What Is SECURENET?

Introduction

Before we can begin our discussion of SECURENET equipment and systems, we must cover some ground work. We are going to begin with the basic building blocks of SECURENET. If you are already familiar with. these concepts, then use this lecture and information for a review. If not, then use them as a necessary learning tool.

Definition / Process

SECURENET is the most sophisticated digital voice encryption technique commercially available. The units that do the actual scrambling and unscrambling are configured to transmit and receive voice messages in either clear or coded mode, sometimes referred to as a dual-mode system.

The process of making a voice signal encrypted is accomplished in several stages or operations. The first operation is to convert the analog audio to a digital signal. This is accomplished by a Continuously Variable Sloped Delta Modulator, more commonly referred to as a CVSD modulator, running at a 12 KHz clock rate. This in turn gives a digital signal output at a 12 kilobit per second rate.

Once the signal is in a digital format, the signal is then encoded or encrypted into a “scrambled” digital signal. This output signal has a pseudo-random digital sequence. This means it has the characteristics of a random signal, but it also has a mathematical structure to it for proper decoding at the receiving end. This process of encrypting the signal uses a multi-register, non-linear combiner algorithm set by a digital code or key.

After the signal is encrypted, it is filtered by a low pass filter to remove high frequency harmonics. The filtered, scrambled signal is then applied to either a modulator, for RF transmission, or a wireline, to be sent to a transmitter. If applied to a modulator the deviation should be adjusted to ±4 Khz.

On the receive side the scrambled signal is recovered from the carrier by the discriminator, like clear audio; or it is received down the wireline from a receiver. It is then applied to the circuitry for decoding.

The first step uses the received signal to synchronize the free-running 12 KHz clock. This operation is accomplished by the clock recovery circuit. Once the clock is synchronized, the “scrambled” signal goes through an amplifier/limiter circuit to reshape it into a squared 12 kilobit per second data stream. Note that the signal is still scrambled upon the completion of this step, and the reshaped signal should resemble the one that left the encoder in the transmitter.

Next the “scrambled” digital signal is sent to the circuits where decoding is performed. If the decoding circuit algorithms were set up with the same key as the encoding circuit, the output will be an “unscrambled” 12 kilobit per second digital signal. If the transmitter used a different key than the receiver, then the output will be a corrupted 12 kilobit signal that sounds like noise and is unusable.

The last step that’s needed to be done is to convert the 12 kilobit per second digital signal into analog audio. This process requires a CVSD demodulator, the CVSD demodulator in the receiver is configured to operate exactly in reverse compared to the CVSD modulator in the transmitter.

These are only a few facts of SECURENET and how it works. We will now go into greater detail of the “scrambling” process including how the CVSD and encryption circuits work. On the receive side, we will learn how the “descrambling” process takes place including clock synchronization and code detection.

Transmit Secure Signal Flow

Introduction

We are now going to discuss the process of converting audio to and from a coded signal. Once we get done with this section, you should be able to take the knowledge gained and apply it to any SECURENET circuit, whether it is a CIU, portable or mobile radio.

First we are going to discuss what happens through the circuitry during transmit. We will talk about what happens with circuit operation when transmitted coded and clear. Refer to ***Figure*** I.

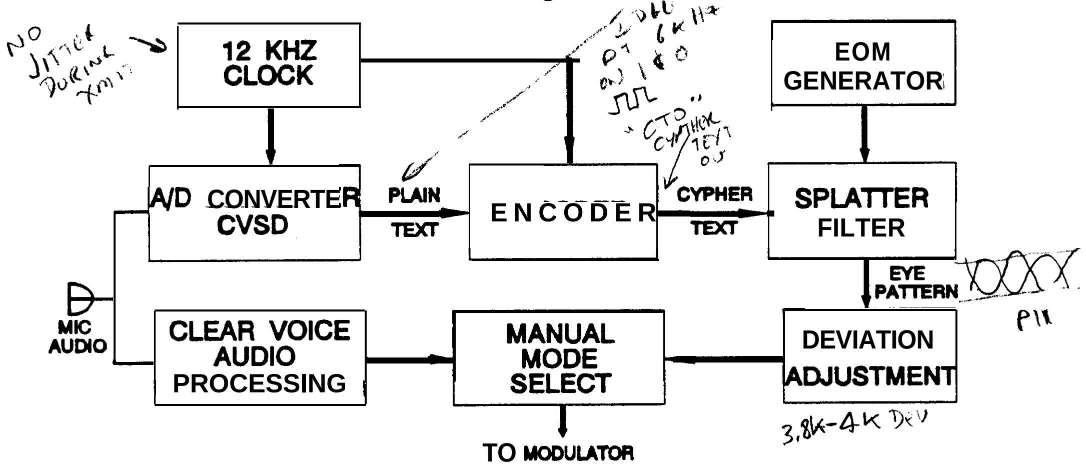


Fig. 1: TRANSMIT SIGNAL FLOW

Coded/Clear Mode Selection

The operator must select how he wants to transmit, clear or coded. For argument's sake we will say that the operator chooses to transmit a coded signal. Once the selection has been made, the operator hits the Push-To-Talk **(PTT)** button. This will automatically switch the secure circuitry output to the modulator and disable the clear processing circuit's output from going to the modulator. If the operator wants to transmit in the clear, he will select to transmit clear and depresses the PIT button. This time, however, the manual mode select block routes audio from the clear processing circuit to the modulator and disables the secure circuitry output to the modulator. The clear audio goes directly from the microphone to the modulator. The clear audio is still going to the secure circuitry, but the switch disables the output.

12 KHz Clock

This block is used to develop a 12 KHz clock that is used for timing, conversion processes and synchronization of the secure circuitry. The reason for using a frequency of 12 **KHz** is due to the analog to digital conversion process of the voice. This conversion process will be discussed later. During transmit the 12 **KHz** clock will be locked, which provides for a stable clock.

CVSD

The clear analog audio is going to be applied to the Continuously Variable Slope Delta (CVSD) modulator. The function of the CVSD modulator is to convert the analog audio to a digital signal.

In the SECURENET system, before the voice message can be encoded it must be converted into a digital format. This digital signal output from the CVSD modulator is referred to as plain text. Plain means the signal is still clear, and text means the signal is in a digital format. Likewise, at the receiver, after being decoded, the digital signal must be converted back into an analog voice format. These functions of analog-to-digital and **digital-to-**analog conversion are accomplished by the CVSD modulator/demodulator.

The CVSD modulation technique has been chosen for the SECURENET system because of several desirable system characteristics. It provides the best possible voice quality for the 12 **kilobit** rate used. Even though such a low bit rate is used, high intelligibility and good voice recognition are provided. The serial digital output requires no frame synchronization; synchronization of transmit and receive clocks is all that is needed. In addition, CVSD operation provides a **companding** feature which makes the “talker-to-microphone” distances less critical. Finally, there is good tolerance to errors in the transmission path, and no adjustments are required for proper operation.

In order to understand CVSD operation, it will help to have an understanding of Delta Modulation. Many of the principles of CVSD operation can be illustrated by first examining the basic Delta Modulator.

“Delta” means difference. When sampling voice signals there are some inherent qualities that we can take advantage of. Never will the amplitude of a voice signal be quiescent from one sample period to another; meaning that the amplitude will continuously be either increasing or decreasing. In delta modulation we will encode the difference in amplitude by generating “l’s” or “0’s”.

The delta modulator, ***Figure*** 2, is basically a loop device which operates by comparing the magnitude of the analog input signal at a specific point in time with its magnitude at the previous sample time by means of an integrated feedback signal. This feedback signal is subtracted from the input audio. This difference signal is then converted into digital form by the limiter. The output of the limiter is a digital “1” if the input audio is greater than the reconstructed audio and a digital **"0"** if the reverse is true. Obviously this is a comparison from the last voice sample.

