DESIGN TRADEOFFS FOR FREQUENCY HOPPED VHF NET RADIOS

John S. Slechta and Glenn S. Williman

US Army CECOM
Fort Monmouth, New Jersey 07703

ABSTRACT

Army Combat Net Radio (CNR) poses a unique set of operational and equipment requirements when compared to those of non-military users. A new generation of radios presently in development must provide all the capabilities of the current radios plus several new ones, notably an active ECCM capability. This paper illustrates how the ECCM design is driven by the electronic warfare threat and by the deployment peculiar to CNR. Considerations in selection of frequency hopping as the ECCM technique are discussed, as well as the design trade-offs necessary to achieve a balance between the conflicting requirements of performance against the threat, self-interference and interference to non-hoppers, and user-transparent synchronization.

INTRODUCTION

Combat Net Radio (CNR) is a term used in the Army to describe tactical communication equipment for "shoot and move" operations. The equipment is manpack or vehicle transportable and is generally associated with the smaller army organizations from battalion down to squad level. CNR is confined to the 30-88MHz frequency range and currently uses a narrow band FM channelization plan (25kHz).

Commercial mobile communication systems are generally modeled as cellular systems; a base station or repeater is located in each cell with a high power transmitter and an optimally located omni-directional antenna that can easily cover the entire cell. Separate frequencies are assigned to different users, with split frequency operation used to allow full duplex communication. Commercial systems can be viewed as discrete address/frequency type systems, where the mobile user communicates on a point to point basis with other mobile users or with fixed locations.

Army CNR distinguishes itself from such commercial systems by requiring a number of users to be netted with each other, sharing a common net frequency, without the luxury of a central node or base station. Each member of the net could be continually changing locations, and all members need to be able to communicate with all other members of the net at any given time, in a push-to-talk or half-duplex manner. In addition, CNR must be capable of changing net frequencies anywhere within the range of 30-88MHz, must be small and lightweight for man-portable operation, ruggedized for extreme environments and simple to operate. Without the benefit of a central base station, CNR performance is subject to environmental noise limitations and relatively low transmitter powers (5 to 50 watts). With unit deployments and restricted operating frequencies it is subject to interference limitations, and in a hostile (enemy) environment subject to intentional interference or jamming. In short it must operate in a "worst case" scenario. A typical Army Division covering a 30 x 60 km area may have as many as 3300 separate radios organized into some 350 functional nets, including field artillery, air defense, combat support, and combat service support nets. There are also administrative and logistics nets, and intelligence nets. Typical planning ranges are 8 km for the man-pack radios and 35 km for the vehicular radios. Important constraints on the design of the manpack radios have always been imposed by the need to limit size and weight as well as battery consumption. The relatively large number of radios dictates that life-cycle costs be low also, even though small size tends to force equipment cost the other way.

The traffic to be handled by CNR includes voice, analog data (FSK tones) and digital data at rates up to 16 kb/s. For frequency hopping, voice is converted to 16 kb/s data by delta (CVSD) modulation, the tone FSK to 16 kb/s data by any of a number of means, and low rate digital data to 16 kb/s by redundant encoding and decoding (with error rate improvement as a bonus). Thus all traffic can be transmitted at an over-the-air information rate of 16 kb/s. The maximum threshhold bit error rate (BER) required by the Army at 16 kb/s is 10%.

EW THREAT TO CNR

By their nature, fixed-frequency radios in battlefield forward areas are subject to three main types of electronic attack.

Intercept

Intercept is "listening-in" to transmissions to obtain intelligence information from them. It can be countered by encryption of the voice or data traffic (but this tends to encourage jamming).

Direction Finding

Direction finding (DF) is using an array of spatially separated DF receiving stations to determine the location of a transmitter. The enemy's use of this information can take several forms, of which intelligence-gathering is the least drastic.

CH 1734-3/82-0001/$00.75©1982 IEEE

Jamming

Jamming can be used to jam one or many operating frequencies, thus denying communications (as well as the possibility of intercept and DF). The types of jammers potentially available to the enemy include the following:

Narrowband (CW) Jammer. In this type all the RF power is concentrated in a single channel. It could be defeated by spectrum spreading over many channels by either direct sequence techniques or, since the jammer cannot be rapidly retuned to a new frequency, by frequency hopping. The AJ margin increases directly with the total spread bandwidth, since this jammer can attack only one channel at a time.

