobile phone to show. Unfortunately, we won't be able to make CDMA calls just yet from Tucson!

The algorithm is called QCELP, Qualcomm Codebook Excited Linear Prediction.

Phil Kahn, KA9Q