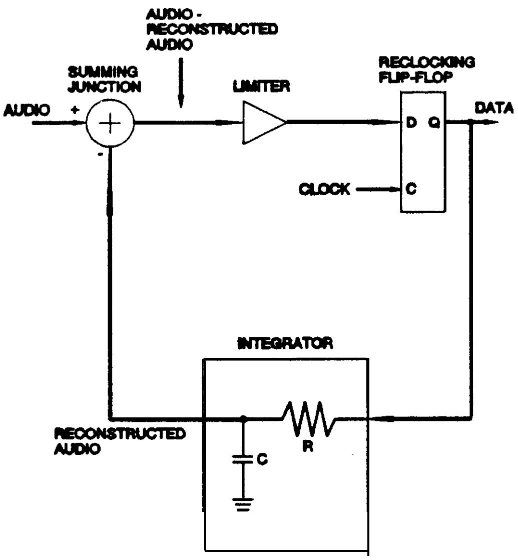


Fig. 2: DELTA MODULATION

In Delta Modulation, only the direction of the change is transmitted and not how much of a change; therefore, the sampling rate has to be higher. The sampling rate should be 8 times the highest expected frequency to be digitized. The typical voice bandpass is up to 4 KHz, meaning that we would be sampling at a 32 KHz rate. To sample at this speed would give us a comparable signal quality to that of the average telephone. There's a problem with this rate of sampling though. If you look at the output data rate of this technique, using a 32 KHz sample rate, it would be at 32 kilobits per second. 32 kilobits per second would correlate to a highest fundamental frequency of 16 KHz.

That's 16 KHz before you even send it to a FM modulator to transmit over the air. TOO much bandwidth...so what can we do to conserve bandwidth, and still maintain an adequate voice quality? We'll answer this question later.

If there is no audio input signal, the delta modulator will produce an output called "idle pattern". Here, at a particular clock sampling time, the integrator will be above the input and thus the reclocking flip-flop output will be a "0" thereby causing the integrator to discharge. At the next clock time, the integrator will have discharged so that it is below the input making the flip-flop output a "1" which will cause the integrator to charge. This process will continue until a voice signal occurs. The reconstructed audio will be a triangle wave and the digital output will be a squarewave both with a repetition frequency of 1/2 the clocking frequency. In the SECURENET system, the idle pattern frequency is therefore 6 KHz due to a 12 KHz clock. The digital difference signal is then synchronized to the clock by passing it through a reclocking, type D flip-flop. The output of this flip-flop is a digital, synchronized representation of the difference, or error, signal. It is this digital signal that is to be encoded.

The fact that the reconstructed audio can only change its slope at discrete times and is limited to a choice of 2 slopes, one positive and one negative, means that the integrator output has been "quantized". The integrator can not perfectly follow the input audio; this gives rise to a noiselike signal called "quantizing noise". It can be reduced by increasing the sampling rate or by providing more than 2 choices for the slopes.

A second important case to examine is called "slope overload". Here the input, a sine wave for example, is of such an amplitude and frequency that the reconstructed audio, since it can only change with a constant slope, cannot rise fast enough to track the input signal. The result is that the reconstructed audio is no longer a good estimate of the input and severe distortion results. In this case, the distortion is evidenced by the amplitude of the reconstructed signal being reduced.

Considering again a sine wave as the audio input, the fact that the input frequency is not synchronized to the clock frequency can cause dynamic amplitude variations called 'beats." For input frequencies at integer sub-multiples of the sampling clock, beats will not occur. This effect can be heard by sweeping the input signal and listening to the integrator output. In addition to the input frequency, a background tone will be heard that increases in frequency then decreases to a very low frequency at a clock sub-multiple, and then increases, etc. Since beats are only heard when the input signal is tone-like and cannot be heard with a complex signal such as voice, they usually are not a serious system problem.

Summarizing the above, there are 3 types of distortion to contend with in a simple delta modulator: 1) quantizing noise, 2) slope-overload, and 3) beats. Not much can be done to eliminate beats, but by adding additional circuitry to a delta modulator, the distortion caused by slope overload and quantizing noise can be reduced. It was improved performance in these areas that led to the selection of CVSD modulation for use in the SECURENET system.

The main problem with the basic delta modulator is that there are only 2 choices for the integrator slope. If, when a large input is present, the slope could be increased to track this signal, slope-overload characteristics could be improved. By changing the slope to try to better match the input signal, the quantizing noise can also be reduced since the quantizing choices of the demodulator are increased.

The signal required to control the variable slope can be formed by monitoring the digital output of the delta modulator. If the output remains in one state for several sampling periods, this is an indication that the delta modulator could be in slope-overload. By increasing the integrator slope gradually until there is no longer a given amount of consecutive "l's" or "O's", it can be assured that the delta modulator will track the envelope of the input signal and not the instantaneous signal variations.

The gradual increase or decrease of the integrator slope is why this form of delta modulation is called “continuously variable slope delta” modulation. Refer to ***Figure*** 3.

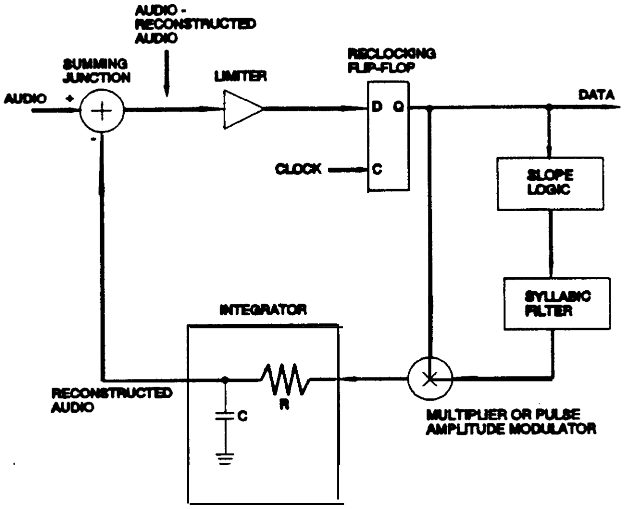


Fig. 3: CVSD DIAGRAM

This gradual change in the slope control signal can be generated by filtering the output of a consecutive “1” or "0" detector with a single section RC lowpass filter with an appropriate cutoff frequency. By using the output of this slope control filter to vary the amplitude of the digital signal applied to the integrator, the slope of the integrator output will vary directly with the slope control signal.

The variable slope filter shown in the block diagram is labeled a “syllabic filter” because its cutoff frequency is set at 50 Hz to track the variations in envelope amplitude as the various syllables of a word are spoken.

What this correlates to is a lower sample rate for the same voice quality. The sample rate required to obtain the voice quality of a typical telephone is 16 KHz. In SECURENET we have settled for slightly less than this in order to further conserve bandwidth. The sample frequency utilized in our CVSD process is 12 KHz. This computes to a data rate of 12 kilobits per second, and a highest fundamental frequency of 6 KHz.

In Figure 4, the CVSD and delta modulator's integrator outputs are compared for a typical audio input. Note how the CVSD is able to reach the input more quickly than the delta modulator and then is able to provide more detail in the region just after the peak.

