MILITARY COMMUNICATION

In general, military communications systems are different from ordinary systems in various specific security requirements, namely, robustness in hostile environments, shielding from adversaries, and immunity from unfriendly eavesdropping.

Hostile environments to communications are radio frequency interference (RFI), spoofing, jamming, and fading, either natural or human-made. RFI is unintentional but can significantly degrade performance. Spoofing is intentional and can cause a great deal of confusion. Jamming is also intentional and can completely shut down the entire communication. Fading can severely disrupt communications. A conventional communication system is not able to survive in such hostile environments. All spread-spectrum schemes can be utilized for counterattacking the measurements from spoofer and jammer. A good military communication system generally requires the addition of an antenna nulling technique that can isolate the effect of an intentional jammer or spoofer. Techniques such as channel interleaving can be employed to "whiten" the channel in the presence of fading to reduce their efficacy. Other schemes such as channel coding, diversity, or equalization are also important to make a system robust under a jamming or a fading environment.

The requirement of shielding from adversaries refers to the ability of not being detected by enemies. In modern warfare, using electronic equipment for communication, position location, and so on, is crucial for tactical movement, combat, evasion, and rescue. However, an adversary can detect the signal that is intended for the friendly party. Consequently, the location of a soldier or a command post can be identified and life can be jeopardized. Therefore, low probability of detect (LPD) or low probability of intercept (LPI) becomes critical for designing military systems.

Eavesdropping is a technique used to surreptitiously intercept intelligence information from an enemy. This can always change the outcome of a battle or a war. Unlike detecting the existence of a signal, which can usually be achieved by using a radiometer, eavesdropping requires the right demodulator, decoder, and so on. In order to be immune to eavesdropping, in addition to sophisticated spread-spectrum techniques, such as direct sequence, frequency hopping, and time hopping, a system needs a cryptography technique to ensure the secrecy of communications.

Other important areas in military communications include target recognition (classification) and navigation. Target recognition involves a great deal of data collection and processing. Optical remote sensing methods, such as optical lenses, laser or infrared light, is always a way of collecting target images. However, in poor weather conditions, it can be difficult if not impossible to obtain any image using optical equipment. In recent years, synthetic aperture radar (SAR) has been extensively utilized for remote sensing. Besides providing better quality and resolution of the image, the SAR system can be operated regardless of the weather condition.

The global positioning system (GPS) is a satellite-based navigation system with global coverage. In view of four GPS satellites, a GPS receiver can determine its three-dimensional position to an accuracy of better than 16 m. Greater accuracy of less than 1 meter can be achieved by using correction information from another GPS receiver at a known location. The Persian Gulf region, with its wide expanses of featureless desert, is the ideal combat environment in which to prove the value of GPS. Without a reliable navigation system like GPS, the U.S. forces could not have performed the maneuvers that contributed to the success of Operation Desert Storm in 1991.

UNINTENTIONAL INTERFERENCE

The radio frequency interference (RFI) from another unintentional interferer can be substantial in a multiuser, multiservice communication system. RFI can penetrate the receiver from main, side, or back lobes of the receiving antenna, resulting in significant performance degradation. From the spectral point of view, the RFI can be located within the intended receiving bandwidth, referred to as the co-channel interference (CCI), or leaked from the adjacent channels, referred to as the adjacent channel interference (ACI).

The CCI can be initiated from intermodulations, leakage from spatial discriminated co-channel signals, and code division multiple access (CDMA) scenarios, such as direct sequence spreading and frequency hopping (to be discussed later). In general, making use of channel coding to enhance the power efficiency of the desired signal can mitigate the CCI problem.

The ACI is caused by leakage of the signal power from adjacent channels next to the desired signal bandwidth. This leakage exists because no ideal brick-wall filter, which passes 100% of the signal power within a certain range of frequencies and also completely cuts off the power beyond this range, can be realized. Thus, portions of the power spectra of adjacent channels overlap each other, resulting in leakage. In addition to the channel coding, the mitigation technique for the ACI rejection includes the adoption of a bandwidth-efficient modulation scheme, such as Gaussian minimum shift keying (GMSK) or filtered phase shift keying (FPSK), which basically has a confined power spectrum with no side lobes.

