3
COMMUNICATIONS ELECTRONIC PROTECTION

3.1 INTRODUCTION

Electronic protection (EP) comprises those actions taken to protect personnel, facilities, and equipment from any effects of friendly or adversary employment of EW that degrade, neutralise, or destroy friendly combat capability. In other words, EP is concerned with minimising the effects of both friendly EA and an adversary's EA and ES. While EP is traditionally most concerned with protecting communications equipment, it is applicable to the protection of all systems [1].

EP is usually divided into *passive EP* and *active EP*, as shown in Figure 3.1. Passive EP comprises measures that are not detectable by an adversary, and is concerned with tactics and procedures for providing electronic protection, including terrain shielding. Active EP, whose measures are detectable by an adversary, is concerned with providing protection by the use of special equipment, or special operating modes of equipment.

One important way in which EP differs to the other EW sub-divisions is that it should be practised by all tactical units, not just by specialist EW units. Unlike other aspects of EW, EP is directly associated with the tactical communications system. The techniques discussed in this chapter relate to the employment of the tactical communications system or to specific features of the equipment that makes up the tactical communications system.

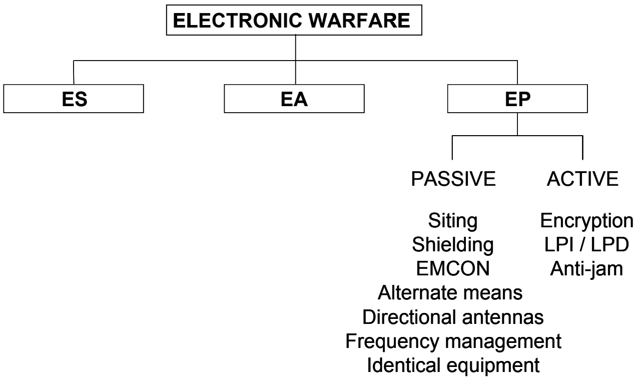

Figure 3.1 EW architecture.

3.2 PASSIVE ELECTRONIC PROTECTION

Passive EP makes use of tactics and procedures to reduce the exposure of friendly use of the electromagnetic spectrum to both friendly and adversary EA. These tactics and procedures include the use whenever possible of identical equipment, shielding, emission control (EMCON), the use of directional antennas, frequency management, the provision and use of alternate means, and siting of communications.

3.2.1 Identical Equipment

Variations in the characteristics of transmissions from different types of equipment can be used to infer a variety of information about a force. In some armies, for example, older CNR equipment in service with reserve forces has a channel bandwidth of 50 kHz; newer CNR, used by higher-readiness troops, has a channel bandwidth of 25 kHz. The type of unit can therefore be inferred from the channel bandwidth being used by integral radio systems. Similarly, coalition forces can often be separated by their equipment. The use of identical communications equipment assists in removing this source of information.

3.2.2 Shielding

All electronic equipment radiates electromagnetic energy, and is potentially vulnerable to the effects of electromagnetic energy radiated by other electronic equipment. Shielding is a means of reducing both the amount of energy radiated and the vulnerability to received radiation, and offers protection against both adversary ES and EA.

The radiation generated by an electronic system is a potential target for adversary ES. While the potential range over which this ES is likely to be effective is small (perhaps hundreds of metres at most), ensuring that adversary ES is excluded from such an area may be difficult, especially in strategic systems and logistics installations. The use of shielding and other measures to reduce vulnerability to adversary ES is known as TEMPEST [2].

The use of shielding to protect systems from external radiation counters the potential use of neutralisation as a form of EA. The major threat historically has been the EMP resulting from a detonation of a nuclear weapon. In the future, such high levels of radiation may be able to be generated by small, non-nuclear devices such as radio frequency directed energy weapons (RF DEW).

3.2.3 Emission Control

An emission control plan may be used to reduce or alter the electronic signature of a force. This may be achieved by reducing the level of particular types of transmissions or the insertion of dummy traffic. Two commonly used modes of emission control are *radio silence* in which all communications transmitters are deactivated, and *electronic silence* in which all electronic emitters, including radars, are deactivated.

When planning emission control, it must be recognised that the imposition of radio and electronic silence may place operational constraints on the force, which may in turn increase rather than decrease its vulnerability.

3.2.4 Directional Antennas

Directional antennas are commonly used in tactical communications systems in which there is a single transmitter and a single receiver. An example of such a system is a radio relay link. The use of a directional antenna for transmission also maximises the amount of power radiated toward the intended receiver and reduces the amount of power radiated in other directions. With careful siting, this can be used to minimise the power received at potential sites for an adversary's ES. The use of a directional antenna for transmission maximises the received power from the intended transmitter, and reduces the amount of power received from other directions. This directionality can be used, for example, to reduce the effectiveness of an off-axis jammer.

For systems, such as CNR, where there is more than one receiver, omnidirectional antennas are usually used. The use of directional antennas is therefore limited. Some of the benefits of a directional antenna can be obtained by using an antenna with a steerable null that can be directed towards an adversary's ES or EA site. However, the practical use of null-steering antennas is restricted in highly mobile nets where the locations of friendly units change rapidly.

3.2.5 Frequency Management

Frequency management is required as part of communications planning to allocate the available capacity of the electromagnetic spectrum to users to avoid co-channel interference. This planning takes into account the relative locations of units, the likely range of communications (which is frequency-dependent), and interference that may be caused by harmonics and intermodulation products between systems located close together. Another important aspect of frequency management that can assist EP measures is the allocation of alternate frequencies that can be used in the event of interference or jamming.

3.2.6 Alternate Means

EP can be provided by the use of a variety of alternate communications means, which may be used either to overcome interfering EA or to reduce the susceptibility to ES. Some alternate means, such as line and messenger, do not involve radio and they are therefore particularly useful during periods of radio silence, but tend to limit mobility. Others may provide a different type of radio channel, such as using a trunk circuit rather than a CNR channel.

3.2.7 Siting

Planning for the siting of communications systems takes into account propagation of radio waves between chosen sites. This planning should also seek to minimise an adversary's potential use of EA and ES.

One means of doing this is to use *terrain shielding* (or *terrain screening*), as illustrated in Figure 3.2 and Figure 3.3. In Figure 3.2, where transmitters are located on the tops of hills, reception is possible at a potential site for an adversary's ES or EA assets. On the other hand, by moving the transmitters down from the tops of the hills as illustrated in Figure 3.3, communication is maintained while denying coverage at the adversary's location.

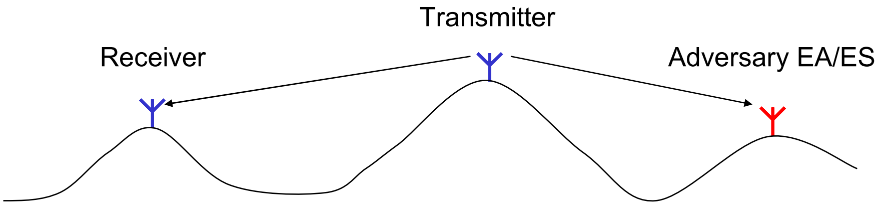

Figure 3.2. Ineffective terrain shielding.

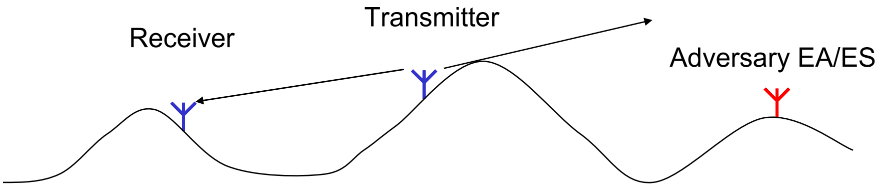

Figure 3.3. Effective terrain shielding.

Terrain shielding is most effective at VHF and higher frequencies where most tactical CNR radios operate. At these frequencies, propagation is essentially line-of-sight, and therefore tends to be terrain-limited rather than power-limited.

Effective siting of radio equipment for EP requires knowledge of the effective range of communications. This requires carrying out radio path planning not only for the communications network being planned, but also for potential sites for an adversary's ES and EA assets.

Some protection can also be gained from the careful use of shields in the area of the communications system, such as metal buildings, to provide screening. It is usually difficult, however, to predict the effectiveness of such procedures in advance. Although their effectiveness against an adversary's jamming may be measurable while the jammer is inactive, it is difficult to estimate their effectiveness against ES.

3.3 ACTIVE ELECTRONIC PROTECTION

Active EP uses special equipment or operating modes of equipment to provide protection. The specific aims of protection provided by active EP are communications security, low probability of intercept (LPI), and resistance to jamming.

Masking, which is the jamming of an adversary's ES receivers in such a way as to prevent their inhibiting friendly use of the electromagnetic spectrum, is sometimes also classified as EP. In this book, however, masking is covered under EA in Chapter 5.

A wide variety of techniques are used to provide active EP, including encryption, modulation, error protection coding, burst transmissions, narrowband excision, diversity, free-channel search, and appropriate use of retransmission.

Encryption. Encryption is used to modify transmitted data in such a way that it can only be decoded by the intended recipient. Encryption also protects against the insertion of dummy traffic by an adversary; some types of encryption also protect against imitative deception. Encryption is typically possible only in digital systems.

Modulation type. Some forms of modulation provide higher levels of protection than others. *Spread-spectrum communications* involves the spreading of a transmission across a wide band of frequencies. This can provide both LPI and a high-level of resistance to jamming. *Morse code* can often be used successfully on communications channels where voice and data communications are not possible. The primary disadvantages are the very low data rates obtained and the large cost of training operators and maintaining their skills.

Error-protection coding. The addition of error-protecting codes can increase the amount of interference that can be tolerated for a given quality of service.

Burst transmissions. An adversary’s EA and ES can be hindered by reducing the length of transmissions. This may be achieved, for example, by using data rather than voice. If the length of a burst is sufficiently short, an adversary’s intercept, DF, or responsive jammer may not be effective.

Narrow-band excision. The impact of an interfering signal that has a much smaller bandwidth than a transmission can be minimised by excising the part of the spectrum containing the interfering signal before decoding. In digital communications systems, this technique is usually useful only when applied in conjunction with error-protection coding.

Diversity. Protection against jamming and other forms of interference can be gained by transmitting data over more than one channel between transmitter and receiver. Diversity can be achieved in space, time, and frequency.