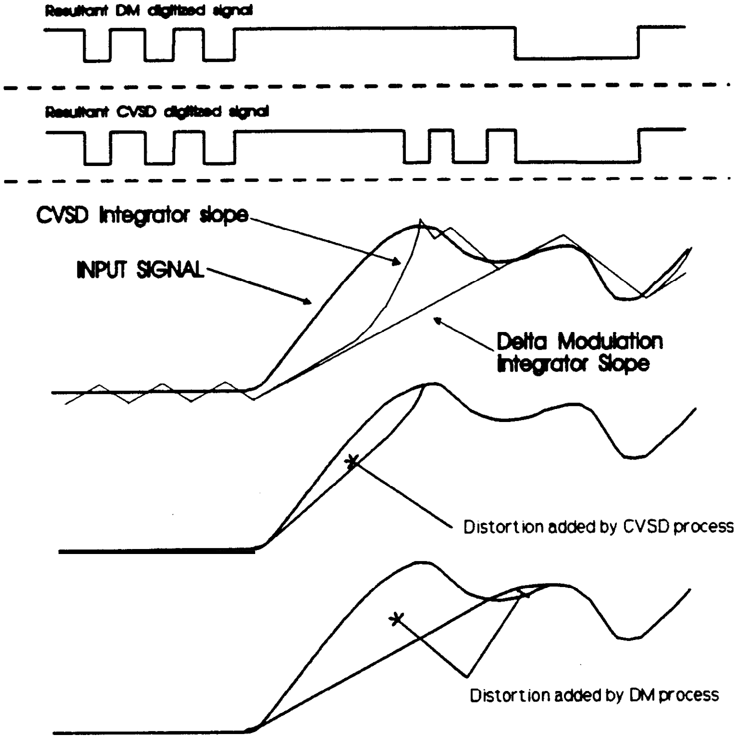

Resultant DM digitized signal
Resultant CVSD digitized signal
CVSD Integrator slope
INPUT SIGNAL
Delta Modulation Integrator Slope
Distortion added by CVSD process
Distortion added by DM process

Fig. 4: WAVEFORM COMPARISONS

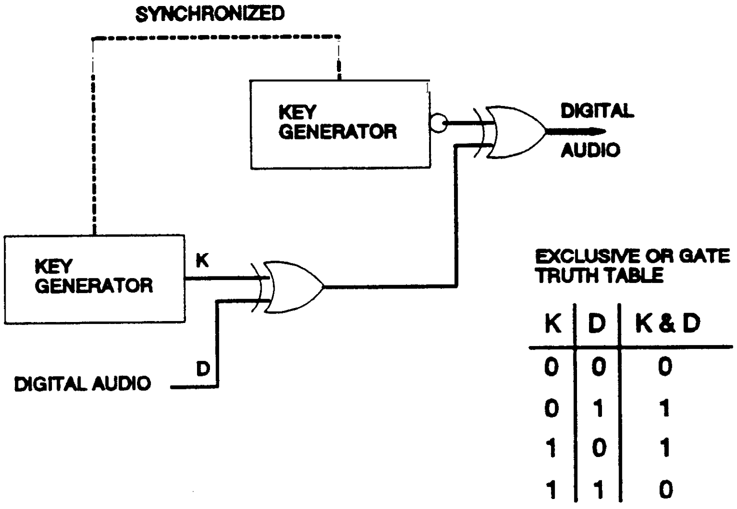
Encryption Fundamentals

The next step is to take the digital signal (plain text) produced by the **CVSD** and encode it. The following explanation will be simplified to give you a general idea of the process that takes place inside the encryption hybrid. Remember this is only an example and isn't the exact process that takes place.

The encoder/decoder used in the SECURENET system is a proprietary coding device which uses a multi-register non-linear combiner algorithm. An additional property of the encoding algorithm is that the encoded output is a pseudo-random digital sequence, which means that the SECURENET signal has the characteristics of a random (i.e. noise-like) signal, but it also has a mathematical structure to decode the message. To any listener, either with a clear radio or a SECURENET radio on the wrong code, the signal has a noise-like sound with no intelligibility.

Encoding is accomplished by adding a pseudo-random key pattern to the digitized audio output of the CVSD modulator. The key pattern is determined by the code key from the Key Variable Loader (KVL) code inserter, the coding algorithm, and past input data. For example, the process used here is modulo or base 2 addition.

Figure 5 shows a block diagram of an encoder with a truth table for the modulo 2 adder. The modulo 2 adder has the same truth table as a logic element called an "exclusive or" gate. At the decoder, the same key is subtracted from the encoded signal to yield the digital audio.



K	D	K & D
0	0	0
0	1	1
1	0	1
1	1	0

Fig. 5: ENCODER BLOCK

Again, the exact process of encryption/decryption used in SECURENET is proprietary, and even if we knew exactly what was done, it wouldn't really benefit us any in performing our jobs as technicians.

Splatter Filter and Eye Pattern Analysis

Once the signal has been encrypted by whatever mathematical processes, it is now referred to as cipher text. Cipher text means that the signal is encrypted and in a digital format. The next step is to process this digital signal, cipher text, through a SECURENET splatter filter. This is a different splatter filter that normal clear audio would be processed through.

The splatter filter is a low pass filter, where F_C = 6 **KHz,** to remove any unwanted high frequency energy from the signal before it is to be applied to the modulator. The output, when viewed on an oscilloscope, gives the appearance of an eye. Therefore, the signal is called an eye pattern, and by analyzing the eye pattern many things can be learned about system performance.

First let us look at how an eye pattern is developed for the presentation on an oscilloscope. The oscilloscope would be set to trigger at l/T, allowing the CRT to display together all signal waveforms and transitions. ***Figure* 6** demonstrates the development of an eye pattern.

The eye opening is an indication of system health. By examining an "original" eye pattern and comparing it to a current one you can determine if there is added timing jitter, noise, or amplitude distortion.

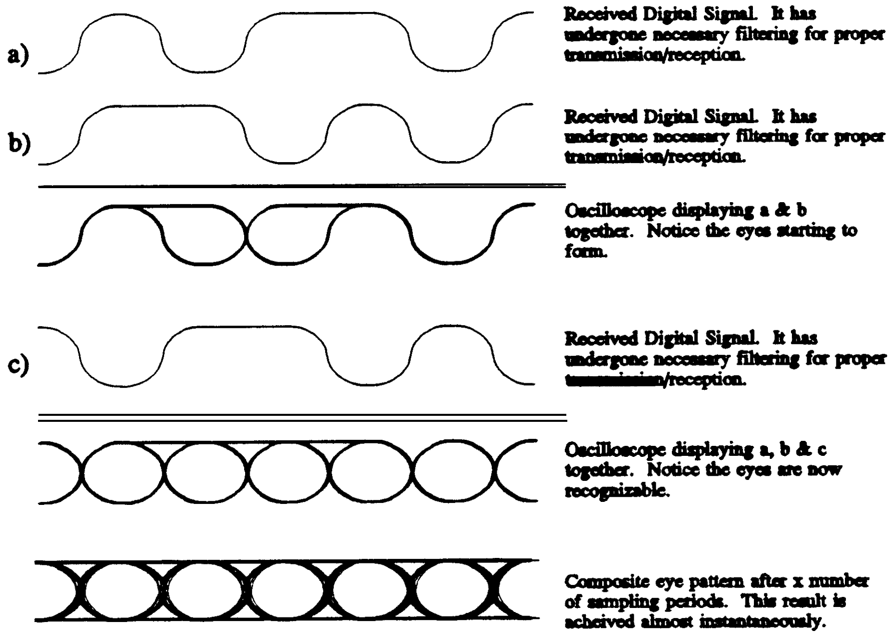

a)
Received Digital Signal. It has undergone necessary filtering for proper transmission/reception.
b)
Received Digital Signal. It has undergone necessary filtering for proper transmission/reception.
Oscilloscope displaying a & b together. Notice the eyes starting to form.
c)
Received Digital Signal. It has undergone necessary filtering for proper transmission/reception.
Oscilloscope displaying a, b & c together. Notice the eyes are now recognizable.
Composite eye pattern after x number of sampling periods. This result is acheived almost instantaneously.

Fig. 6: EYE PATTERN DEVELOPMENT

Notice, in the composite eye pattern that the transition points are exact (pin-points). Due to the self-synchronizing format that SECURENET uses, these pin-points will probably not be achievable. Because of this it is even more important to have a “reference” eye pattern to compare measured eye pattern waveforms against.

Now let’s examine some different eye pattern waveforms that are distorted for one reason or another. By analyzing these eye patterns and determining the types of problems that can cause them to distort, you can learn a lot about your system and its optimization.

Analyzing the right eye pattern in ***Figure*** 7, we can see that the signal’s “eye” has closed vertically. This indicates that the transmission medium has added amplitude distortion. In this case the amplitude has been attenuated. When this is discovered it would indicate that line-loss tests should be performed in order to determine if the line still meets established specifications.