Wideband Jammer. The jammer's power is spread over many channels, either as broadband noise or as a comb-like spectrum with each noise-modulated tooth of the comb sitting in the center of a 25 kHz channel. This type of jammer is effective against any spread spectrum system, whether direct sequence (DS) or hopping and irrespective of hop rate, as long as it jams a significant percentage of the spread bandwidth. To do this effectively requires the wideband jammer to put as much power in every channel as the narrowband jammer can concentrate in only one channel. Our AJ margin against the wideband jammer depends on the fact that he is forced to spread his power among many channels. In this respect the frequency hopper has an advantage over DS spreading in that its channels need not be contiguous; they can be scattered over the entire 30-88 MHz spectrum. This complicates things for the broadband jammer since he cannot readily manipulate his output spectrum to attack only the hopping channels and avoid wasting power in the intervening ones (which he may need for his own communications). A single broadband jammer might have a 10 MHz bandwidth; therefore six of these could jam the entire 30-88 MHz band, with relatively simple operational control. An important penalty for the enemy is that he tends to jam his own communications, and also provides a high-power, high visibility target which facilitates jammer destruction.

Repeat Jammer. This jammer receives a signal, delays it for a preset amount of time, and rebroadcasts it at high power. It thus functions to corrupt the desired signal with multipath distortion at the friendly receiver. But if the repeater is too close to the receiver (or too powerful) the repeated signal takes over via the FM capture effect and the message is received anyway, with the "aid" of the jammer. The repeat jammer can be effective in a one-on-one situation but, since it repeats all the signals it receives, either the multiple-emitter CNR environment or intentional spoofing will cause it to divide its available transmitter power among the many repeated signals, thus rapidly losing its effectiveness for any one of them. Like the wideband noise jammer, it tends to jam the enemy's own communications also.

Follower Jammer. This is in effect a CW jammer which can be retuned very rapidly to follow a hopping signal. A compressive scanning receiver and real-time computer processing enable a limited number of nets to be sorted out of the multiple user environment and attacked individually. If the number of nets to be sorted is not too large, this is an extremely effective jammer since all its power can be concentrated in the single channel it is attacking at a given instant.

Our only defense against the follower is to "outrun" it by hopping fast enough so that the propagation delay from transmitter-to-jammer-to-victim receiver (plus the processing delay) prevents the jamming signal from reaching the receiver until after it has hopped off that frequency.

ANTIJAM TECHNIQUES FOR CNR

Jamming can be countered by passive or active means, which further subdivide into operational procedures and electronic techniques. Here we will be concerned with active electronic countermeasures, which may be used together with passive electronic methods such as null-steering antennas, and with familiar operational measures like transmit power adjustment, antenna siting, etc. In a CNR environment (many simultaneous users in a crowded RF spectrum) the most suitable active ECCM is some form of spectrum spreading. Of the available forms, including pseudo-noise (PN) direct sequence (DS), burst, chirp, and frequency hopping, only frequency hopping has the required properties for RF compatibility in the crowded VHF band. This results from its capability to hop on only a set of assigned channels while deleting those which need to be avoided. While the continuous RF spectrum of the other forms of spread spectrum makes them difficult to detect at normal range, it tends to jam friendly narrowband receivers at close range which share the operating bandwidth. Conversely a DS receiver is susceptible to friendly narrowband transmissions at close range.

For example, a DS system using a spread ratio of 200:1 would have a processing gain of 10 log (200/1) = 23 dB. If this system requires a 5 dB signal-to-noise ratio before spreading, then a narrowband signal which is 18 dB stronger than the desired signal will jam the receiver. To express this approximately in terms of distance using simple free space propagation, the ratio of received signal levels is related to the ratio of their distances from the receiver by eq. 1.

$$\frac{S}{I}\,(\text{dB}) + 20 \log \frac{D_S}{D_I} \qquad (1)$$

S = the desired signal at distance D_S
I = the interfering signal at distance D_I

For an 18 dB S/I ratio the distance ratio turns out to be about 8:1. Thus for a desired signal 30 km away, a narrowband (or nonsynchronous PN modulated) interferer of equal power on a radius of 3.75 km or less, will jam the receiver. On the other hand, the tolerable near/far ratio for a properly designed hopping system is on the order

of 80 dB due to the fact that interference occurs only during actual frequency collisions on the same channel on a probabilistic basis. The available processing gain for a frequency hopper is calculated in an analogous manner to that for DS spreading, where the "spread ratio" is replaced by the number of channels in the hop set. If these channels are contiguous, then the AJ margin of the hopping system against a broadband noise jammer is equal to the processing gain, e.g. for 200 channels it would be 23 dB. But if the channels are spread across the 30-88 MHz band, the AJ margin may be higher since the broadband jammer's power cannot now be concentrated on only the hopping channels.