Free-channel search. Conventional CNR uses a single channel for each net, with operators required to change frequency manually to overcome interference or jamming. Free-channel search allocates a group of frequencies to a group of nets. Radios on the net automatically identify a free channel when they wish to transmit, and then signal this choice of channel to other stations on the same net. Each transmission on the net may therefore use a different frequency. The potential drawback of such a system is that a jammer may be able to keep stations locked to a particular frequency by making it appear that this frequency is still in use by the net.

Appropriate use of retransmission. Retransmission is often required for line-of-sight communications. A radio-relay network, for example, is built from point-to-point links between nodes. In CNR, retransmission is often required to overcome the effects of terrain. Care in siting, use of manual retransmission, and considered action on jamming is required to limit the vulnerability of retransmitted links to jamming. Rebroadcast stations are typically sited on the tops of terrain features, where they are most vulnerable to ES and EA. Siting in less exposed locations may reduce this vulnerability, while still permitting effective rebroadcast. An automatic rebroadcast will transmit not only voice and data, but also jamming signals, so some form of manual control may be used so that jamming signals are not retransmitted. A rebroadcast station may continue to rebroadcast on a frequency even when other stations on the net have moved to an alternate frequency due to jamming. This increases an adversary’s difficulty in evaluating the effectiveness of jamming.

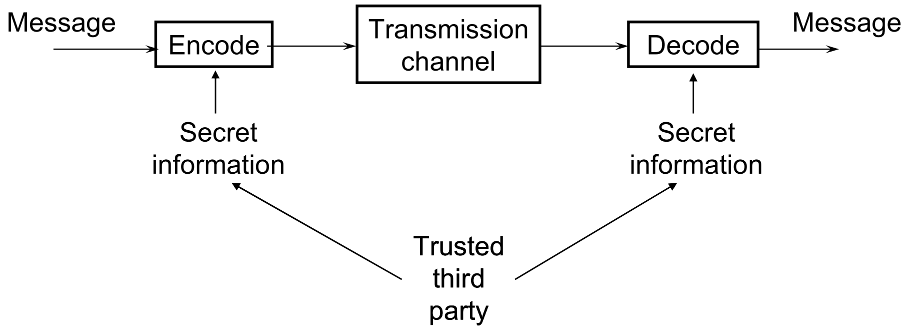

Figure 3.4 Generic structure of a secure communications system.

3.3.1 Encryption

Encryption protects digital data by transforming the original data (*plaintext*) into a different form (*ciphertext*) that can be revealed without disclosing the original data [3]. The basic structure of a secure communications system employing encryption is shown in Figure 3.4. Encoding (known as encryption) and decoding (decryption) involve a security-related transformation. Secret information, which is distributed by a trusted third party, is usually used to modify this transformation so that the security of the system can be maintained even if the encoding and decoding algorithms are widely known. This secret information is often referred to as a *shared secret* or *key*.

There are three main forms of encryption: bulk encryption, message encryption, and message-content encryption:

- *Bulk encryption.* Here, encryption of all data on a link on which transmission is continuous prevents both unauthorised reception and traffic analysis. This form of encryption is used by most trunk communications systems, and is therefore sometimes referred to as *trunk encryption*. As well as protecting against interception, this form of encryption protects against deception.
- *Message encryption.* In message encryption, individual messages on a link are encrypted including both message header and contents. This form of encryption is used in most CNR systems. While the contents of the messages are protected from interception, message encryption does not prevent traffic analysis. If synchronisation is achieved through a preamble, no protection is provided against deception by delayed replay of previous traffic.
- *Message-content encryption.* In message-content encryption, the bodies of messages are encrypted, leaving message headers in plain text. This form of encryption is often used in packet-switching

systems. It has the advantage that intermediate switches and routers are not required to have attached cipher equipment. The disadvantage, however, is that detailed information that can be used in traffic analysis is provided in plain text. If synchronisation is achieved through a preamble, this type of encryption does not protect against deception by delayed replay of previous traffic.

In general, the aim of an encryption system is to generate ciphertext that appears to be a random bit stream. In an ideal system, this randomness includes:

- *No structure observable in ciphertext.* Any structure of the plaintext, such as regular repeating patterns or different probabilities of occurrence for different symbols, should be removed in the encryption process to produce a ciphertext that has no regular structure.
- *Long key.* The maximum amount of work required for cryptanalysis is to decrypt the ciphertext using every possible key. The use of long keys maximises the difficulty of this task. For a key that is n bits long, there are 2^n possible keys.
- *Strong avalanche effect.* There should be large differences in ciphertext for similar keys with the same plaintext and similar plaintexts with the same key. Without the avalanche effect, similar plaintext can lead to similar ciphertext, greatly simplifying cryptanalysis.
- *Diffusion.* Every bit of plaintext should affect a large number of bits in the ciphertext.

In communications systems that introduce errors into transmitted bit streams, both the avalanche effect and diffusion can lead to a single bit error in the ciphertext causing multiple bit errors in the deciphered plaintext. This phenomenon is known as *error extension*. For this reason, many practical encryption systems do not exhibit either a strong avalanche effect or diffusion.

In message encryption and message-content encryption, the encryption engine is re-started in a known state at regular intervals. In CNR for example, where each transmission is independently encrypted, the decryption engine must know the initial state of the encryption engine at the start of each transmission. If this known state is always the same, the task of the cryptanalyst is greatly simplified. Some additional information that is known to both encryption and decryption systems is normally used to allow the encryption engine to begin each new message in a different state. Synchronisation between transmitter and receiver can be achieved by transmitting a preamble containing the additional synchronisation information at the beginning of each transmission, and possibly transmitting further synchronisation information at regular intervals during the transmission; or deriving the additional synchronisation information from an accurate time reference known to both transmitter and receiver.

3.3.1.1 Stream and Block Ciphers

A *stream cipher* operates on each bit of the transmitted message separately. This is usually implemented by generating a pseudo-random keystream. Each bit of the transmitted stream is the exclusive-OR (XOR) of the corresponding bits of the keystream and the message, as shown in Figure 3.5. Alternatively, a *block cipher* operates on blocks of the message. It requires buffering of a block of data, followed by processing and transmission of that block on the output channel.

Stream ciphers are easy to implement on synchronous communications channels because they produce one output bit for every input bit, produce only one bit-period of delay, and do not require additional buffering. Their disadvantage is that they cannot exhibit either diffusion or the avalanche effect with respect to the message.

Many military encryption systems are used to encrypt data on synchronous communications channels. Such systems usually employ stream ciphers. For data transmission, this prevents the transmission of synchronisation information, except as a preamble at the beginning of a transmission. Some voice systems steal bits during the transmission to transmit synchronisation information, reducing their susceptibility to loss of synchronisation when jammed. Off-line systems, such as one-time letter pads, are usually block ciphers.

3.3.1.2 Public-key vs Secret-key Encryption

In traditional crypto systems, the same key is used for encryption and decryption. This type of system is referred to as a *secret-key* (or *symmetric*) encryption system, and is illustrated in Figure 3.6. The key that modifies the operation of the encryption and decryption engines is the shared secret.

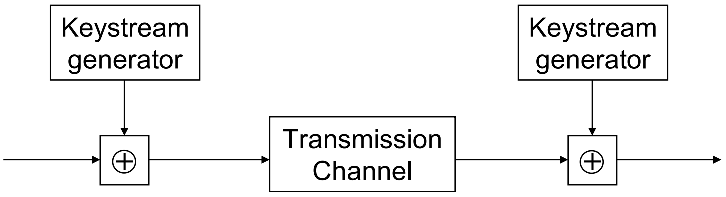

Figure 3.5. Structure of a stream-cipher system.

Secret-key encryption can only provide limited security services. It can provide for *confidentiality* (that is, ensuring that messages are not disclosed to unauthorised parties). Encryption can also provide a limited form of authentication, since a receiver can assume that only trusted parties possess the secret key? It is difficult, however, to guarantee the integrity of a message, because any party capable of decrypting a message is also capable of changing the message and re-encrypting this corrupted version.

The solution to this problem is to separate the encryption and decryption keys, such that one can be made public without compromising the security of the other. This form of asymmetric encryption is known as *public-key encryption*. Public-key encryption makes possible a range of additional security services, including integrity and authentication.

The technical basis of public-key encryption is in the differences in computational complexity for particular inverse mathematical operations. Multiplication, for example, is much less complex than factorisation. Public-key encryption systems make use of the simpler operation to generate the keys. Any attack on the security of the system must be based on the more complex, inverse operation. It is therefore possible to create a system in which it is easy to generate a matched pair of encryption and decryption keys, but that it is very difficult to obtain one of these keys from the other.

The computational operations required for public-key encryption and decryption typically include multiplication and exponentiation. These operations tend to be best implemented using general-purpose computation engines, such as those found at the heart of a computer. Most secret-key systems utilise only basic logic operations (AND, OR and XOR) and a small number of additions. These operations can be efficiently implemented in fast, special-purpose hardware. Because of this difference in the types of operations required, public-key encryption is much more expensive to implement, especially for high-speed communications.

Hybrid systems use secret-key encryption to transfer data, with the keys for the secret-key encryption being transferred using public-key encryption. Such systems have the advantage that they provide only small amounts of public-key ciphertext for cryptanalysis and favour regular changing of the secret keys used to encrypt the data to be transferred.

The advantages of secret-key encryption over public-key encryption are simplicity of implementation and low computational complexity. The primary advantage of public-key encryption over secret-key encryption is the variety of security services that can be offered.

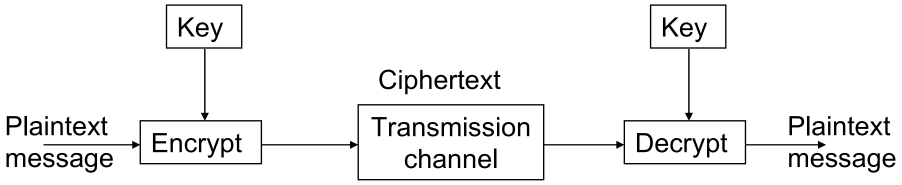

Figure 3.6. Structure of a secret-key secure communications system.

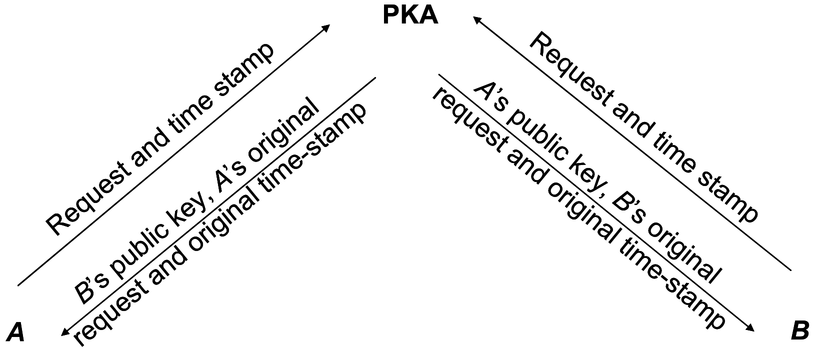
PKA
Request and time stamp
B's public key, A's original request and original time-stamp
Request and time stamp
A's public key, B's original request and original time-stamp
A
B

Figure 3.7. Use of the public key authority.