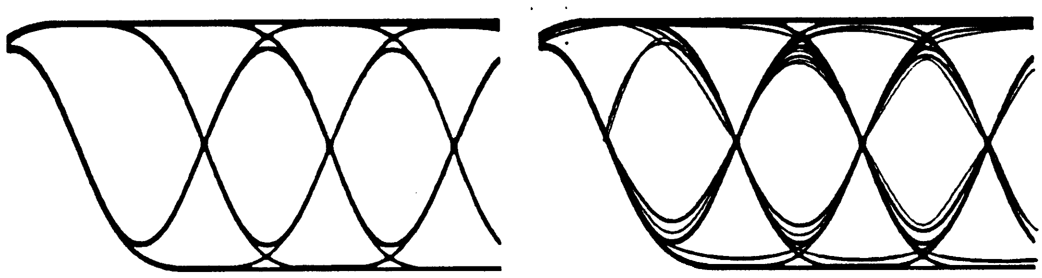


Fig. 7: EYE PATTERN WITH AMPLITUDE DISTORTION

In ***Figure*** 8, notice that the right "eye" in has closed horizontally. This is an indication that there may be timing jitter distortion problems. Once this has been identified you may want to do a jitter unit interval test to determine if the transmission medium being used still meets specifications.

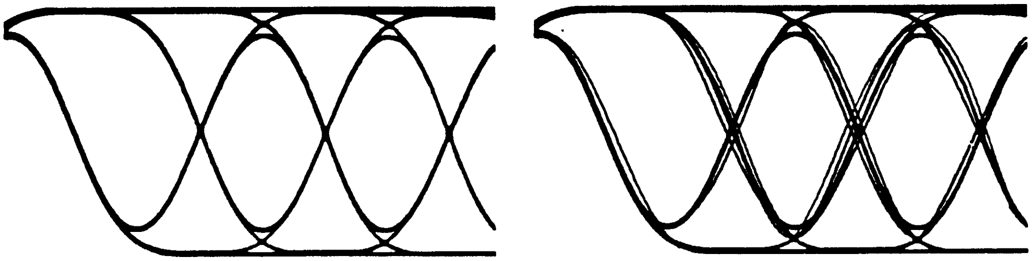


Fig. 8: EYE PATTERN WITH PHASE DISTORTION/JITTER

Comparing the patterns in ***Figure*** 9, notice that the right signal, as compared to the eye on the left, appears to be "fuzzy". This would indicate noise problems, and gives an indication of both amplitude and phase distortion. This type of problem could render that link inoperable. A high-noise level would necessitate investigation of all end-to-end equipment. Checks to perform may include Idle-Channel-Noise (ICN), Noise-Power-Ratio (NPR), and grounding.

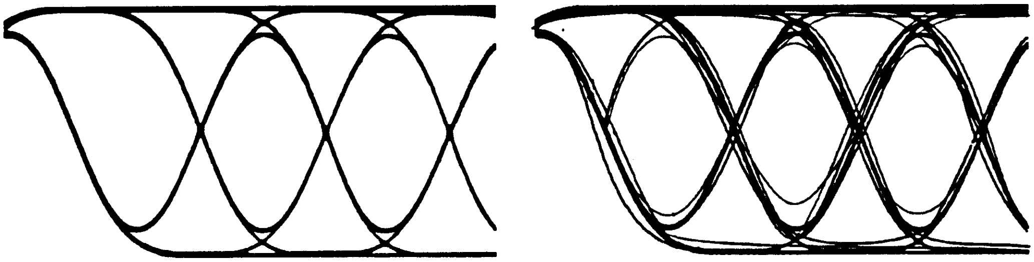


Fig. 9: EYE PATTERN WITH NOISE

All the forementioned situations could render that link/channel inoperable; they could also cause an increased bit error rate to occur.

Deviation Adjustment

The next step which occurs during transmit time is that the coded signal's deviation is set prior to being applied to the modulator, if in an RF transmitting unit. Like the splatter filter circuit, there is a separate deviation adjustment for the coded signal and the clear signal. The deviation level of the coded signal should be set to ±4 KHz, or as close to it as possible. If the deviation level isn't set properly, a degradation of your system may occur. If the splatter filter is in a CIU, then there is no deviation adjustment. The signal is level adjusted and applied to the line outputs.

EOM

Lastly, as long as there is a **PTT,** an eye pattern will be developed and transmitted. Once the P'IT is released, the End Of Message (EOM) generation circuit develops an EOM. This is a 6 **KHz** clear sine wave burst at the end of transmission and will be discussed in more detail when covering the receive circuitry.

Transmit Clear Signal Flow

Process

If the operator doesn't choose to transmit in the coded mode, then all this discussion is for naught. Referring back to ***Figure 1, you can see*** that clear audio will effectively bypass the SECURENET circuitry and go through clear processing circuits which consists partly of a separate splatter filter and deviation adjustment. From there it is routed through the manual mode select switch and applied to the modulator or wirelines.

Receive Coded Signal Flow

Introduction

Now let's see what happens during receive time of a secure capable unit. For this discussion refer to ***Figure 10***, a basic block diagram of the receive path signal flow.

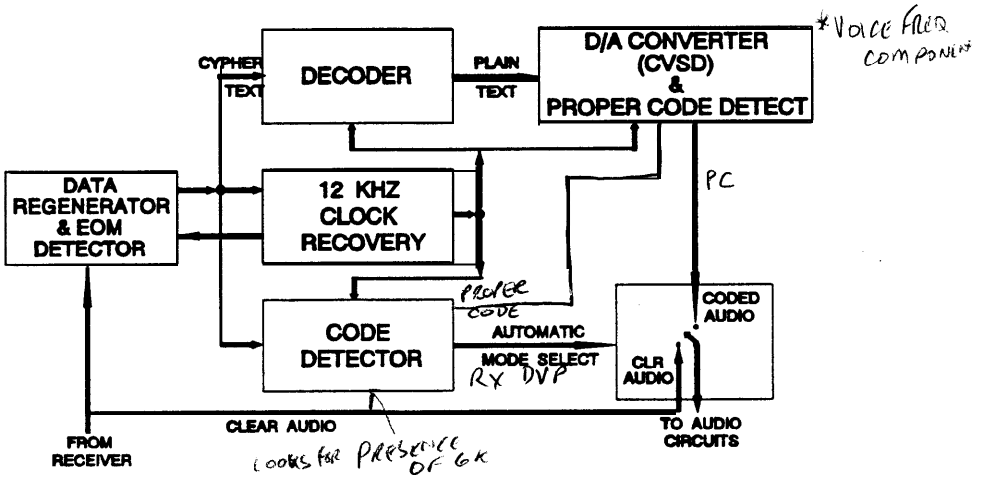


Fig. 10: RECEIVE SIGNAL FLOW

Coded/Clear Mode Selection

The first thing that needs to be mentioned is the fact that during receive time, the radio will automatically determine whether the signal being received is coded or clear. Once this is accomplished, the radio will automatically enable the proper processing circuits and disable the other circuits. Therefore, unlike during transmit time, receiving coded or clear is all automatic as far as the operator is concerned.

Assume that a coded signal is being received. Let's see how the signal is processed to give audio that can be heard and understood at the speaker.

Data Regeneration

Whatever type of signal is being received, be it clear or coded, it is going to be processed by the data regenerator circuit. This is effectively a limiter to convert the discriminator signal, which is an analog signal, to a digital format. Here, the zero crossing line is used as a reference - it is found by low pass filtering the discriminator output with a cutoff frequency of 10 Hz. If the discriminator output is above the reference, the limiter output is "1"; and if it is below the reference, "0" is the output. Again if clear audio is being received, it will still be applied to the circuit. Thus we have a digital signal applied to the next stage which is the clock recovery circuit.

12 KHz Clock Recovery

This circuit is going to synchronize its 12 **KHz** clock to the incoming signal so that the its clock is synchronized to the transmitting unit's clock. Although the algorithm used by the decoder is self-synchronizing for recovery of the key, it does require that the receive clock be synchronized to the transmit clock. It is the function of the clock recovery circuitry to do this, and in a manner such that the data can be recovered with minimum error. The clock recovery circuit must not only synchronize to the transmit clock, but it must have the proper phase relationship with the discriminator output. In the SECURENET system, these requirements are handled by using a digital Phase Lock Loop (PLL).