FREQUENCY HOPPING DESIGN PARAMETERS

System design parameters to be chosen include hop dwell time, transmit duty factor, hop rate (hops per second), number of information bits per hop, RF waveform, and synchronization method. Factors affecting choice of these parameters include: performance against the jamming threat, multiple-user performance (interference to other hoppers) and interference to non-hoppers.

Dwell Time, Duty Factor, Hop Rate

The dwell time, or the time the system is on frequency transmitting or receiving information can range from several seconds to a few microseconds on each available frequency, and is determined mainly by the threat. A CW jammer is easily evaded by hopping, even with fairly long dwell time. But if the threat is a broadband barrage jammer covering a large percentage of our hopping frequencies, then our digital bit error rate increases to more than the 10% threshold and we are no better off with hopping than with a fixed frequency, no matter what the hopping dwell time is. At the other extreme of jammer sophistication, the fast follower jammer, if built and deployed, can potentially sort out one of our nets from the general spectrum babble and follow it from frequency to frequency. To evade this follower jammer we must hop on and off a frequency quickly enough so that our dwell time is less than the sum of the jammer's response time plus its propagation path delays relative to the direct path. An example is shown in figure 1. Here the assumed response time of this sophisticated jammer is 100 μs and its distance from the transmitter is 20 km. The curves show how close to the transponder jammer the receiver can be and still be safe from its jamming signal. As it moves closer than this, the jammer signal overlaps an increasing portion of the hopper's dwell time. The three curves show that for longer hop dwell times, the receiver must be closer to the transmitter. If we assume a longer reaction time for the transponder jammer, a longer dwell time for the hopper is permissible.

The most critical part of a frequency-hopping radio in terms of hardware is the frequency synthesizer. Commonly available, low-cost designs can switch frequencies in a few milliseconds. These usually employ a single voltage-controlled oscillator (VCO) in a phase-locked loop with a programmable frequency divider, and are known as

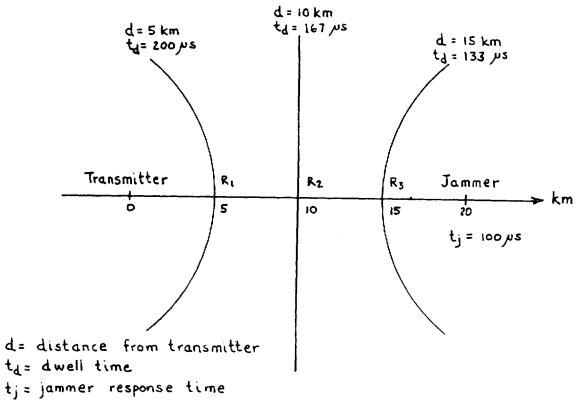

Figure 1 Permissible dwell time versus transmitter to receiver distance

"indirect" synthesizers. They can be made to serve nicely for a slow-hopping system at up to 100 or 200 hops per second. For fast-hopping radios a more complex design is required. "Direct" synthesis using banks of oscillators and filters with frequency combiners etc. will do the job but are too expensive and complex for the CNR application. Recent developments in multiple loop indirect synthesizers (compound versions of the simple single-loop indirect type) have produced fast-switching designs with acceptable spurious and noise outputs at a tolerable cost and power drain. The switching time is of the order of 100 microseconds. Whether a slow or fast system, the synthesizer switching time largely determines the off-time of the hop waveform. The permissible dwell time is determined by the jamming threat to be countered, as discussed above. Then (fig. 2) the dwell time, in turn, determines the number of information bits per hop that can be transmitted; the ratio of dwell time to frame time is the hop duty factor, and these factors determine the required hop rate and also the transmitted bit rate.