A number of secret-key encryption systems are in common use. The Data Encryption Standard (DES) has been established by the US National Institute of Standards for the secure transmission of commercial data. It uses a 56-bit key to encrypt blocks of 64 bits of data. The short length of the key is a serious weakness, leading to the use of the so-called *triple-DES*, which provides a key length of 112 bits with backwards compatibility with DES if the first and second 56-bit halves of the key are the same. The *International Data Encryption Algorithm (IDEA)* developed at the Swiss Federal Institute of Technology is also based on 64-bit blocks, but uses a 128-bit key. Skipjack [4] is a block cipher using a 64-bit block size with an 80-bit key, designed by the US National Security Agency. This algorithm was initially classified, but has been recently released publicly. The basic GSM A5 [5] is a stream encryption system that employs a 64-bit key. Because the keystream generator is restarted every 228 bits, however, it is effectively used as a block cipher.

The most commonly used public-key encryption systems are the Rivest-Shamir-Adleman Algorithm (RSA) [6], and the Key Exchange Algorithm (KEA) [7].

3.3.1.3 Public-key Authorities and Certificate Authorities

Establishment of secure communications requires a trusted intermediary to enable secure distribution of public keys. Given the existence of this third party whose public key is already known to both parties, known as a *public-key authority* (PKA), two parties *A* and *B* can exchange public keys and authenticate the other party. For *A* to receive *B*'s public key, (Figure 3.7), *A* sends plaintext message to the public-key authority, containing a time-stamp and a request for *B*'s public key. The authority sends *A* an encrypted message containing *B*'s public key; *A*'s original request, so that *A* can verify that it has not been altered during transmission from *A* to the public-key authority; and the original time stamp, so that *A* can verify that the message was generated in response to this particular request.

A uses the public-key authority's public key to decrypt this message. The placement of both *A*'s original request and the original time stamp in the message returned by the public-key authority is required to prevent spoofing attacks on the key exchange.

The potential drawback of public-key authority is that it may become a bottleneck, especially if a large number of parties wish to establish secure communications. This problem is overcome by the use of a *certificate authority* (CA). The certificate authority creates certificates, which are encrypted messages containing a user's public key, the user's identification, and a timestamp. The user then distributes this certificate with the time stamp. The authenticity of the certificate can be assured if the CA's public key is known. Furthermore, if the certificate authority has suitable controls for the issuing of certificates, a certificate can authenticate the holder of the certificate.

3.3.1.4 Level of Security

The process of attempting to obtain plaintext without access to the shared secret is known as *cryptanalysis.* The computational resources required to attack a particular encryption algorithm define the difficulty of cryptanalysis and therefore the security of the algorithm.

An *unconditionally secure* encryption system is one for which it is impossible to obtain plaintext from ciphertext without possessing the shared secret. The only such system known is the *one-time pad*, which works by defining a sequence of randomly chosen transformations that are applied to each symbol of the plaintext to produce ciphertext. If a particular one-time pad is only used once, and the transformations are perfectly random, cryptanalysis is impossible.

Most practical systems are not based on the one-time pad, however, and are therefore not unconditionally secure. While it is therefore possible to apply cryptanalysis successfully to such systems, it may not be feasible. An encryption system may be said to be *computationally secure* if either the cost of breaking cipher exceeds the value of the encrypted information, or the time required to break the cipher exceeds the useful lifetime of the information.

Figure 3.8 shows how the time required for exhaustive cryptanalysis varies with the key length. The times shown take into account both processing time and Moore’s law, which states that the computational power of computers increases by approximately a factor of 10 every five years. It can be seen that short keys provide only low levels of security. Longer keys, such as 128-bit and 256-bit keys, provide much higher levels of security, exceeding 100 years even if the initial computational power available is 10^{18} operations per second. This far exceeds the capability of any current computer.

Some encryption systems have systematic weaknesses that allow cryptanalysis without having to try all possible keys—that is, the structure of the algorithm can be exploited by the cryptanalyst. These systematic weaknesses can greatly reduce the required effort for cryptanalysis and hence the security provided.

Systematic weaknesses can be the result of technical shortcomings in the design of the encryption algorithm, which is the case for the GSM encryption system, known as A5. These weaknesses are discussed further in the section on GSM later in this chapter. Systematic weaknesses can also be introduced by procedures: the WW2 German Enigma system had two such weakness that were crucial in breaking it: the first group of three letters in the plaintext was used to key the deciphering Enigma machine, and these three letters were encrypted twice, and the choice of these letters was often predictable. In addition, it was common for some stations to transmit messages beginning with phrases such as “Heil Hitler”, providing corresponding plaintext and ciphertext for the cryptanalyst.

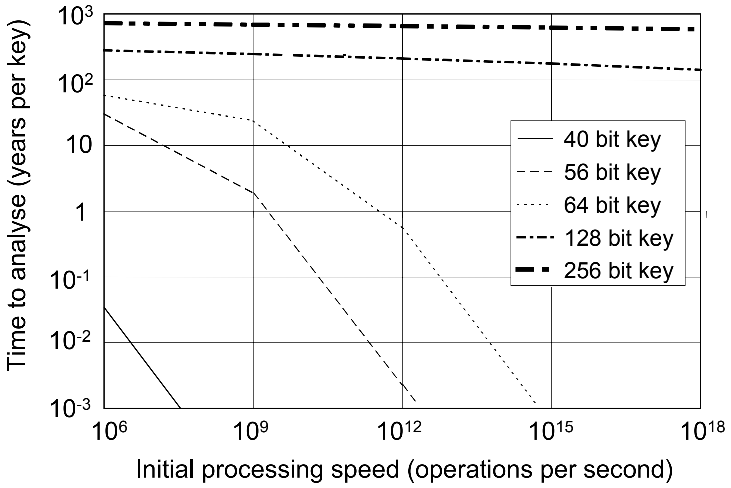

Figure 3.8. Time required for exhaustive cryptanalysis, taking into account Moore's law.

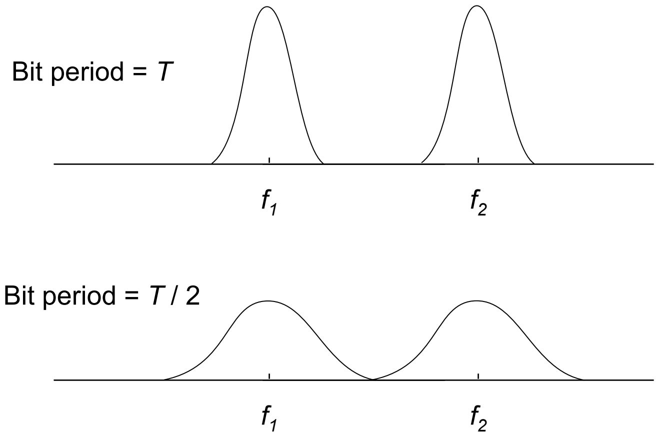

Figure 3.9. Changing bandwidth with symbol time.

3.3.2 Spread-spectrum Communications

Spread-spectrum techniques are used in communications to provide multiple access, resistance to jamming and other interference, and LPI [8]. In military communications systems, resistance to jamming and LPI (that is, EP) and multiple access are the major motivation for the use of spread-spectrum techniques. In commercial systems, the major benefits are multiple access and resistance to accidental interference. These features are all achieved by expanding the bandwidth of a signal so that it is transmitted across a number of channels.

There are several types of spread-spectrum techniques. The major types are *direct-sequence spread-spectrum (DSSS)*, *frequency hopping (FH)*, and *chirping*. Chirping is used to provide EP for radar systems, but is not commonly used in communications systems, and is not considered further here.

3.3.2.1 Direct-sequence Spread Spectrum (DSSS)

Regardless of the type of modulation used, the bandwidth occupied by a digital signal is proportional to its symbol rate. Figure 3.9 illustrates this point for a pseudo-random bit stream modulated with FSK. When the bit period is halved (that is, the bit rate is doubled), the bandwidth of the signal around each of the tones is doubled.

A bit stream can therefore be spread over a larger frequency band by increasing its rate. One way that this can be achieved is to modulate the stream with a pseudo-noise (PN) stream at a higher rate. For clarity, the terms ‘bit’ is used here to refer to the data unit of the original stream and ‘chip’ to refer to the individual data units of the pseudo noise stream. The number of chips per bit is often referred to as the *spreading gain* or *processing gain*. The spreading gain is also the factor by which the channel bandwidth is increased.

In a simple example, each 0-valued bit of the stream 01001110 can be replaced with the three chips 010 and each 1 with 101, giving a new chip-stream 010101010010101101101010. This stream has three times as many chips as the original stream has bits.

Decoding the DSSS stream requires replacing each group of three chips with either a 0 or a 1 to return the original bit stream. For security, a military DSSS system would usually modify the spreading sequence used from one bit to the next to avoid transmitting a short, easily decoded, repeating pattern.

Where errors have been introduced into the chip-stream, a voting procedure is used which maps each group of three chips to the closest-valued bit.

000 → 0	100 → 1
001 → 1	101 → 1
010 → 0	110 → 0
011 → 0	111 → 1

This process can also be illustrated directly in terms of the bandwidth of the signal. The transmitted spectrum is spread as shown in Figure 3.10 by modulating the baseband signal with the digital code sequence produced by the PN Code generator. The DSSS receiver uses the same PN sequence to convert the wide-band spread signal back to its original form.