SPOOFING

Spoofing is defined as the purposeful degradation, denial, or deception to a receiver by an external source using a "look-alike" signal. Spoofing can cause greater damage than other intentional interference, such as jamming, because armed forces personnel may make a costly or deadly mistake in response to a deceived command without knowing it.

JAMMING

A jammer is a device that seeks to nullify a communication system by inserting energy into the target spectrum. The jammer power at the target antenna system can be represented by

$$J = P_j G_j / (4\pi R_j^2) B_{s/j} / L_j \tag{1}$$

where

J = jammer power at target antenna
P_j = RF power delivered to the jammer antenna
G_j = gain of the jammer antenna
R_j = range from jammer to target antenna
$B_{s/j}$ = ratio between the bandwidth overlap between the energy inserted into the target spectrum and the jammer's transmitted spectrum
L_j = losses in propagation between jammer and target antenna

To be effective, the jammer must act to lower the SNR, and hence the E_b/N_{total}, to raise the bit error rate (BER) of the communication system beyond acceptable levels:

$$E_b/N_{total} = E_b/(N_0 + J_0) = [(1/E_b/N_0) + (1/E_b/J_0)]^{-1} \tag{2}$$

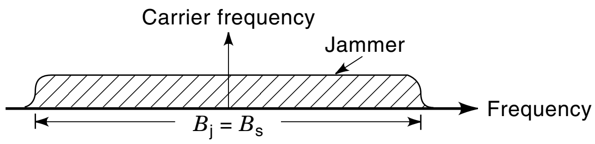

Figure 1. Spectrum of a broadband noise jammer.

where E_b is the signal energy per bit, J_0 is the jamming energy per bit, and N_0 is the one-sided power spectral density of the received additive white Gaussian noise (AWGN).

A measure of jammer power versus signal power is

$$J/S = (P_j G_j)/(P_t G_t)(B_{s/j})(R_t/R_j)^2(L_a/L_j) \tag{3}$$

where

S = signal power at antenna
P_t = power delivered to transmit antenna
G_t = gain of the transmit antenna
R_t = range from transmit to receive antenna
L_a = losses in propagation between transmit and receive antenna

If there are differences in range between the communications transmitter and jammer from the receive antenna, a stand-off distance can be computed for a known J/S value where the jammer becomes ineffective:

$$\text{Stand-off distance} = R_t[(P_j G_j)/(P_t G_t)(S/J)(B_{s/j})(L_a/L_j)]^{1/2} \tag{4}$$

The jammer nominally attempts to disrupt communications with minimal resource use; that is, for a given total power it will maximize jamming energy at the detector. The jammer can use several waveform strategies to maximize its effectiveness and reduce E_b/J_0.

Broadband Noise Jamming

A broadband noise jammer, as shown in Fig. 1, employs a noise source of bandwidth B_j that covers the entire allocated spectrum B_s of the communication system under attack. The noise density is

$$\text{Noise density} = J/B_j = J_0 \qquad (B_j = B_s) \tag{5}$$

Partial-Band Noise Jamming

A partial-band noise jammer (PBNJ), as shown in Fig. 2, employs a noise source that covers some fraction α of the allocated spectrum of the communication systems under attack. For a given jammer power J, this raises the noise density over that part of the band:

$$\text{Noise density} = J/B_j = J/(\alpha B_s) = J_0 \qquad (B_j < B_s) \tag{6}$$

Worst-Case Partial-Band Jamming

A worst-case partial band jammer (WCPBJ) is employed against a system whose instantaneous bandwidth is less than allocated spectrum, $B_j = \beta B_s$. One must compute the joint probability of likely coincidence, ρ_0, with the waveform and noncoincidence, $(1 - \rho_0)$, to obtain statistics of BER. The WCPBJ would attempt to vary the value of ρ_0, the fraction of bandwidth occupied, to maximize BER in the joint probability computation.