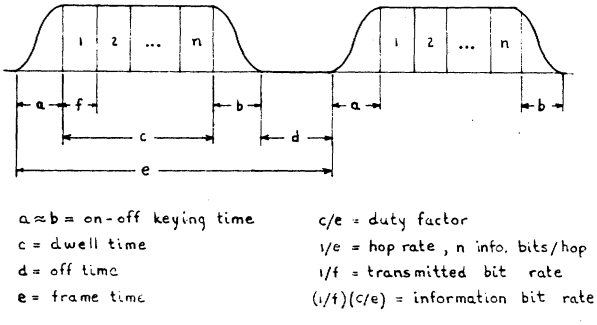

Figure 2 Transmitted Frequency Hopping Waveform

Modulation

There are two important criteria which determine the type of carrier modulation: 1) the ability to operate in a single channel mode to provide interoperability with existing radios,

and 2) the need to minimize adjacent channel interference. The requirement to interoperate is often in direct conflict with the requirement to provide improved performance. In this case the selection of a modulation scheme must provide compatibility with existing single channel radios, of either a 50 kHz or 25 kHz channelization, and be compatible with analog or 16 kb/s information. The issue of interoperability in the Army's case is satisfied by a binary FSK modulation scheme. Analog voice compatibility is generally no problem; however modulation index (i.e. deviation) must be considered since some degradation in signal to noise ratio will occur due to the discriminator characteristics of the older 50 kHz radios. The CNR baseline for digital signals is 16 kb/s data and the new generation CNR has been optimized for this. Again, interoperability with older radios presents a problem, since little or no provision is made in older radios for control of digital modulation index or premodulation filtering. It is clear that interoperability in the digital mode will be far from optimum. The new CNR is basically a digital radio and as such we must consider several factors for the given modulation technique: 1) transmission bit rate, 2) modulation index, 3) pre-modulation filtering, and 4) carrier on-off switching when frequency hopping. After selecting the modulation scheme and given the information bit rate as 16 kb/s, the transmission bit rate will determine what modulation index and pre-modulation filtering can be used to optimize bit error rate performance and minimize adjacent channel interference. A modulation index of 0.7 and a pre-modulation bandwidth to transmission bit rate ratio of 0.625 have generally been found to be near optimum values. Keeping adjacent channel performance in mind, CNR is required to confine 99% of its transmitted energy within the 25 kHz channel. When operating at less that 1000 hops/s it is possible to do this. Assuming a duty factor of 76%, the transmission bit rate would be 21 kb/s, and with the proper pre-modulation filtering, the 25 kHz criterion could be met. Once the hop rate increases beyond this, limitations in synthesizer switching times dictate a decrease in the duty factor which causes a corresponding increase in transmission bit rate. In addition to pre-modulation filtering, consideration must be given to the pulsing on and off of the RF carrier when switching between frequencies. This pulsing of the carrier is an additional modulation effect causing what is termed as hop splatter. Hop splatter is due to the shape of the pulse envelope as well as the duration (period). As the hop rate increases, and the duty factor decreases due to limitations of the synthesizer, there is a temptation to speed up the pulse rise and fall time (on-off keying time in figure 2) thus easing the switching requirements of the synthesizer. However there is an adjacent channel performance penalty for doing this. To calculate the effects of hop splatter, the Fourier integral of the pulse envelope is computed and then the energy spectral density function can be determined.

As an example of how these interrelated factors impact adjacent channel performance, consider