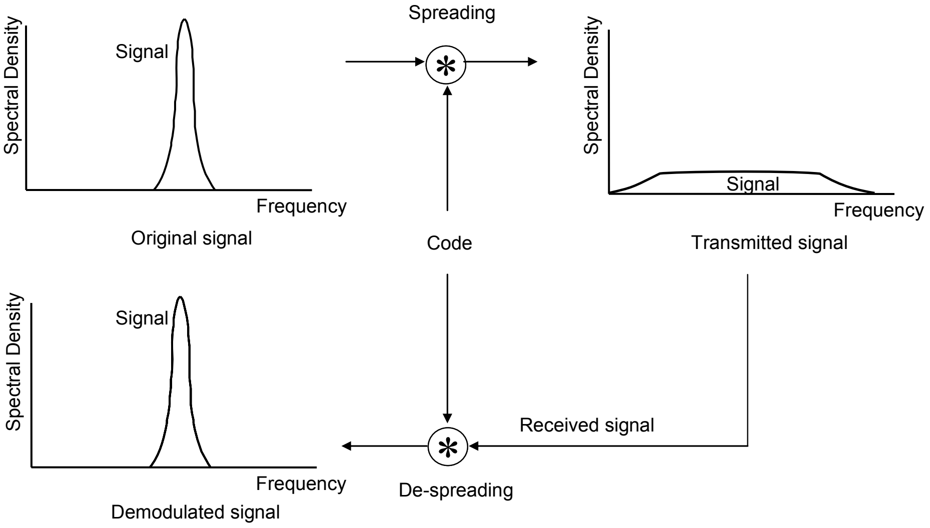

Figure 3.10. Direct-sequence spread spectrum.

DSSS can be implemented in two ways. In *wide-band spread-spectrum*, a transmission with a fixed information rate is spread over a number of channels, resulting in an increase in the data rate. In *in-band spread-spectrum*, a single channel is used at a fixed data rate, resulting in a decrease in information rate. This form of spread spectrum permits only very small data rates to be transmitted.

In order to carry out the de-spreading operation, a DSSS receiver must know the spreading sequence that has been used to spread the original bit stream before transmission. The receiver must also synchronise itself with the transmitter. This may involve knowing (at least implicitly) how many bits have been sent in the current transmission and the location in the PN sequence at which the transmission started. This can be achieved by transmitting a synchronisation preamble at the beginning of each transmission, and possibly inserting resynchronisation information at regular intervals during the transmission; or by using an accurate time reference known to both transmitter and receiver.

Interference from other DSSS signals is covered in the following section. Interference caused by single DSSS transmission to other types of signals will have similar effects to a small increase in channel noise, leading to a reduction in the signal-to-noise ratio at the input to the receiver. Where multiple DSSS transmissions take place in a particular part of the spectrum, this noise level will rise significantly and may preclude operation of other systems in the frequency band used.

3.3.2.1.1 Resistance to Jamming and Interference

When a spot jammer, or single-channel transmitter, introduces the interference spike shown in Figure 3.11, the receiver de-spreads the signal but, by the same process, spreads the interference. This means that the receiver can remove most of the interfering signal in the demodulation process. As a result, a spot jammer has significantly less impact on the spread signal than on a conventional signal. Additionally, the DSSS signal can occupy the same bandwidth as a number of single channel radios without significant interference.

Figure 3.12 shows that spread-spectrum transmission also provides protection against wide-band interference, such as that caused by a barrage jammer or by other spread-spectrum transmissions that use different spreading sequences. Again, any signal not originally spread by the transmitter will not be de-spread at the receiver, but will be spread to reduce its impact on the wanted signal.

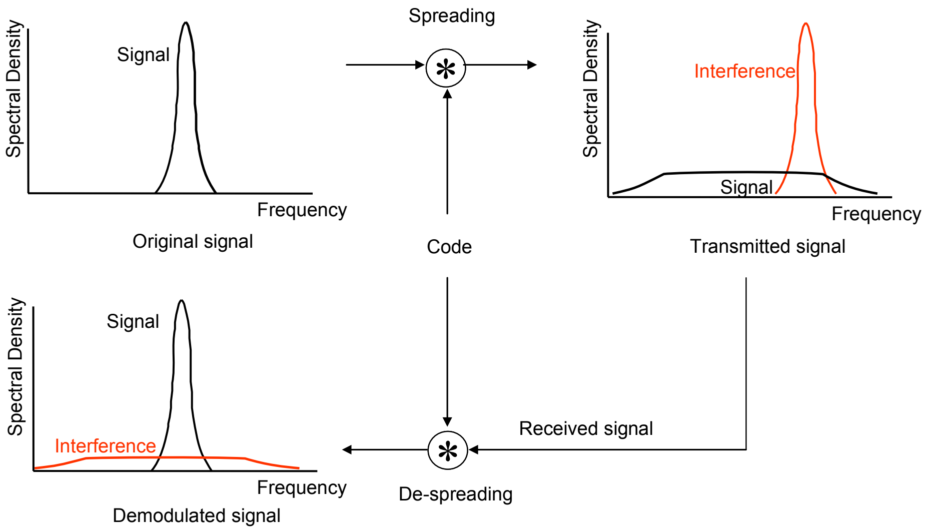

Figure 3.11. **Direct-sequence spread-spectrum in the presence of narrow-band interference.**

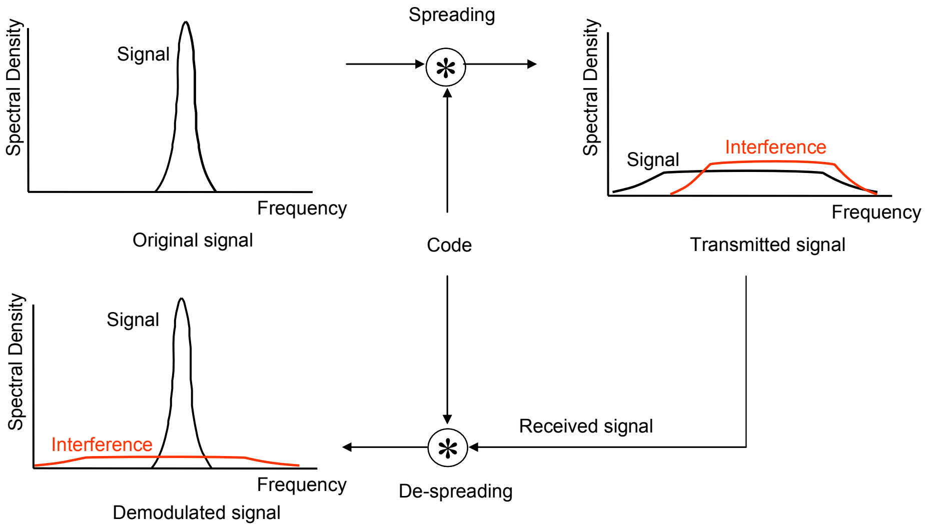

Figure 3.12. **Direct-sequence spread spectrum in the presence of broad-band interference.**

The observations in Figure 3.11 and Figure 3.12 give rise to the concept of *spreading gain*. A signal with original bandwidth f_0 that is spread using DSSS to a bandwidth of f_s is said to have a spreading gain g_s:

$$g_s = \frac{f_s}{f_0}$$

The spreading gain is a measure of the increased tolerance of a spread-spectrum signal to interference compared to a conventional signal. A signal spread using DSSS transmission will provide the same bit error rate as a conventional signal with the in-band interference power higher by a factor of g_s.

For a jammer, this means that where DSSS is used to protect a single signal, a jammer must deliver g_s times as much in-band power to the receiver as would be required to achieve the same effect on a conventional transmission. As the number of DSSS transmitters sharing a part of the spectrum rises, the total jamming power required to achieve a particular effect on each of the DSSS transmissions individually does not rise. As the number of transmitters rises to g_s, the amount of jamming power required to achieve an effect is the same as would be required if the same signals had been combined using FDMA. The gain from the use of DSSS is that combining using FDMA provides the jammer with the option of jamming a subset of the signals and of concentrating limited jamming power on these signals; the use of DSSS aims to reduce the jammer's flexibility by offering only the options of jamming all of the transmissions or none.

DSSS may also be combined with other EP techniques, including frequency hopping; the use of error correcting codes to reduce the impact of residual errors after despreading; and the use of narrow-band excision to remove narrow-band interfering signals such as would be introduced by spot jamming before despreading, leading to an improved signal-to-noise ratio in the receiver.

If a DSSS system uses a preamble to provide synchronisation, this preamble may be more susceptible to jamming than other parts of the transmission. If the preamble is successfully jammed, none of the rest of the transmission will be successful. One means of avoiding this vulnerability is to base synchronisation on a common, accurate time reference.

3.3.2.1.2 Provision of Multiple Access

DSSS can be used to provide multiple access in a radio channel by allocating a different spreading sequence to each transmitter. This system of *code division multiple access (CDMA)* is commonly used in military communications systems as well as in commercial systems such as cellular mobile systems and satellite communications.

Expanding on the simple example used above, three channels may be allocated the (orthogonal) spreading sequences:

Transmitter 1:	0 → 001, 1 → 110
Transmitter 2:	0 → 011, 1 → 100
Transmitter 3:	0 → 111, 1 → 000

These spreading sequences can then be used to convert the following three bit streams into a chip stream:

Transmitter 1:	0011 → 001001110110
Transmitter 2:	1010 → 100011100011
Transmitter 3:	1101 → 000000111000

If these three sequences are transmitted onto the same channel at the same power, and the three transmissions arrive synchronised at the receiver, the received chip stream is found to be 000001110010 by selecting the value of a chip as 0 if two or more of the individual channel chips are zero and 1 otherwise. In practical systems, this voting process occurs when the three modulated signals are combined in the receiver's antenna. Even though the chip timing of the transmissions is synchronised, the carriers of these modulated signals may not be synchronised, causing the received power level to be lowered by destructive interference between the received signals.

Decoding of one channel can be carried out by taking the exclusive-OR of the received chip stream with the chip sequence associated with the value 0 for that channel, and applying the same voting procedure as described previously.

For the example above:

Receiver 1:	000001110010 ⊕ 001	→	001000111011
Receiver 2:	000001110010 ⊕ 011	→	011010101001
Receiver 3:	000001110010 ⊕ 111	→	111110001101

In this example, a spreading factor of three has allowed three channels to be multiplexed. The maximum number of bit streams that can be multiplexed onto a single channel error-free is equal to the spreading factor.

In many practical situations, the transmissions do not arrive at the receiver synchronised at the chip level. In this case when one channel is to be decoded, the combination of the other interfering signals behaves like noise. The performance obtained depends on the spreading gain and the number of channels being multiplexed. In this case, high levels of error protection of usually used to reduce the error rate of the output bit stream.

Where DSSS is used to provide multiple access for a number of transmitters all operating at the same data rate, the best performance is obtained when the received power from all DSSS transmitters is equal and the performance is significantly degraded when this cannot be achieved. In the above example, if one stream were operating at a power significantly higher than the other two, it would have a greater weight in determining the value of each chip on the channel. This issue is examined further below.

The proportion of the total channel capacity allocated to a stream can be controlled by adjusting its spreading factor and transmit power.