The digital phase lock algorithm uses the data transitions from the limiter to sample the recovered clock. Using the desired phase relationship between limiter output and recovered clock, the following rules can be formed. If the data transition occurs when the recovered clock is high, the clock is running slow and should be speeded up. If the data transition occurs when the clock is low, the clock is running fast and should be slowed. If no data transitions occur, the clock is allowed to run at the nominal frequency - 12 **KHz.** The action of these rules is to have the receive clock position its negative going edge on the data transitions. The pseudo-random nature of the encoded signal guarantees that there will be many data edges, thus providing many opportunities to correct the receive clock. With the above rules, there can never be a point at which corrections are not made (at a data transition); this means the receive clock will jitter about the correct value of clock phase. This jitter is minimized by using small increments to speed and slow the clock.

Once the clock has been adjusted, it is applied to the rest of the circuitry used for decoding the signal. In effect, all the SECURENET circuits on the receiving unit are synchronized to the transmitting unit so proper decoding can now take place.

Code Detection

The next step is to determine whether the signal being received is clear or coded. This process takes place in the code detect block. An important operational feature of the SECURENET system is its ability to automatically determine whether a received message is in the clear or coded voice mode. All receivers in the SECURENET system have this feature.

This automatic coded/clear receive operation is made possible because of two properties of the SECURENET signal that differentiates it from clear voice, silent carrier or receiver noise: 1) the SECURENET signal is pseudo-random and contains a significant number of “101” and "010" data sequences; and 2) the SECURENET signal always has level transitions that occur in some fixed time relationship to one another as determined by the clock, i.e. the data transitions are spaced apart by integer multiples of the clock period. Each of these conditions is necessary, but alone neither is sufficient to identify a coded message.

A block diagram of the code detector is shown in ***Figure II. The*** first property given above is looked for by the 6 KHz detector; the output of this detector is a pulse whenever the "101" or "010" pattern is present in the limited data. As long as one of these patterns is detected in a given time interval, the output of the 6 KHz counter is a logic **"1",** allowing the dropout counter to count. After this continues for a sufficient number of such intervals, the dropout counter reaches its maximum count and latches. If it happens that the **"101"** or "010" pattern is not detected in any interval, the dropout counter is reset and the audio gate is placed in the clear mode. If the proper pattern returns, the entire cycle must be completed before the 6 **KHz** dropout counter latches with a logic **"1"** output. Two input signals will satisfy the condition for this counter, noise and the SECURENET signal.

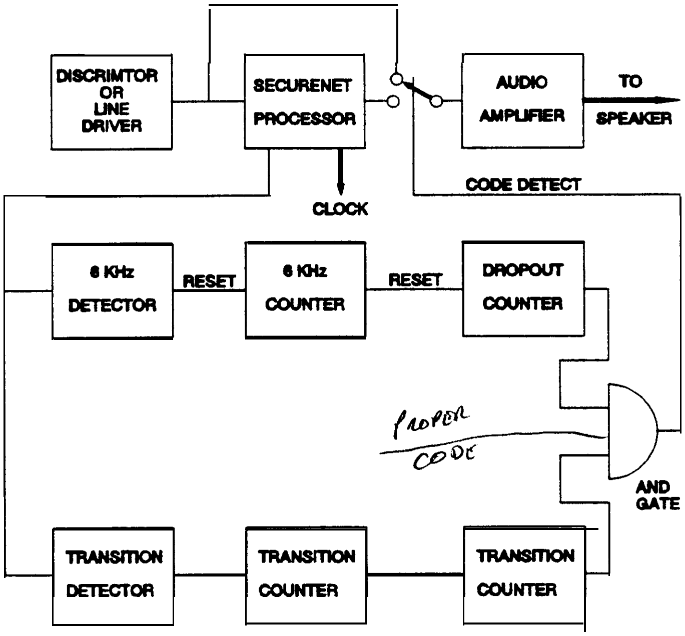
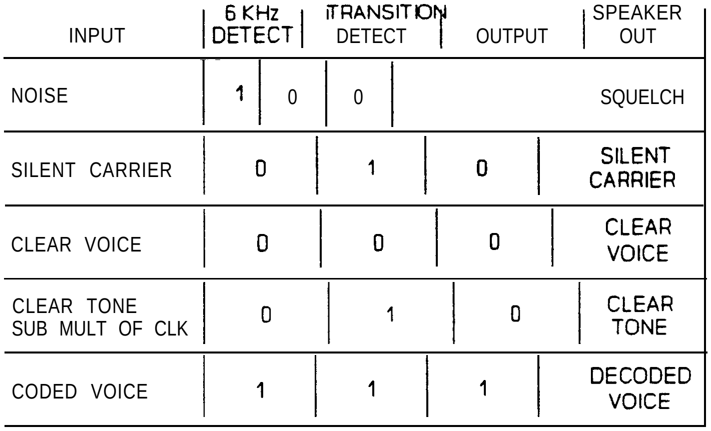


Fig. 11: CODE DETECTOR BLOCK

The second property is implemented with the transition detector. Here a window detection scheme is used to watch for transitions synchronized to the recovered clock. As long as no transitions fall outside this window in a given interval, the output of the transition counter is a logic **"1".** This is the condition that will occur for either a SECURENET signal or if the clock is locked to a sub multiple of the clock frequency. The circuit is an indicator of the receive clock being locked to the input signal.

The outputs of the two detectors are applied to a logic "AND" gate to give the code detect output. ***Table 1 gives*** the state from the code detector circuit for various input signal conditions. Once the code detector determines the type of received signal, control signals will be generated to route that signal. For any signal other than secure, the automatic mode select will bypass the secure circuitry and route the signal to the clear processing path.



INPUT	6 KHz DETECT	TRANSITION DETECT	OUTPUT	SPEAKER OUT
NOISE	1	0	0	SQUELCH
SILENT CARRIER	0	1	0	SILENT CARRIER
CLEAR VOICE	0	0	0	CLEAR VOICE
CLEAR TONE SUB MULT OF CLK	0	1	0	CLEAR TONE
CODED VOICE	1	1	1	DECODED VOICE

Table 1: CODE DETECT TABLE

Decryption Fundamentals

For a coded signal, the next step of the processing to be mentioned is to take the signal, now in cipher text format, to the decoder hybrid. The decoder, now properly synchronized will do the exact opposite process that took place in the transmitting unit. If the decoder hybrid was loaded with a different key as the encoder hybrid in the transmitting unit, the output from the hybrid will, effectively, be noise. However, if the decoder hybrid was loaded with the same key as the encoder hybrid, the output will be a signal referred to as plain text.

CVSD

Once the clear signal is recovered from the decoder hybrid, the next process is to convert the data signal to an analog signal. This uses a CVSD demodulator, which does the exact opposite process discussed in the CVSD modulator of the transmit section. With plain text input to the CVSD demodulator, the output will be the decoded analog audio. Since the code detector block already determined the signal was coded, the automatic mode select switched to the coded audio path to route the decode audio to the speaker.

Another function of the CVSD circuit during receive is to perform the operation of “proper code detect.” Internal to the CVSD circuit there is another correlation counter. This counter is looking for plain text. Of course, the only way the CVSD will receive plain text is if the same key was loaded in the encoder and decoder hybrids. If the keys were different, the output from the decoder is noise. The proper code detector evaluates the signal to determine whether it resembles noise. If the signal does resemble noise, a low correlation count will be achieved, and this causes the speaker to stay muted. However, if the signal doesn’t resemble noise, plain text, a high correlation count is achieved, and the speaker is unmuted. Proper code detect in a secure radio operates on the same principle as Private Line (PL) or Digital Private Line (DPL) in a standard radio. The speaker will not be unmuted until the proper signal is received.

Now the operator finally hears audio on the speaker. He didn’t have to physically do anything to the radio to receive a clear or coded signal. It was automatically accomplished by the circuitry.