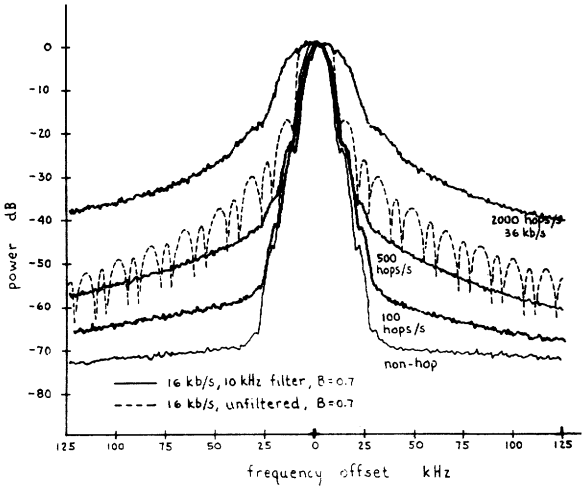

Figure 3 Power spectra of different hop waveforms

figure 3. These curves illustrate the effect of hop splatter. A non-hop 16 kb/s spectrum is shown with and without pre-modulation filtering compared to hopped spectra at 100, 500, and 2000 hops/s. The modulation is 16 kb/s binary FM with a modulation index of 0.7 and a pre-modulation filter 3 dB bandwidth of 10 kHz. The curves were generated by RF switching with no envelope shaping, and as such are typical of worst case situations. The 100 and 500 hops/s curves were pulsed with an 80% duty factor and show a significant increase in energy beyond the first adjacent channel. The curve for 2000 hops/s typifies the effects of fast frequency hopping. In this case the transmitted data rate was increased to 36 kb/s with the same modulation index and data rate/filter BW ratio as in the slow cases. The higher data rate is required because the duty factor is assumed decreased to approximately 45%. Again, there is a marked increase in sideband energy beyond the first adjacent channel. In order to control hop splatter some shaping or filtering of the on-off control pulse in the transmitter must be provided and, as shown, as the hop rate increases and the duty factor decreases, the necessity for control pulse shaping becomes increasingly important.

Hop Synchronization

To permit communication among the radios in a net, all radios must hop synchronously onto the same frequency at the same time. To facilitate this, each radio is furnished with certain parameters which can be changed periodically. These include the actual frequencies comprising the "hopset", the "net identifier" (which generates a code determining the sequence in which the hop frequencies will be used) and the time of day (TOD). The hopset and the net ID are stored in memory. TOD is a digital representation of actual clock time which is transferred to the independent crystal-controlled clock in each radio so that each receiver knows approximately where in the pseudorandom hop sequence the transmission is to be found. However, because of unavoidable error in timekeeping accuracy due to clock drift, the receiver may still be several hops ahead of or

behind the transmitter at the start of a message; thus a means of exact synchronization must be provided. The selection and implementation of one synchronization scheme over another is largely dependent on the hop duty factor. There are other criteria which need to be met by the synchronization scheme.

Non-Unique RF Signature. Any type of unique waveform for synchronization is undesirable from a vulnerability standpoint. The synchronization waveform must not be easily distinguishable from that of the message.

High Probability of Sync. The correlation threshold must be low enough to operate at or near 10% BER, but high enough to prevent false sync (false alarm) on noise or spoofing signals. The longer the synchronization code, the less likely false sync will be, however it will require a longer time-to-sync. False synchronization will temporarily tie up the receiver's sync processing circuitry and until defaulted or reset could prevent a true synchronization transmission from being detected.

Short synchronization time. For a CNR push-to-talk system, short sync times are needed so the message is not delayed. Short times usually imply short sync codes. It is undesirable from the operator's standpoint to have a perceptible delay after keying the handset before he can start talking. Most synchronization techniques perform asynchronous, multiple correlations with a predetermined synchronization code. To satisfy the above criterion the codes need to be short enough to be transmitted only over a few hops; have good autocorrelation and crosscorrelation properties; and be transmitted at a bit rate equivalent to the transmission bit rate.

For a given net, the net ID sequence is permuted with a non-linear key sequence (the TRANSEC variable). This new sequence defines the frequency pattern in a virtually non-deterministic way. Thus the receiver waiting to synchronize knows which frequencies will be used, but without the same precise time reference as the transmitter, does not know exactly when these frequencies will be used (if accurate universal time distribution and tracking were available this would not be a problem). One technique is to have the receiver scan the hop set frequencies at a slow rate (relative to the actual system hop rate) and wait for the transmitter to overrun a monitor frequency or group of frequencies to be used during synchronization. At each frequency scanned by the receiver, multiple correlations are continually performed until the synchronization code is detected and the number of agreements exceeds the sync threshold. The skill in designing frequency hopping synchronization systems lies in reducing the time uncertainty in the receiver, and at the same time not relying on extremely precise crystal oscillators, which are expensive and bulky, or over-simplifying the search procedure which would tend to make the system vulnerable to jamming or spoofing.