Where DSSS is used as a multiple access technique, a jammer still needs to deliver g_s times as much power to a receiver as would be required for a conventional signal. However, g_s is also the maximum number of signals that can be orthogonally multiplexed. When CDMA is used to full capacity, therefore, the difficulty of jamming all these signals is the same as to jam the same set of signals using conventional modulation. The difference is that the jammer does not have the option of concentrating power into one (high-priority) signal; it is forced to jam all signals or none. This effectively prevents a jammer from obtaining the benefits of spot jamming.

3.3.2.1.3 Impact of Overloading

Unlike FDMA and TDMA, CDMA allows (at least theoretically) over-allocation of channel capacity. CDMA can support an essentially arbitrary number of streams, so long as each stream is allocated a different spreading sequence. There is, however, a strict limit on the number of streams that can be carried without mutual interference. The spreading gain g_s, which is equal to the maximum number of orthogonal PN sequences, provides an upper bound on this number of streams. In the absence of external interference or jamming, this limit is equal to g_s. In the presence of external interference, the number of streams that can be carried without error is less than g_s.

3.3.2.1.4 Frequency Management

Spectrum management for DSSS transmissions involves managing both frequencies and spreading sequences. Interfering signals in a DSSS system have a similar impact to an increase in channel noise. This means that when the system approaches its capacity, the quality is gracefully degraded. Frequency management in DSSS systems usually takes advantage of this graceful degradation, implementing statistical rather than deterministic separation between signals. This has the potential to greatly simplify the frequency management process, minimising the need for procedures such as the analysis of harmonics and intermodulation products.

3.3.2.1.5 Near-far Effect

A requirement for efficient implementation of CDMA (that is, the use of DSSS as a multiple access technique) is that each transmitter adjusts its transmitted power so that all receivers receive the same power from each transmitter. This requirement for power balancing has two key implications. First, such power balancing is not possible where there are multiple transmitters and multiple receivers. This makes CDMA unsuitable as a multiple access technique for net-oriented communications, such as CNR.

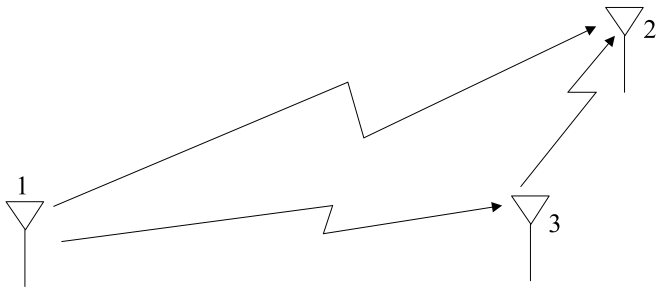

Figure 3.13. The power-balancing problem to overcome the near-far effect.

This effect is known as the near-far effect. Second, successful implementation requires continuous monitoring of received power levels by receivers. The measured levels are sent to transmitters on a signalling channel.

Power balancing is used in CMDA cellular telephone systems to overcome the near-far effect. This is only possible because all communications are either to or from a base-station; there is no direct mobile-mobile communications.

The power-balancing problem is illustrated in Figure 3.13 If stations 1 and 3 set their transmit power so that the same power is received at station 2, then station 1 cannot adjust its power to achieve the same received power at station 3 as station 2. The only solutions to this problem are to accept a loss in efficiency or to structure the system so that all CDMA operates with a single transmitter or a single receiver. This can be achieved in systems that require all communications to pass through a base-station, such as in mobile telephone networks. However, it cannot be achieved satisfactorily in CNR nets.

3.3.2.1.6 Protection against ES

As shown earlier, the use of DSSS spreads the power of a transmitted signal over a large band. This spreading increases the difficulty of detecting the signal. Typically, a DSSS signal cannot be detected by a narrow-band search receiver. Detection by a wide-band search receiver can sometimes be achieved by measurement of power levels across a wide band of frequencies.

A DSSS transmitter provides two types of protection against DF. First, a DSSS signal must be detected before direction-finding techniques can be applied. Second, a DSSS signal must be separated from other in-band interfering signals (including both DSSS and conventional signals) before DF is possible. DF techniques able to operate on multiple co-channel signals, such as Doppler DF, may be capable of providing this separation internally. For widely spaced transmitters, removal of these interfering signals may be achieved by the use of directional antennas. For conventional interfering signals, the use of narrow-band excision may also be an option.

Signal interception is hindered both by the difficulty of detection and by the fact that received chips need to be despread before decoding. This can only be achieved if the spreading PN sequence is known or can be inferred from the received data. Military systems are usually designed with very long PN sequences to maximise the difficulty of intercept. Commercial systems, on the other hand, tend to use shorter spreading sequences, which may be known in advance or easily inferable from the received signal.

In conventional half-duplex communications systems, a user community (or net) consists of those stations that share a particular channel. When DSSS is introduced, transmissions on a net are no longer confined to a single frequency, removing this means of identifying user communities.

3.3.2.2 Frequency Hopping

Frequency hopping (FH) is a form of spread-spectrum communications where the transmitter periodically changes the frequency of transmission, as illustrated in Figure 3.14. By knowing the hopping sequence, a receiver follows the changes in frequency and is able to receive the transmission. A non-hopping receiver is unable to receive data transmitted by a hopping transmitter. The effectiveness of frequency hopping relies on having a large set of frequencies in the hop-set and on the pattern of frequency changes appearing to be random.

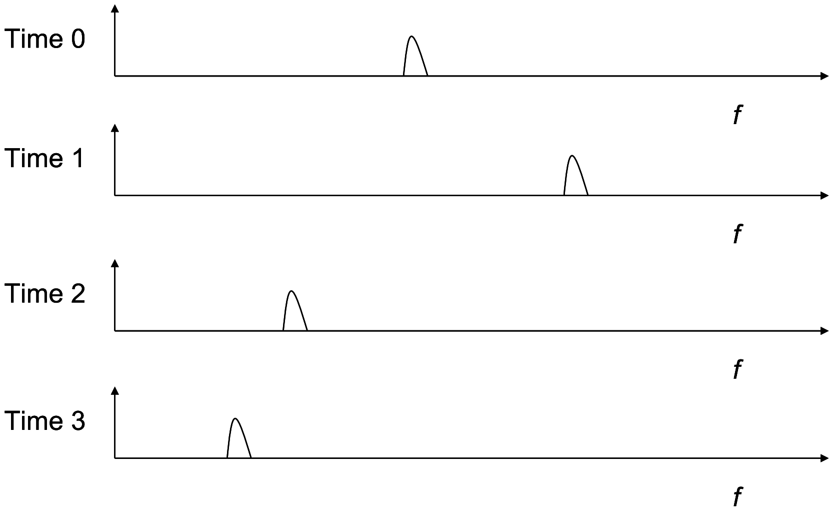

Figure 3.14. Effect of frequency hopping.

In order to provide resistance to jamming, it is necessary that a pseudo-random hop sequence be used. This requires that a receiver synchronise itself to the transmitter, which can be achieved by transmitting a preamble at the beginning of each transmission and possibly transmission of further synchronisation information at regular intervals during the transmission, or using an accurate time reference known to both transmitter and receiver.

The term *hop rate* refers to the number of times per second that a frequency hopping transmitter changes frequency. *Dwell time* is the reciprocal of hop rate and is the time interval in which data is transmitted between consecutive changes of frequency.

The terms *slow* and *fast* hopping are sometimes used. Fast frequency hopping refers either to a hop rate that is higher than the bit rate or to a hop rate significantly faster than 100 hops per second for VHF and UHF transmissions, and 10 hops per second for HF. Slow frequency hopping refers to slower hop rates.

In most frequency hopping systems, there is a *guard interval* during which no information is transmitted while the transmitter changes frequency. This is required because the transmitter's power amplifier cannot instantaneously change frequency. In order to avoid sweeping its power across the band and causing widespread interference, the transmitter stops transmitting during the period of the frequency change.

One of the advantages of frequency hopping is that it is possible to choose the hop set from an arbitrary list of channels. Unlike DSSS, there is usually no requirement for these channels to be adjacent.

Frequency hopping may also be combined with other EP techniques, including DSSS and the use of error correcting codes and interleaving to reduce the impact of errors caused by clashes with other transmissions.

3.3.2.2.1 Resistance to Jamming and Interference

In order to jam a hopping transmission effectively, a jammer must either generate power across a high proportion of the frequencies used (which implies a large total power) or be able to follow the frequency changes. A fixed-frequency spot jammer will have minimal impact on a frequency hopping transmission.

The number of channels in the hop set is analogous to the spreading gain g_s of a DSSS system, and is a measure of the increased difficulty of jamming using jammers that are unable to follow the hopping. The gains that can be achieved with frequency hopping may be much larger than can be achieved with DSSS. It is common, for example, for frequency-hopping VHF CNR to be able to hop across the whole of the 30–88 MHz band.

Effective jamming of a hopping transmission requires that the jamming signal arrive at receiver before end of transmission in one hop. Unless the frequency in use is known in advance, the following sources of delay occur between the beginning of transmission and the jamming signal arriving at the receiver:

- the propagation delay difference between the path from transmitter-jammer-receiver and the direct path from transmitter to receiver:

$$t_{propagation} = \frac{distance_{Tx-J} + distance_{J-Rx} - distance_{Tx-RX}}{3 \times 10^8}$$

- the processing delay at the ES receiver, which is greater than the reciprocal of the receiver bandwidth; and
- the jammer's power-up delay.

Successful jamming requires that the sum of these delays is a small enough proportion of the dwell time that a sufficient portion of the transmitted signal is jammed.

Table 3.1 shows the maximum distances over which it is possible to jam a single hop as part of a frequency-hopping transmission, based on the assumptions that the receiver is close to the transmitter, the length of the guard interval is zero, all delay is due to propagation and the detection time of the receiver (that is the jammer power-up delay is zero), and the jamming is effective if one-third of the hop-time is jammed.

From Table 3.1, it is clear that even for a rate of 100 hops/second (that is a dwell time of 10 ms) the use of satellite jammers is unlikely to be possible. Stand-off airborne or ground-based platforms, however, are likely to be within this range limit. At 10,000 hops per second, stand-off airborne platforms (such as high altitude UAVs) are also infeasible. Jammers, such as UAJ, capable of close-in deployment are the only systems likely to be effective against such high-speed hoppers.

Table 3.1. Maximum path differences (km) over which a frequency-hopping transmission can be jammed.