Multitone Jamming

A multitone jammer, as shown in Fig. 3, employs sets of sinusoids instead of noise sources to cover the jamming band. Generally these are generated by a harmonic source, resulting in frequency spacings that are equidistant. The power per tone for the equal amplitude case is

$$P_j = J/N \tag{7}$$

where N is the number of tones. For the case of equidistant frequency tones, the total jamming bandwidth occupied is

$$B_j = f_s(N - 1) \tag{8}$$

where f_s is the frequency spacing.

Pulsed Jamming

A pulsed jammer, as shown in Fig. 4, seeks to obtain a high instantaneous power output by reducing its duty cycle; that is, the power production is for a fraction of time. Some microwave tubes have the ability to produce large amounts of instantaneous but not continuous power. The source waveform for small duty cycles is generally rectangular—that is, a pulse, which is rich in harmonics and can cover a wide instantaneous bandwidth.

Smart Jammers

The category of smart jammers includes the frequency follower, the store and forward, and frequency chirp jammers.

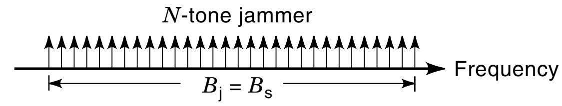

Figure 3. Spectrum of a multitone jammer.

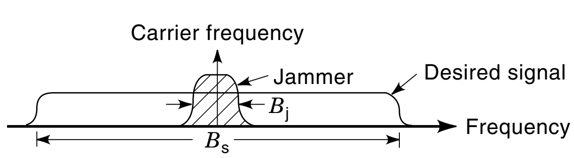

Figure 2. Spectrum of a partial-band jammer.

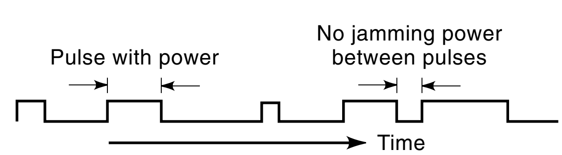

Figure 4. A pulsed jammer in time domain.

The frequency follower and the store-and-forward class of jammers is nominally frequency-agile and captures or senses the victim signal and mimics the carrier frequency and perhaps the modulated waveform. These jammers are effective against stationary or slow frequency hoppers where the signal stays at frequency long enough for the jammer to copy and transmit to the victim in one frequency hop period.

The frequency chirp jammer, as its name implies, frequency sweeps or chirps the intended jamming band to put energy into the victim receiving system. These jammers would be employed if certain aspects of the victim system are known and can be exploited by a nonstationary signal.

ANTISPOOFING AND ANTIJAMMING TECHNIQUES

To make a system robust in hostile environments, antispoofing and antijamming techniques need to be implemented. Different techniques should be adopted to counterattack different types of jamming. They can be based on the concepts of power, frequency, time, and spatial discriminations. In most cases, a hybrid system that includes more than one antijamming technique is implemented. All techniques described here can be used for antispoofing purposes as well without being particularly specified in the context.

Direct Sequence

Direct sequence (DS) is a spread-spectrum technique that is usually used with the phase-shift-keying (PSK) signaling. A pseudorandom (PN) binary sequence whose elements have values of +1 or −1 are generated by a PN sequence generator N_c times faster than the data rate. Conventionally, the unit of each element of a PN sequence is called a "chip." Therefore, the chip time T_c equals T_d/N_c, where T_d is the data bit duration. Practically, the N can be between 100 and 10^6 or higher, depending on the capability of antijamming (antispoofing) and/or the spread bandwidth of the system. Let $d(t)$ and $c(t)$ be denoted as the original data and PN sequence, respectively. Then

$$d(t) = \sum_{k=-\infty}^{\infty} d_k p_d(t) \tag{9}$$

and

$$c(t) = \sum_{k=-\infty}^{\infty} c_k p_c(t) \tag{10}$$

where d_k and c_k are either +1 or −1, and $p_d(t)$ and $p_c(t)$ are unit pulse functions with duration T_d and T_c, respectively. In the DS spread PSK system, the modulating signal is the multiplication of $d(t)$ and $c(t)$. Figure 5 illustrates the waveforms of $d(t)$, $c(t)$, and $d(t)c(t)$.