EOM

The last topic to be discussed during receive time is EOM. It was stated that when the operator released the P’IT, an EOM signal was generated and transmitted. Now let’s see what the receiving unit does with the EOM.

One property of an encrypted message is the presence of significant 6 KHz components at all time. As most FM receiver squelch circuits have been designed to view energy above 3 KHz to 4 KHz as noise, these squelch circuits have a tendency to “block’ or mute coded signals. All secure radios are therefore designed to bypass the receiver squelch circuit in the coded mode of operation, and use the code detector output to perform the squelch function.

As a result, however, squelch “tails” of considerable length can result at the end of coded messages. To eliminate these, an EOM scheme was developed which operates in a fashion similar to PL reverse burst. At the end of each coded message a burst of 6 KHz tone approximately 150 msec long is transmitted. Detection of this tone by any coded receiver resets the code detector and mutes the audio. For clear messages, the operation of the receiver squelch circuit and PL decoder, if present are unaffected. The net result of this procedure is that in PL radios there are no squelch tails in either the clear or coded mode, and in carrier squelch units, there are only squelch tails for clear mode operation.

Algorithm Types

Introduction

Now that we have an idea of what SECURENET is and a basic understanding of what takes place with the circuitry, we will discuss some of the SECURENET types, or more commonly, algorithms.

First, let's define some acronyms used by Motorola. **DVP** stands for Digital Voice Protection, and DES stands for Data Encryption Standard. XL is the nomenclature used to identify an enhanced DVP/DES encryption algorithm. The enhancements and differences will be discussed later in the section. For now, know that none of the algorithms are compatible with each other. ***Table 2*** shows the features of the algorithms produced by Motorola and sold domestically.

	DVP	DVP-XL	DES	DES-XL
KEY FORMAT	OCTAL	HEX	HEX	HEX
# OF KEYS	2 3 x 10^{21}	7.9 X 10^{28}	7.2 X 10^{16}	7.2 X 10^{16}
DUAL CODE	YES	NO	NO	NO
NSA APPROVED	NO	NO	YES	YES
MOTOROLA PROPRIETARY	YES	YES	YES	YES
CODE RANGE = CLEAR RANGE	NO	YES	NO	YES

Table 2: ALGORITHM FEATURES

Key Format

The numbering system that the codes or keys of the different algorithms are written in is called the key format. For example, DVP is written in an octal format (0 - 7), and all the others are written in hexadecimal format (0 - F).

# of Keys

This field represents the number of different, unique keys available for a particular algorithm. This number is determined mainly by the key format and the number of entries per keys. Again as an example, with **DVP** written in octal format and 24 entries per key, there will be the approximate number of keys indicated in ***Table 1.***

Dual Code

Normally, an algorithm is capable of holding only one key at a time. Dual code is the ability of the algorithm to develop a 2ND, unrelated code from the first code. You'll notice that DVP is the only algorithm capable of dual code. The one thing to remember with DVP and dual code is that a radio using the original code isn't capable of communicating with another radio using the 2ND derived code.

NSA Approved Algorithms

NSA is an acronym for National Security Agency. These algorithms must meet security specifications written and approved by the NSA. If they don't, then the algorithm can't be sold to other U.S. government agencies. The NSA specifications are the same for a competitor as well, but again Motorola's algorithms aren't compatible with the competitor's.

Motorola Proprietary

Notice that all the algorithms are Motorola proprietary. Information about the exact mathematical processes that take place can't be discussed.

Coded Range = Clear Range

The last line of the ***Table 1*** shows one of the differences between non-XL and XL algorithms. Later, we will discuss a couple of more differences. **A** non-XL system will have some range loss in the coded mode verses the clear mode. However, with the enhanced XL version, the coded range is approximately the same as the clear range.

Differences Between Non-XL And XL

Introduction

This of the discussion will cover differences between non-XL and XL algorithms. We will discuss differences in synchronization methods, Bit Error Rate (BER), and more on range differences of coded verses clear.

Synchronization Methods

The first difference between algorithms concerns synchronization methods used in the SECURENET receive circuitry, Figure 12. **A** non-XL type of encryption, sometimes referred to as cipher feedback, uses a method called self-synchronization to synchronize the receive 12 KHz clock. As shown by the top half, the trailing edge of the 12 KHz will fall at or near every transition of the incoming data. If the trailing edge of the clock doesn't fall at the same time as a transition of data, the clock recovery circuits will either slow or speed up the clock to coincide with the falling transition of data. The incoming encrypted data actually synchronizes the clock.

The bottom half is a representation of how an XL type of encryption, sometimes referred to as counter addressing, synchronizes the data. Notice that with XL the signal is preceded with a preamble. This performs a similar function as High Level Guard Tone (HLGT) to a station. Once the preamble is received, sync bits are inserted into the data stream, and these sync bits are used to synchronize the clock, instead of the data synchronizing the clock.

At the end of either transmissions EOM is sent by the transmitting unit. When the receiving unit detects the EOM, which is a clear 6 **KHz** sine wave, it will mute the speaker before the loss of the received carrier. This will prevent a noise burst, "squelch tail", from being heard at the speaker. EOM operates on the same principle as PL reverse burst or DPL EOM tone.

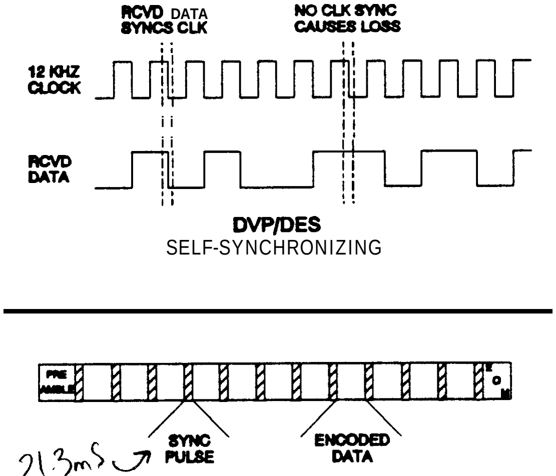


Fig. 12: SYNCHRONIZATION METHODS

BER

The second difference between the two encryption types is Bit Error Rate (BER). The first thing that needs to be discussed about BER is, what is BER? Bit error rate is defined as the percentage of mistakes made by the receiving units digital regeneration circuits due to signal degradation.

Any time a message is transmitted from one unit to another by any means, a certain amount of degradation occurs. This degradation is caused by many factors which may be generalized into three main categories: 1) the addition of noise to the signal; 2) limitations in the bandwidth of the equipment or the transmission medium; and 3) phase non-linearities in the equipment or path. In any analog transmission scheme, including clear voice transmission, there is little which can be done to eliminate most of this degradation once it occurs. Rather the emphasis is placed on trying to prevent the degradation from occurring in the first place, hence such concentrated efforts to obtain high selectivity and intermodulation rejection specifications (to eliminate much of the noise interference by filtering) and close attention to frequency response and harmonic distortion.

When a digital message is transmitted it is subject to the same interferences and distortion, but due to the nature of such a signal many of the standard approaches of dealing with such problems do not apply. Within broad limits, for example, concerns with frequency response and distortion really doesn't apply in the same manner. While an analog signal can't be *'cleaned up" once degraded, a digital signal can be "cleaned up" to a great extent if it is transmitted synchronously. This "clean up" or regeneration consists of limiting the incoming signal to eliminate any noise component which has been added to it, and reclocking it to eliminate any jitter acquired due to system phase non-linearities.

The application of this digital regeneration technique to thetransmission of digital voice messages (as in DVP and DES) causes an effect which is not common in normal radio applications. With conventional FM radio systems, the quality of a received signal slowly degrades as the signal strength drops until eventually the signal-to- noise ratio is so poor that communication ceases. With a digital voice system, the received signal quality is constant as the signal strength drops until it reaches the point where the noise component is so strong that the regeneration circuitry can no longer reconstruct the signal, at which point communications cease. This "cliff' effect makes conventional sensitivity measurements misleading, as 20 dBq and 12 dB SINAD are already below the "knee" of the performance curve, and are therefore not desirable operating points.