Hop Rate	Receiver Bandwidth (kHz)			
(hops / sec)	25	50	100	Infinite
100	992	996	998	1,000
500	192	196	198	200
1,000	92	96	98	100
10,000	2	6	8	10

3.3.2.2.2 Provision of Multiple Access

Frequency hopping can also be used as a means of multiple access by allowing several nets to share frequencies in their hop sets. As long as these frequencies are used in a unique sequence by each net, a statistical separation between nets is provided.

3.3.2.2.3 Impact of Overloading

As the number of frequency-hopping transmitters sharing common frequencies increases, the proportion of the time during which two or more transmitters clash on a single frequency increases. Under these circumstances, it is possible that neither signal will be correctly received.

Voice. For voice, loss of data due to clashes causes glitches that may be annoying. The comprehensibility of voice, however, tends to degrade gracefully. This is because even though the voice is digitally encoded and compressed, the human auditory system is quite forgiving of errors introduced in transmission. Voice tends to become unusable only when approximately one third or more of all data is lost due to interference from other hopping or non-hopping signals. Since it is difficult for a jammer to maintain power levels over one third of the hopping band, frequency hopping provides robust voice performance in a hostile electromagnetic environment.

Data. Loss of data due to clashes in the use of a frequency is a particular problem for data communications, especially on slow hoppers. Unlike voice services, quality-of-service can be significantly degraded for data services with interference due to clashes or jamming in only a small proportion of hops. Some systems, such as those used for situational awareness, overcome this problem by providing regular repetition of information. Protection can also be provided using a combination of interleaving and forward error correction.

3.3.2.2.4 Frequency Management

Frequency management for frequency hopping requires the allocation of a hop set to each hopping transmitter. One or more frequencies in this set can be allocated to more than one net, as long as each net is allocated a different hop sequence. In other words, separation between systems can be provided by choice of different frequencies in the hop sets or by the use of the same frequencies in a unique sequence for each net. There is therefore a reduced need for frequency deconfliction between nets, including processes such as harmonic analysis that are an important part of conventional frequency management. There is also no extra management overhead if the capacity allocated to the nets varies.

Interference with non-hopping systems is minimised by excluding frequencies used by these systems from the hop set. The acceptability of these clashes depends on the particular service. Some channels, such as those used for emergency communications, are usually excluded completely from hop sets.

Interference with other hopping systems is minimised by choosing hop-sets with no frequencies in common. This will only be possible, however, on very rare occasions. More commonly, interference is managed by ensuring that the proportion of hops for which two or more hoppers in the same area will share a common frequency does not exceed a quality-of-service threshold. This issue is discussed further in the next section.

3.3.2.2.5 Near-far Effect

Unlike systems using either DSSS or TDMA, frequency-hopping communications are not subject to the near-far effect. This is because no attempt is made to synchronise frequency-hopping transmitters on different nets, and multiple-access using frequency hopping is based on FDMA, which does not require synchronisation.

3.3.2.2.6 Protection against ES

Frequency-hopping transmissions are relatively difficult to detect using narrow-band search receivers. This is because detection only occurs when the frequency of the hopping transmission coincides with the frequency of the scanning receiver. A wide-band receiver is more suitable for detection of frequency hopping transmissions because it can effectively monitor a number of channels simultaneously.

DF of a frequency-hopping transmitter typically requires detection and DF to occur within the dwell time. This suggests that a high level of integration between search and DF is required.

Intercept of a frequency hopping transmission can be achieved by using a multi-channel receiver with a directional antenna. Such systems are most successful where there is only a single frequency-hopping transmitter active in a band at any time, or the frequency hoppers are widely dispersed. Consequently, the LPI properties of frequency hopping are enhanced by the use of multiple frequency hopping nets that share at least some frequencies in their hop sets.

In conventional single-frequency, half-duplex communications systems, a user community (or net) consists of those stations that share a particular channel. When frequency hopping is introduced, transmissions on a net are no longer confined to a single frequency, removing this means of identifying user communities. Frequency-hopping systems, however, that transmit a preamble either on a fixed frequency or in some other identifiable way, may lose this protection.

3.3.3 Comparison of Spread-spectrum Techniques

The advantages of DSSS are that it hinders adversary ES, making transmissions hard to detect above the noise floor; it hinders adversary EA, provides graceful degradation in the presence of jamming and other types of interference; it provides multiple access, known as Code Division Multiple Access (CDMA); and it allows mutual interference to be managed more easily than in frequency hopping.

The disadvantages of DSSS are that the near-far effect makes power management of multiple access in multi-net environment difficult; mutual interference contributes to total jamming power; it provides less efficient multiple access than TDMA or FDMA; and spreading usually occurs over contiguous band (that is, most practical systems do not allow spreading over an arbitrary collection of channels.) In-band spread spectrum has the additional disadvantage of providing only very low data rates.

The advantages of frequency hopping are that hinders adversary ES/EA, the hopping frequencies can be chosen from arbitrary set, the channels used need not be contiguous, and it can be used as a multiple access technique.

The disadvantages of frequency hopping are that hopping nets will usually share some or all of the frequencies in their hop set, resulting in mutual interference between hopping nets and interference with non-hopping nets whose frequencies are included in the hop set of a hopping net; and ES techniques, based on using multi-channel receivers and directional antennas, and EA techniques, based on follower-jammers, exist that can overcome the EP provided by slow-hopping transmitters, especially when used in isolation.

3.3.4 Error Protection Coding

Digital signals passing through transmission channels are subject to errors introduced in the transmission process. While all channels introduce errors, some channels, especially radio channels subject to jamming, will introduce very high error rates. The types of impairments introduced by an imperfect transmission channel include additive noise and channel perturbations. Additive noise may take the form of Gaussian noise with stationary statistics, impulsive noise that is not always stationary or easy to characterise, or jamming. Channel perturbations may occur due to fading in radio channels, synchronisation slip in digital channels, and breaks in transmission of diverse origin.

The likely effects of these channel impairments on a digital signal are one of *uniformly random errors*—errors occurring individually and independently, with approximately uniform probability density, primarily due to noise (often just called *random noise*), *burst errors*—errors grouped in clusters, mainly the result of a combination of noise and channel perturbations, and *erasures*—irregular intervals when it is known that no reliable signal can be detected, because of severe channel perturbation.

Channel coding is used to correct errors caused by these channel impairments through the introduction of controlled redundancy to enable messages corrupted in transmission to be corrected before further processing [9]. With this controlled redundancy, only a subset of all possible transmitted messages (bit sequences) contains valid messages. This subset is called a code, and the valid messages are called *codewords* or *codevectors*. A good code is one in which codewords are so separated that the likelihood of errors corrupting one into another is kept small.

Error detection is simplified to answering this question: is the received message a codeword or not? If it is a codeword, one assumes that no errors have occurred. The probability of an undetected error getting through is then the probability of sufficient errors occurring to transform the real transmitted codeword into another, apparently correct but in reality a false one.

If an error is detected, it can be corrected in principle by *automatic repeat request (ARQ)*, or *forward error correction (FEC)*.

3.3.4.1 Automatic Repeat Request (ARQ)

In ARQ, the recipient rejects the received message as erroneous and requests a repeat transmission. If propagation delays due to distance are large, however, the technique may become so inefficient as to be useless. There are also many cases where retransmission is impossible, such as extracting information from a damaged archive.

3.3.4.2 Forward Error Correction (FEC)

In FEC, the recipient corrects the errors by finding the valid codeword "nearest" to the received message, on the assumption that the nearest is the most likely because few corrupting errors are more likely than many.

There are two types of FEC: *block coding* and *convolutional coding*. In block coding, source data is partitioned into blocks of *k* bits, converted by the encoder into blocks of *n* (>*k*) bits with enough checks to enable the decoder to correct errors of the more probable kinds. Error-correcting codes have more redundancy than error-detecting codes, and the decoding algorithms are much more complex. The most common types of block codes [10] are Cyclic Redundancy Check (CRC) Codes, which provide only error detection; Golay Codes; Bose-Chadhuri-Hocquenghem (BCH) Codes; and Reed-Solomon (RS) Codes. For a convolutional code, the encoder operates not on disjoint blocks, but on a running block of bits held in a shift register, generating a sequence of higher rate. This procedure is normally used for FEC, but the correcting capabilities are not so clear cut as with block codes. Probabilistic decoding, approximating maximum likelihood, is generally used.

Block codes are used when information is naturally structured in blocks, when channel capacity is relatively low and we do not want to waste it further with unnecessarily low code rates, and when quick efficient decoding is required because of limited processing time available.

When long streams of relatively unstructured data are transmitted on high-capacity channels (such as satellite 10 Mbps channels) and when the complexity of the decoder represents a relatively small proportion of the total cost of the receiving equipment (such as a satellite receiver), then convolutional codes can offer the best error-correcting solutions.

3.3.4.3 Interleaving

Error correcting codes can be used to detect and correct random bit errors. The codes are effective so long as the number of errors close together remains small. In many types of channel, especially radio channels, however, the channel errors occur in bursts of many errors followed by long periods with almost no errors.

The problem of bursty channel errors can be overcome by interleaving the transmitted data. This is achieved by rearranging the coded data at the transmitter in a predefined pseudorandom order. This means that a burst of errors will be randomised at the receiver when the bits are placed back in their original order.

3.3.4.4 Concatenated Codes

Concatenated codes use two levels of coding—an inner code and outer code—to achieve the desired error performance. As illustrated in Figure 3.15, the inner code is configured to correct most channel errors; the outer code reduces the probability of error to an acceptable level.

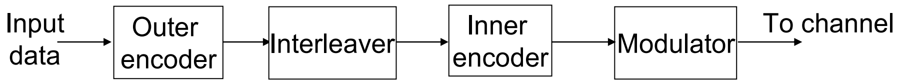

Figure 3.15. Block diagram of a concatenated coder.

One of the most popular systems uses a convolutional inner code and a Reed-Solomon outer code. The Reed-Solomon coder is chosen because it can operate on symbols that consist of a number of bits. Like other FEC, it operates best on isolated symbol errors. Because the symbols may consist of a number of bits, the Reed-Solomon coder is quite effective at correcting bursts of bit errors.

3.3.5 Burst Transmission

Many communications systems transmit continuously, making them easy targets for adversary ES, especially DF, and EA. Even systems that only transmit when they have data to send have traditionally used voice transmission, resulting in lengthy transmissions that once again present good targets to adversary ES and EA.

The term *burst transmission* is used to refer to systems that provide protection against ES and EA by transmitting for short periods only when they have data to pass. At its simplest, burst transmission may be used to describe the operation of a data-enabled CNR system. More sophisticated covert communications systems based on burst transmission use the combination of high data rate transmission and low transmission time as a means of frequency spreading. This may be used in conjunction with other EP techniques, such as error protection, spread spectrum, and encryption.