The DS spread binary PSK (DS/BPSK) signal can be expressed as

$$x(t) = \sqrt{2S}d(t)c(t)\cos\omega_c t = c(t)s(t) \tag{11}$$

where

$$s(t) = \sqrt{2S}d(t)\cos\omega_c t \tag{12}$$

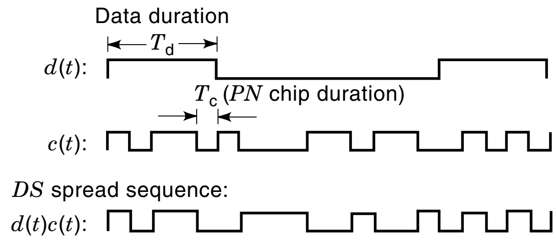

Figure 5. Waveforms of data $d(t)$, PN sequence $c(t)$, and modulating signal $d(t)c(t)$.

is the ordinary BPSK signaling. Since $c(t)$ changes its polarity N_c times faster than $d(t)$, the bandwidth of $x(t)$, denoted by W_{DS}, is N_c times wider than that of $d(t)$, which is R_d (= $1/T_d$). The processing gain of this DS/BPSK system is simply

$$\mathrm{PG} = \frac{W_{DS}}{R_d} = N_c \tag{13}$$

In the presence of jamming signal $J(t)$, the received signal at the receiver can be represented by

$$r(t) = x(t) + J(t) \tag{14}$$

The receiver multiplies the received signal $r(t)$ by a duplicate of the PN signal $c(t)$ to obtain

$$z(t) = c(t)(x(t) + J(t)) = s(t) + c(t)J(t) \tag{15}$$

since $c^2(t) = 1$. Therefore, the effective noise component at the input to the BPSK demodulator becomes $n(t) = c(t)J(t)$. Again, for the case that jammer's bandwidth B_J is much smaller than $R_c = 1/T_c$, the bandwidth of $n(t)$ will be approximately N_J (= R_c/B_J) times wider than that of $J(t)$. For a fixed amount of jammer power J, the value of the power spectrum density function of $n(t)$ at the carrier frequency ω_0 is approximately $1/N_J$ that of $J(t)$. As a result of this, after the signal $z(t)$ passes through the front-end filter of the BPSK demodulator, which is approximately R_d, the effective noise component contributed to the decision rule is significantly reduced. Hence, this technique essentially enhances the effective SNR input to the demodulator. This implies that the direct-sequence spread-spectrum approach is based on the concept of power discrimination.

It has been shown (1) that the BPSK data modulation with QPSK direct sequence spreading is a robust antijamming system to combat either continuous-wave (tone) or random (partial-band) jammer.

It is worthwhile to mention that the DS technique can be also used for the purpose of multiple access. The multiple access scheme that adopts the DS technique is called code division multiple access (CDMA). Other types of multiple access include frequency division multiple access (FDMA) and time division multiple access (TDMA). In a CDMA system, users each have their own unique code ID. The same idea of using process gain stated early in this section is the concept used to discriminate the unwanted user from the desired one.

Frequency Hopping

A frequency hopping (FH) system is driven by a frequency synthesizer that responds to a PN sequence from a PN code