To derive a useful measure of coded mode receiver sensitivity, a new concept (to voice communications) must be introduced, known as the "Bit Error Rate". Bit errors are caused by the digital regeneration circuitry making a mistake in recovering the received signal, due either to excessive noise or phase jitter or to bandpass limitations rolling off too much of the amplitude of the signal.

The bit error rate is a measurement of how many bit errors occur in a fixed sample period, usually of **1000** bits or more, expressed as a percentage. There are two distinct types of error rates which are encountered in DVP/DES equipment: 1) the channel error rate and 2) the decoded error rate. The channel error rate is the measure of how many mistakes the regeneration circuitry is making due to imperfections in the transmission path itself. Each bit interpreted incorrectly here is one bit error. Due to the error multiplication property of the DVP/DES decoder, the decoded bit error rate will be considerably higher as this is a measure of the number of wrong bits going into the CVSD. In practice, channel errors are extremely difficult to measure, so in all subsequent discussion “bit error rate” should be taken to mean decoded bit error rate. Coded mode receiver specifications are referenced to 5% bit error rate, which occurs just about the knee of the “cliff’ mentioned before.

Figure* 13 gives** a simplified diagram of the Bit Error Rate differences between non-XL and XL. Notice in a non-XL system, which is represented in the top half of ***Figure 13, 1 channel error in will be multiplied by a factor of 32 through the decoder to give 32 decoded errors on the output. In an XL system, shown in the bottom half of ***Figure*** **13,** 1 channel error in will be multiplied by a factor of 1 through the decoder to give 1 decoded error out. These multiplication factors for non-XL and XL circuitry are due mainly by the synchronization method used in the decoding process mentioned earlier.

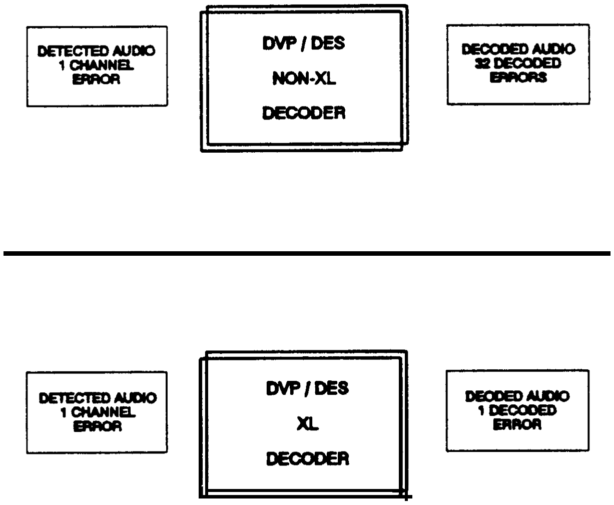

DETECTED AUDIO 1 CHANNEL ERROR
DVP / DES NON-XL DECODER
DECODED AUDIO 32 DECODED ERRORS
DETECTED AUDIO 1 CHANNEL ERROR
DVP / DES XL DECODER
DECODED AUDIO 1 DECODED ERROR

Fig. 13: BER DIFFERENCES

Range Differences

The last topic to be discussed between non-XL and XL concerns differences in coded range as compared to clear range for audio coverage purposes. ***Figure 14*** gives a pictorial representation of clear ranges, coded ranges when using a non-XL system, and coded ranges when using an XL system. Please note that these ranges are approximations and depending on your particular system configuration and optimization, the actual coverage will probably vary.

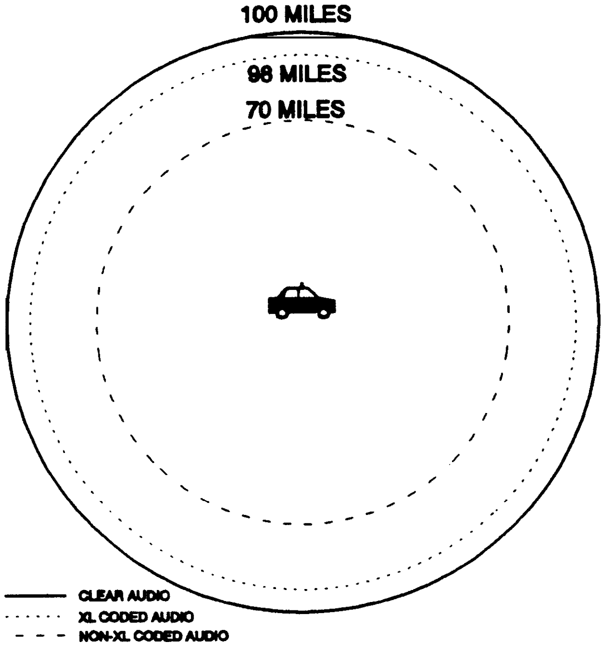


Fig. 14: RANGE DIFFERENCES

In the example, the normal clear range for intelligible audio on the receiving unit's speaker is 100 miles. The non-XL coded audio effective range is about 70 miles. Thus with a non-XL system is use, the effective coverage area is reduced by approximately 30% as compared to clear coverage.

The XL coded audio effective range, however, is about 98 miles. Therefore, with an XL system in operation, the effective coverage is more like clear audio coverage. In this example, the coverage area is approximately 98% that of clear audio coverage.

The reasons for better coverage in an XL system are due mainly to the other differences that were previously discussed: synchronization methods and the multiplication factor with the bit error rate. For some applications a non-XL system will operate with little or no degradation to communications, but in other systems XL may be necessary, such as in trunked system.

Basic SECURENET Systems

Introduction

Now that there is an understanding of what SECURENET is, the different types of algorithms, and the differences between non-XL and XL, we are ready to graduate to the next level of learning. We are going to discuss some basic, generic SECURENET systems. These will be discussed on a block level to get you familiar with components and operation of some typical systems.

Encode/Decode System

The first system is a basic encode / decode system. In an encode/decode system, the encryption key is stored in the base station, mobile and portable radios. The required equipments for this system are a console, encode / decode base station, encode / decode mobile and portable radios. The fact that the base station is capable of encoding and decoding the actual signal, is where the name for this particular system is derived.

Let's take a signal through the system from the console to the subscriber units. Please refer to ***Figure 15*** for the following discussion on the system.

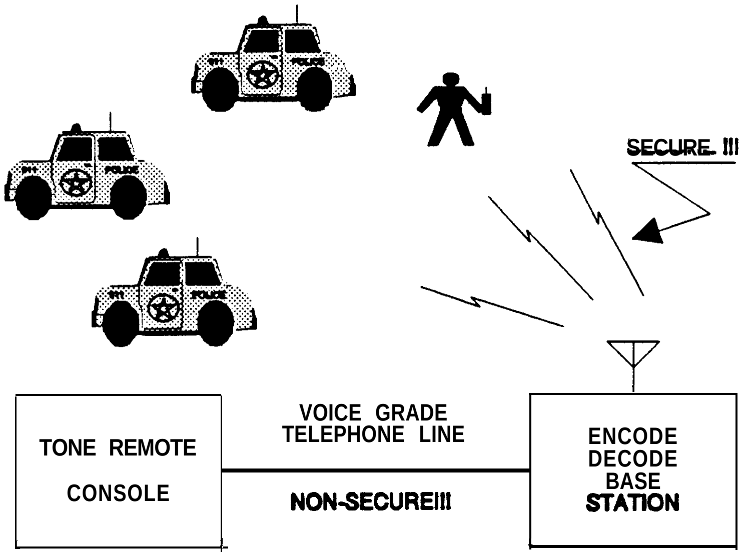


Fig. 15: ENCODE/DECODE SYSTEM

Transmitting of a clear or coded signalis manually selected by the initiating unit, in this case the dispatcher. If the dispatcher selects to transmit coded audio, the tones and voice will travel down normal voice grade telephone line if the station is remotely located. The tones will inform the station to encode the audio before sending it to the modulator. The audio is encoded internally in the base station, sent to the modulator, and transmitted out into the air waves as a "scrambled" signal.