The effectiveness of the burst transmission as a form of EP is controlled by the length of a burst and the predictability of its transmission. The length of the burst depends on the amount of data to be transmitted, overheads such as error protection, the transmit data rate, and the length of any preambles required for synchronisation. Parameters associated with the predictability of the transmission include the time of start, duration, carrier frequency, code (if DSSS is used), and bandwidth of the transmission.

The effectiveness of burst transmission can be increased by delays in handing over targets within the EW system. For example, in a system with separate search and DF systems, a burst transmission may be over before the DF has even received the target information. Because of the short transmission times, similar constraints to those discussed for frequency hopping apply to the maximum range over which a jammer can be effective against burst transmissions.

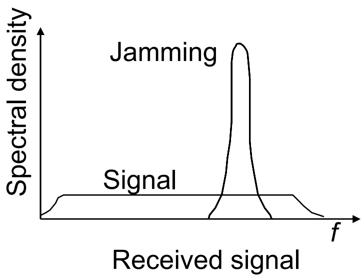

Figure 3.16. Narrow-band jamming of a wide-band signal.

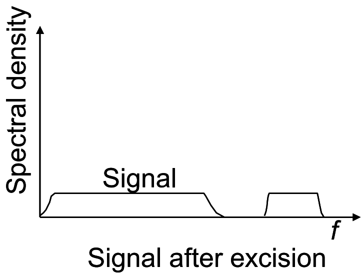

Figure 3.17. Signal after narrow-band excision.

3.3.6 Narrow-band Excision

A jammer may sometimes transmit in only a portion of the band being used for communications. This is most likely to happen in higher capacity channels, such as those used for radio relay or DSSS signals. This is illustrated in Figure 3.16. Such jamming can be effective against conventional receivers. Even for a DSSS receiver, the power of the jamming signal is turned into noise in the demodulation process and therefore does have some effect on the reception of the signal.

In a receiver employing narrow-band excision, narrow-band jamming is detected and removed from the signal before it is passed to the demodulator as illustrated in Figure 3.17. While this also removes any information in the excised band, the overall effect is beneficial because the jammer power is prevented from having any impact on the demodulation process. Because the loss of some portion of the received signal is a necessary side-effect of narrow-band excision, some means for correcting the resulting errors is usually required.

3.3.7 Diversity

Diversity is a means of protecting against jamming and interference by transmitting data over two or more channels [11]. There are three types of diversity commonly used in communications systems: *space diversity*, *frequency diversity*, and *time diversity*.

Space diversity. The impact of narrow-band fading in a communications channel can change significantly when the location of the receiver's antenna is moved by more than half the wavelength of the signal. In space diversity, two or more receive antennas are placed more than half a wavelength apart, effectively providing two channels between transmitter and receiver. This type of diversity is commonly used in microwave transmission systems.

Frequency diversity. By transmitting data on two or more different frequencies, the impact of fading or jamming and interference on one of the channels can be overcome. This type of diversity is used in HF skywave communications, including TADIL-A (Link-11) [12].

Time diversity. Data can be transmitted twice on the same channel, protecting against short-term jamming and interference.

3.4 USE OF EP TECHNIQUES IN COMMUNICATIONS SYSTEMS

Many military and commercial communications systems employ one or more EP techniques. In this section, a selection of these systems is reviewed, highlighting the differences between the military and commercial use.

3.4.1 CNR

VHF CNR typically operates in the frequency range 30–88 MHz. Modern CNR systems provide both secure voice and secure data capabilities. Most systems, such as the US SINCGARS, also provide an in-built frequency-hopping capability. In some radios, the frequency hopping is provided by an add-on appliqué unit. Free-channel search is also found in some systems.

CNR does not usually employ DSSS because the use of DSSS would require that channels much larger than the conventional 25 kHz are allocated to each net, reducing the overall capacity in the 30–88 MHz band; and the near-far effect prevents the effective use of CDMA in CNR to improve the efficiency of use of the electromagnetic spectrum.

Encryption is commonly provided either using in-built systems or an appliqué. Traditionally, such encryption has been used at battalion and higher levels, leaving lower-level transmissions open to intercept. Increasingly, encryption is being pushed down to the lowest levels.

Because the encryption used in CNR is message-based, the synchronising preambles of these transmissions are particularly vulnerable to jamming. Adversary EA may deliberately jam preambles to force nets to operate in plaintext, allowing their transmissions to be intercepted.

Error protection is not commonly used for voice transmissions in CNR. The digital voice coding algorithms used tend to provide very high levels of robustness against transmission errors, operating satisfactorily with bit error rates as high as 10%. However, some form of error protection may be provided for data.

3.4.2 Military Radio Relay

Military radio relay systems operate in the VHF/UHF bands above 200 MHz. A network is formed from a number of point-to-point links that interconnect nodes that perform switching. Traditionally, these systems have provided circuit-switched voice and data services.

Because they are based on point-to-point links, radio-relay systems almost always use directional antennas. The gain of these antennas is typically around 10 dB. These directional antennas provide a high level of protection against adversary EA and ES.

Encryption in radio-relay networks is based on bulk encryption of the point-to-point links, with switching occurring on plaintext data, which protects against vulnerabilities associated with the restarting of cryptographic algorithms in message-based encryption. Frequency hopping and DSSS transmission are also sometimes employed in these systems to provide additional protection. Additionally, many radio-relay systems, especially those that provide for the carriage of data as well as voice, provide some form of error protection, which is commonly based on a half-rate convolutional code.

3.4.3 TADIL-J (Link-16)

TADIL-J is a secure, high capacity, jam-resistant, nodeless data link which uses the Joint Tactical Information Distribution System (JTIDS) transmission characteristics and the protocols, conventions, and fixed-length message formats defined by the JTIDS Technical Interface Design Plan (TIDP) [13]. TADIL-J operates in the UHF band in the frequency range 960-1215 MHz, and therefore provides line-of-sight operation. Operation beyond line-of-sight can be achieved by means of a relay, which may be an airborne or satellite-mounted system.

TADIL-J operation is based on all-informed nets. Multiple access between nets is provided by a combination of frequency hopping, FDMA and

CDMA. 51 channels are supported. Multiple access within a net is provided by TDMA. The TDMA structure is shown in Figure 3.18. *Time slots* of 7.8125 ms are allocated to stations on the net. 1,536 time slots make up a *time frame*, and 64 time frames form an *epoch*. Each station on the net is allocated at least one time slot per epoch.

Table 3.2 shows the TADIL-J maximum range and data rates, which depend on the operating mode.

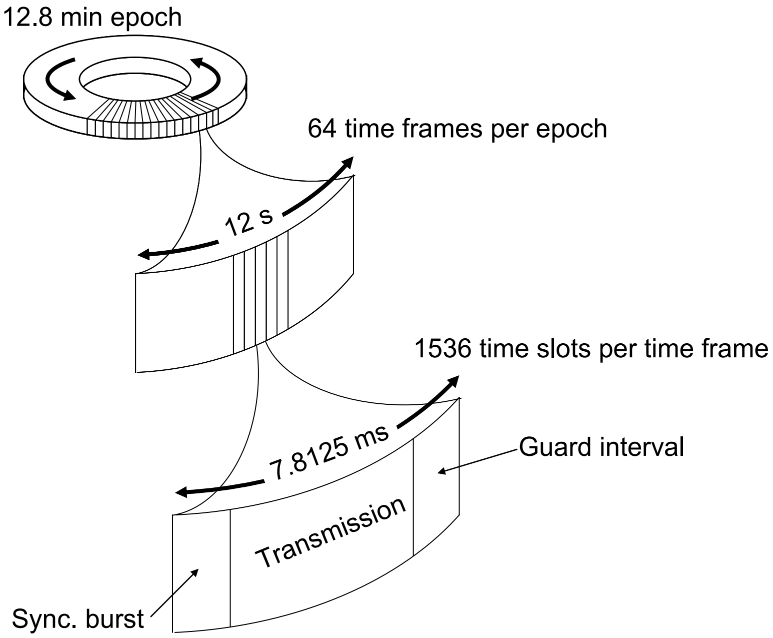

Figure 3.18. TADIL-J time-slot structure.

Table 3.2 . TADIL-J operating modes.

Mode	Guard Interval (ms)	Guard Interval Range Limit (nm)	Throughput After Error Correction (kbps)	Hops / second
Standard Full Slot	4.4585	700	30	33,000
Packed-2 Full Slot	4.4585	700	59	33,000
Packed-4 Full Slot	2.0405	300	119	57,000

EP in TADIL-J is provided by a combination of frequency hopping with an instantaneous hop rate of 77,000 hops per second over 51 frequencies, direct-sequence spread spectrum with a spreading gain of 6.4 and a chip rate of 5 MHz, repeated transmission with data optionally transmitted twice in successive hops, and forward error detection and correction, using a (31,15) Reed-Solomon code.

In each hop, the transmitter is turned on for 6.4 μs, which means that power from a jammer with transmitter-jammer-receiver path length 2 km longer than the transmitter-receiver path length will reach the receiver after the end of the data transmission.

3.4.4 Enhanced Position Locating and Reporting System (EPLRS)

EPLRS is a US situational awareness system that is designed to provide services for position location, navigation, identification, and communications. EPLRS also supports a number of control measures such as boundaries, fire support coordination lines, limits of advance routes, passage lanes, and attack directions.

The EPLRS radio supports a variety of data communications services [14], providing both point-to-point links and an extensive multi-cast capability, including all-informed nets. Data rates up to 57,600 bps per connection, known as a *needline*, are possible. Each EPLRS user community has a maximum practical data capacity of between 300 and 450 kbps, depending on configuration. This capacity is reduced when retransmission is required. Capacity is also reduced when the area over which the user community increases, because the requirement for larger guard intervals between TDMA slots.

Frequencies in the range 420–450 MHz are used, with the band being segmented into eight channels, each of 3 MHz bandwidth. Multiple access within a net is provided by TDMA technology, in which users transmit information in bursts during pre-determined time slots. Multiple access between nets is provided by a combination of FDMA, frequency hopping, and CDMA.

Resistance to jamming is provided through DSSS transmission with a spreading gain of approximately five, frequency hopping operation among eight channels with a hop rate of 512 Hz, error detection and correction, and network management that facilitates the automatic routing and re-routing of messages in the EPLRS network using any EPLRS radio as a relay of opportunity.