The sync search process can be broken up into coarse and fine processes. The coarse synchronization search may result in only a partial correlation due to code length or the degree of transmitter and receiver time offset. The coarse sync information will narrow down the time uncertainty but not enough for full hop synchronization; the receiver will use this information to know when and where to monitor for complete synchronization. When the offsets in time between the receiver and transmitter exceed the normal operating parameters, the system may need to be placed in a late entry mode which would extend the time to sync by several orders of magnitude. This would be a special case and not within the capabilities of normal push-to-talk operation.

Another consideration is whether a block sync (message sync) or continuous sync (hop by hop) format is used. In block sync, the hop synchronization is performed only at the beginning of the message and the receiver clock stability must maintain hop sync until another transmission is made. A continuous sync system will send sync information on a hop by hop basis or at certain periods during a transmission thus allowing resync during a message transmission but also requiring more overhead bits devoted to sync time keeping. Whatever the specific design of the hop synchronization circuitry, one thing is certain; the complexity and costs associated with it tend to reflect into all other parameters of the frequency hopping system. A simple but effective synchronization design eases timing considerations throughout the system.

DESIGN EFFECTIVENESS: MULTIPLE USER PERFORMANCE

Because of the large number of radios on the battlefield, frequency hopping will result in some degree of self-interference due to "collisions" whenever two nets randomly hop onto the same frequency, or onto the frequency of a non-hopper. Self-interference between hoppers can be minimized if all the hop sequences are arranged to be orthogonal and if all nets change frequency synchronously. This would avoid direct collisions on the same frequency (but not on adjacent channels, hence the need for minimizing hop splatter). But the "top-down" coordinated distribution of time required for synchronous net operation may not prove operationally practical under all battlefield conditions; therefore we must assume asynchronous hopping at present.

To analyze multiple user performance we can relate number of users, AJ margin and near/far ratio. Figure 4 shows typical curves based on uniform distribution of hopping radios over a circular geographical area, the desired-signal receiver being at the center. The curves show that as the number of users increases, the AJ margin decreases because the tolerable interference at the receiver (a mix of friendly interferences and enemy jamming) is increasingly being supplied by the friendly interferers, leaving less margin against the jammer. Once detailed hopping system parameters are known, the multiple user performance is analyzed using a validated tactical deployment model rather than this simplistic uniform distribution of users.

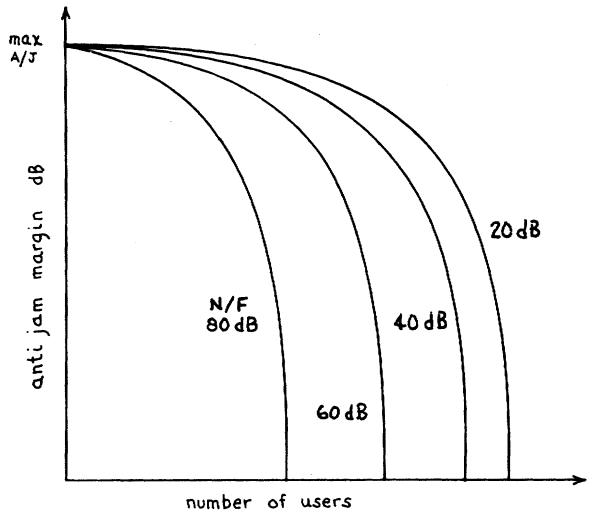

Figure 4 A/J margin as a function of number of users for broadband jamming

CONCLUSION

This paper provides an overview of system design considerations for FH CNR. It is clear that of the various design parameters that are discussed, there are primarily two opposing forces which drive the selection of these parameters; the electronic warfare threat and electromagnetic compatibility (EMC) with other users (this includes spectrum sharing with existing non-hopped systems and the need to maximize the number of FH users in a given region). Designing the system using only the EW threat as the driver can result in a very fast hop design that will have poor electromagnetic compatibility performance. On the other hand, reducing the system parameters to achieve good EMC performance may make the system unusable when attacked by a relatively unsophisticated jammer. Since it is imperative to maximize the system's multiple user performance, the definition of the threat that system designers are required to live with will then place bounds on all other parameters.

The Army is currently developing a CNR FH system called SINCGARS-V (single channel ground and airborne subsystem-VHF) which will complete development by the end of 1982. During the course of the system development all of the considerations outlined here plus many others have been carefully weighed and arduous decisions made to determine the proper balance point between threat and EMC. Very soon the results of these decisions and designs can be tested and verified.