The subscriber units receive the RF, discriminate the signal to recover the intelligence, and decode the signal before sending the audio to the speaker. If the subscriber units are loaded with the same key as the station, then the subscriber operator will hear the audio. If a different key is in the subscriber unit than the station, the operator will hear noise or nothing if proper code detect function is used.

For clear transmission from base station to subscriber unit, the only difference is that the dispatcher selects to transmit in the clear mode. Next the console will now send tones to inform the station not to encode the incoming audio. Clear audio is now sent down the phone lines to the transmitter and over the air.

The exact opposite operation takes place when the subscriber unit wants to talk back to the dispatcher. The mobile or portable radio now converts the clear audio to a “scrambled“ signal. Once again the operator of the subscriber unit has to select to transmit coded audio. The VF signal is encrypted, transmitted, and received by the base station, where it is decoded. The station outputs clear audio on to the phone line and the dispatcher hears the audio at the console.

For clear transmissions from subscriber unit to dispatch operator, the subscriber operator selects to transmit in the clear mode. The base station receives the RF, discriminates the signal to recover the audio, and sends it down the phone line to the dispatcher. Nothing complicated for this type of transmission.

The advantage of this type of system is that any ‘bad guys” listening with scanners will not be able to hear anything usable since the audio is being encrypted. They will only hear noise, and perhaps think that their scanner is broken. Of course if the communication is transmitted in the clear, the scanner will pick it up and the “bad guys” will hear the conversation.

There is also a disadvantage to an encode / decode system. With the technology and money available today, the “bad guys” could possibly tap into the phone lines between the console and base station to monitor dispatch communication before encryption and after decryption. They are now able to hear everything that is being communicated before it is encrypted.

Transparent System

An improved system was developed and is called a transparent system, ***Figure*** 16. Its named is derived from the fact that the base station is now considered transparent to the encryption process This means the base station doesn't hold a key, encode, or decode. It is transparent.

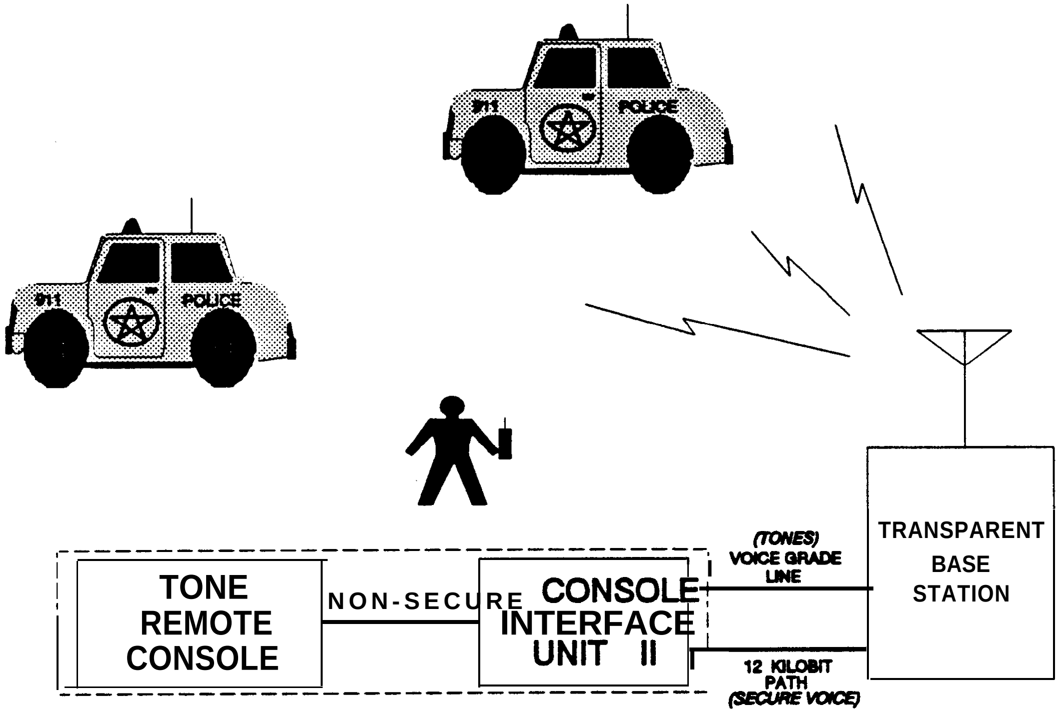


Fig. 16: BASIC TRANSPARENT SYSTEM

The big advantage to this type of system is that security is maintained between dispatcher and base station. Usually the console and CIU are co-located in a secure area. Therefore the link between console and CIU is secure and is very difficult to compromise. The link between CIU and base station can now be guaranteed to be secure. If bad guys can tie into the phone lines, they will hear the guard tones. Big deal! If they tie into the 12 kilobit path and encoded audio is present, what will they hear? That's right, NOISE! The link between dispatcher and base station is now secure as is the RF link. Much, much better for security purposes!

As you can see there are differences between this system and an encode/decode system. The addition of the console interface unit, referred to as a CIU, is now where the encoding and decoding take place. Also in this system, the base station is transparent and not an encoding/decoding station. Therefore, the actual key is loaded and stored in the CIU.

Let's take audio through the system from the console to the subscriber units. Transmitting of a clear or coded audio is again manually selected by the initiating unit, in this case the dispatcher. If the dispatcher selects to transmit coded audio, the tones will travel down a normal voice grade telephone line to the station if the station is a MICOR.

If the station is an MSF 5000, the tones will travel down the same path as the audio. The tones will inform the station that encoded audio is coming and to disable the clear processing circuits and enable the coded processing circuits. The audio is encoded in the CIU and sent to the base station down a 12 kilobit path. Due to the frequencies that comprise an encoded signal and bandwidth restrictions of a voice grade phone line, a dedicated path is required for the data. The base station then sends the encoded signal to the modulator and transmitted out into the air waves as a “scrambled” signal.

As far as the subscriber units are concerned in a transparent system, nothing different takes place during receive or transmit conditions. For clear transmission from base station to subscriber unit, the only difference is that the dispatcher selects to transmit in the clear. Next the console will now send tones to inform the station to enable the clear audio processing circuits. Clear audio is now sent to the CIU. The CIU does nothing with the audio but pass it through and down the 12 kilobit path lines to the transmitter.

The exact opposite operation takes place when the subscriber unit wants to talk back to the dispatcher. The mobile or portable radio now converts the clear audio to a “scrambled” signal. Once again the operator of the subscriber unit has to select to transmit coded audio. The RF signal is now encrypted, and received by the base station, where it is processed but not decoded. The station outputs coded audio onto the 12 kilobit path line to the CIU where it is decoded. The clear audio from the CIU is sent to the dispatcher who will hear the audio at the console.

For clear transmissions from subscriber unit to the dispatcher, the subscriber operator selects to transmit in the clear. The base station receives the RF, discriminates the signal to recover the audio, and sends it down the 12 kilobit path to the CIU. The CIU passes the clear audio through and sends it to the dispatcher. A little bit different than an encode/decode system, but again nothing is done to the clear audio throughout the signal path.

ADDITIONAL READING

The following materials were used as reference materials for part of the discussion. For more detailed information concerning delta modulation, CVSD, analysis of eye patterns and testing for distortion in the eye pattern please refer to these sources.

1. Advanced Digital Audio. Pohlmann, Ken C., ed. Carmel, Indiana: Sams, 1991.

2. Bellamy, John C. Digital Telephony. New York: John Wiley & Sons, 1982.

3. Hughes, Larry. Data Communication. New York: McGraw-Hill, Inc., 1992.

4. "SECURENET Digital Voice Protection System - System Planner." Motorola, Inc. Schaumburg, IL. 1986. Manual No. R4-2-57A.

5. "SECURENET Systems Video." Motorola, Inc. Schaumburg, IL. 1989. Video No. RO-15-02.

6. Smith, David R. Digital Transmission Systems. New York: Van Norstrand Reinhold, 1985.

7. Transmission Systems For Communications. Jordan and Penney, ed. Holmdel, New Jersey: Bell Telephone Laboratories, Inc., 1982.