In each hop, the transmitter is turned on for up to 1.1 ms, which means that the transmitter-jammer-receiver path length must be no more than 33 km longer than the transmitter-receiver path length if jamming is to be effective.

The combination of DSSS and frequency hopping also provides LPI. Security is provided by an embedded cryptographic system. While the use of DSSS provides a multiple-access capability, the near-far effect will limit its efficiency. The use of DSSS also provides protection against interference from other EPLRS nets. This would otherwise be a significant problem because only eight channels are available among which the transmitter can hop.

3.4.5 NTDR

The Near-term Digital Radio (NTDR) is an experimental system being developed by the US Army under the Force XXI program to explore the limits of near-term technology and to provide a technical baseline for development of a multi-band, multi-mode digital radio system.

The NTDR can be viewed as an RF system with an embedded router/gateway such as those found in fixed local area networks. The NTDR transports up to 288 kbps of user information for each cluster of users, backbone channel, or point-to-point connection for the operating frequency range of 225–450 MHz with a channel bandwidth of 4 MHz.

EP will be provided by a combination of DSSS, fast frequency hopping, and narrow-band excision at receivers to eliminate effects of narrow-band jamming. Further protection against error will be provided by three-quarter-rate convolutional coding. Once again, the combination of DSSS and frequency hopping is designed to minimise detectability of signals. The use of narrow-band excision allows jamming signals from narrow-band jammers to be removed before despreading, reducing even further the impact of such signals.

3.4.6 IS-95

IS-95 is an air-interface standard for cellular telephony. It uses a combination of CDMA and FDMA to provide multiple access on both downlinks (forward channels) and uplinks (reverse channels).

Data on the forward channel is grouped into 20 ms frames. This data is convolutionally encoded, repeated if necessary to increase the data rate to 19.2 kilosamples per second (ksps) and interleaved, as illustrated in Figure 3.19. The signal is randomised with a long PN sequence and spread with a Walsh code to produce a 1.2288 megachips per second (Mcps) signal.

Power control information is inserted every 1.25 ms by puncturing. Mobile terminal transmit power is adjusted in 1 dB steps. This high-rate, fine adjustment of transmit power is required to provide power balancing between mobile stations, and to maximise the bandwidth efficiency of the system.

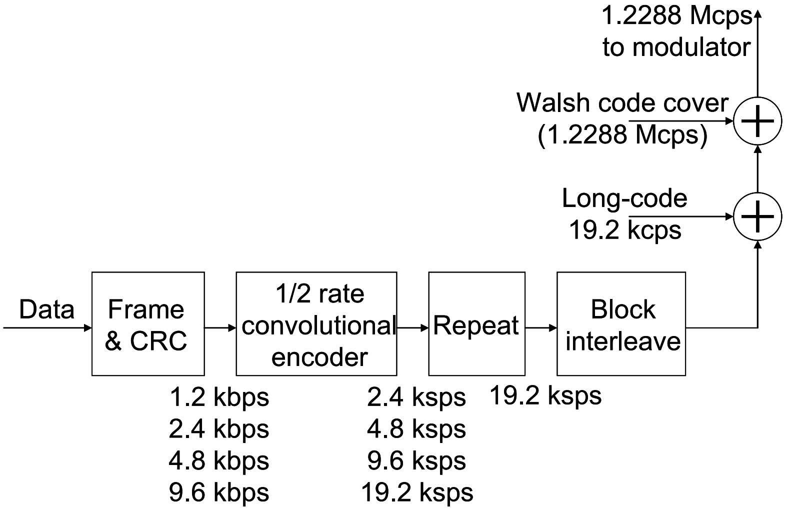

Figure 3.19. Downlink processing for IS-95.

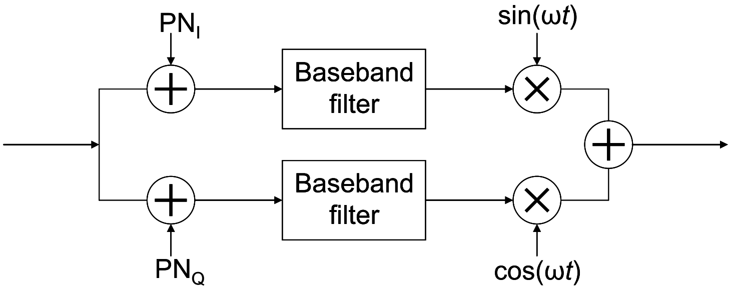

Figure 3.20. Downlink modulation for IS-95.

Quadrature modulation is performed as shown in Figure 3.20, with in-phase and quadrature components having an orthogonal covering applied before modulation. At the receiver, this makes the received components approximately independent. The covering is performed with a short code that is relatively easy for a receiver to acquire.

The use of DSSS in IS-95 is purely intended to provide multiple access. Because the PN sequences are known or easily deducible, IS-95 does not provide an LPI or anti-jam capability, except against a very unsophisticated attack. The use of high levels of forward error correction is intended to overcome the noise introduced by interfering signals, both narrow-band and wide-band.

3.4.7 GSM

The GSM digital cellular telephone system provides multiple access using a combination of FDMA and TDMA. Eight TMDA channels are multiplexed onto a carrier with a channel bandwidth of 200 kHz. Each time-slot contains 114 bits of user data [15].

GSM provides an optional frequency-hopping mode. This mode does not provide an LPI or anti-jam capability, because the specification for the hop sequence is published in the GSM standards, and the hop sequence can therefore be deduced from the signals transmitted by a base-station.

Frequency hopping in GSM does, however, provide frequency diversity. This diversity is intended to minimise the impact of multipath propagation, which may lead to much higher losses in some channels than in others. Because GSM was not designed for military use, no extra benefit was perceived for LPI or anti-jam capabilities.

Error protection in GSM takes 240 bit blocks of data, and codes them with a half-rate punctured convolutional code to produce 456 bits that are interleaved across four 114-bit TDMA frames. This interleaving spreads burst errors (that are caused largely by channel fading) over a longer period, reducing the reduce peak bit error rate, and allows the channel coding to correct the (now) randomly spaced bit errors.

Encryption in GSM is based on a proprietary, stream-cipher algorithm, known as A5. A5 comes in two variants: A5/1 is used in European systems and A5/2 (which is known to provide a significantly lower level of security) is used in export systems. A5 is a stream cipher whose state is re-initialised at the beginning of every TDMA time-slot. Its vulnerabilities include [16] the fact that in most deployed versions of GSM, the 10 least significant bits of the key are set to zero, reducing the effective length of the key to 54 bits; the keystream is frequently re-initialised, permitting attacks based on a known initial state; while the state transition function of A5 is not uniquely invertible, it can be efficiently inverted because the number of possible parent states is small; and cryptanalysis of A5/1 requires approximately 2^{24} operations (with 2^{48} pre-computed stored values), while cryptanalysis of A5/2 requires only 2^{16} operations.

3.5 ENDNOTES

[1] US doctine for EP is contained in U.S. Army Field Manual FM 24-33 "Communications Techniques: Electronic Counter-Countermeasures", July 1990.

[2] *Electromagnetic Pulse (EMP) and TEMPEST Protection for Facilities,* Engineering and Design Pamphlet EP 1110-3-2, U.S. Army Corps of Engineers, Dec. 1990.

[3] Sources of information on encryption techniques include:
Denning, D. E., *Cryptography and Data Security*, Reading, MA: Addison Wesley, 1983;
Schneier, B., *Applied Cryptography: Protocols, Algorithms and Source Code in C*, New York: Wiley, 1994;
Singh, S., *The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, New York : Anchor Books, 1999;
Sinkov, A., *Elementary Cryptanalysis, a Mathematical Approach*, The Mathematical Association of America, 1966;
Stallings, S., *Network and Internetwork Security*, 2nd Edition, Englewood Cliffs, NJ: Prentice Hall, 1995; and
Torrieri, D. J., *Principles of Secure Communications*, Norwood, MA: Artech House, 1985.

[4] *SKIPJACK and KEA Algorithm Specifications*, Version 2, National Security Agency, May 1998.

[5] Biryukov, A., Shamir, A., and Wagner, D., "Real Time Cryptanalysis of A5/1 on a PC", *Fast Encryption Software Workshop 2000*, New York City, April 2000.

[6] Stallings, S., *Network and Internetwork Security*, 2nd Edition, Englewood Cliffs, NJ: Prentice Hall, 1995.

[7] *SKIPJACK and KEA Algorithm Specifications*, Version 2, National Security Agency, May 1998.

[8] See, for example, Simon, M. K., *Spread Spectrum Communications*, Rockville, Md: Computer Science Press, 1985; or Nicholson, D. L., *Spread Spectrum Signal Design : LPE & AJ systems*, Rockville, Md: Computer Science Press, 1988.

[9] See, for example, Sklar, B., *Digital Communications*, Englewood Cliffs, NJ: Prentice-Hall, 1988; and Proakis, J. G., *Digital Communications*, New York: McGraw-Hill, 2nd Edition, 1989.

[10] See, for example:
Sklar, B., *Digital Communications*, Englewood Cliffs, NJ: Prentice-Hall, 1988; and Proakis, J. G., *Digital Communications*, New York : McGraw-Hill, 2nd Edition, 1989.

[11] See, for example:
Gibilisco, S., *Handbook of Radio and Wireless Technology*, New York: McGraw Hill, 1999, pp. 252-253; and ITU-R, Recommendation F.106-2, 1999.

[12] *MIL-STD-188-203-1A—Interoperability and Performance Standards for Tactical Digital Information Link, (TADIL) A*, Jan. 1988.

[13] See, for example:
Stiglitz, M., "The Joint Tactical Information Distribution System", *Microwave J.*, Oct. 1987;
"JTIDS/TIES Consolidate Tactical Communications", *EW*, Sep./Oct. 1977;
Toone, J. and S. Titmas, "Introduction to JTIDS", *Signal*, Aug. 1987, pp. 55-59; and

MIL-STD-6016 “DoD Interface Standard Tactical Digital Interface Link (TADIL) J Message Standard”, Feb. 1997.

14 U.S. Army Field Manual FM 24-41 “Tactics, Techniques, and Procedures for the Enhanced Position Location Reporting System (EPLRS)”, Final Draft, July 1999.

15 Mouly, M. and Pautet, M., *The GSM Systems for Mobile Communications*, Palaiseau: Cell and Sys, 1992.

16 Biryukov, A., Shamir, A., and Wagner, D., “Real Time Cryptanalysis of A5/1 on a PC”, *Fast Encryption Software Workshop 2000*, New York City, April 2000.