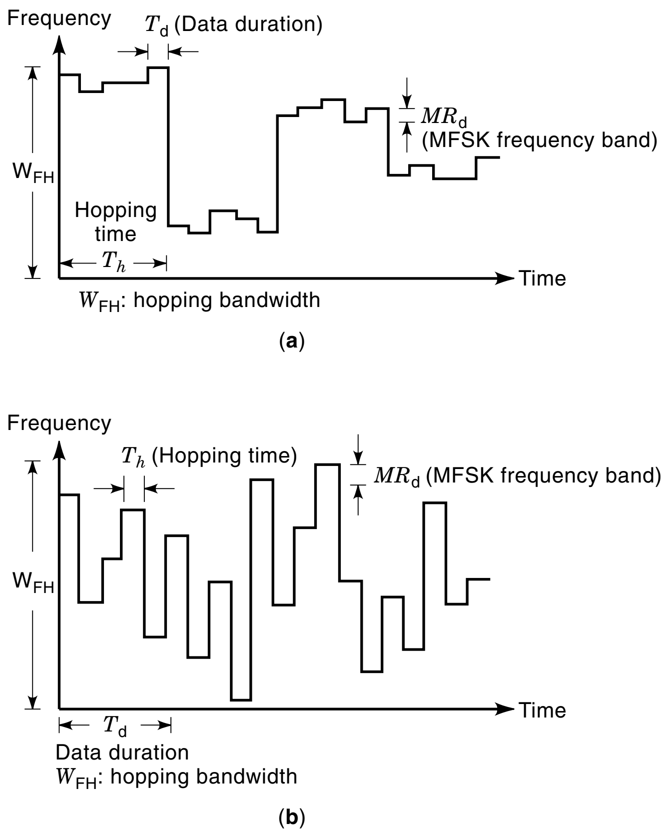

Figure 6. (a) Slow frequency hopping. (b) Fast frequency hopping.

generator. The most commonly used modulation schemes when the FH technique is adopted are M-ary frequency-shift-keying (MFSK) modulations. Based on the output sequence from a PN code generator, the frequency hopper outputs a continuous sinusoidal waveform that frequency jumps from one value to another. These frequencies are, in turn, used as the carrier frequencies of a MFSK signal.

Depending on the hopping rate that the frequency changes, the FH system can be categorized into slow frequency hopping (SFH) and fast frequency hopping (FFH).

- *Slow Frequency Hop.* The hopping rate is slower than or equal to the date rate, which implies that there are one or more data bits in each hop, as shown in Fig. 6(a).
- *Fast Frequency Hop.* The hopping rate is faster than the data rate, which implies that there are multiple hops within each data bit duration, as shown in Fig. 6(b).

Note that the FH/MFSK system has a much wider range of frequencies than the ordinary MFSK system. For a fixed jammer power J, the broadband jammer needs to spread its power over the entire FH bandwidth W_{FH}. Hence, the effective corrupting power fallen into a single MFSK band is J/PG, where PG is the processing gain of the FH/MFSK system and is defined as

$$\mathrm{PG} = \frac{W_{\mathrm{FH}}}{MR_{\mathrm{d}}} \tag{16}$$

Because the PG is usually very large, the FH/MFSK is very effective in counterattacking broadband jamming.

For a stationary partial-band or multitone jammer, an FH system is also considered to be robust. This is due to the fact that the signal is lost for only a small portion of time when the hopping frequency falls into the fixed jamming band. For a majority of time, the signal is free of jamming. This implies that the FH is based on the concept of frequency discrimination.

Unfortunately, the partial-band or multitone jammer is intelligent enough to be able to detect the transmitted FH/MFSK signal, follow the hopping pattern, and concentrate its total power J to jam the full band of M MFSK carriers. Therefore, the FH/MFSK system becomes vulnerable to the intelligent partial-band and multitone jammers. To solve this problem, an FFH must be adopted so that the jammer is not able to follow the hopping pattern. In addition, the coding and time diversity becomes desirable is this scenario.

Time Hopping

Like FH, time hopping (TH) is also driven by a PN sequence generated by a PN code generator. Instead of hopping the carrier frequencies in a much wider frequency band, the time hopper controls the time stamps for turning on and off the signal transmission in the time domain. This technique is effective only to the pulsed jamming. A TH system can force a jammer to stay on at all times in order to be effective. Under the constraint of a fixed energy, the jammer needs to reduce its transmitting power, resulting in less interference. Obviously, the TH system is based on the concept of time discrimination (2).

Time Diversity

Time diversity is a technique in which each information bit is subdivided into multiple equal spaced sub-bits before entering the modulator. It is usually implemented in the FFH system to counterattack the partial-band or multitone jamming. To make the counterattack more effective, the hop duration has to be equal to or less than the sub-bit duration. Therefore, if one sub-bit is jammed, other sub-bits of the same bit may be hopped to a frequency outside the jamming band and detected without errors. This antijamming technique is also based on the concept of time discrimination.

Antenna Nulling

A spatial discriminating technique for antispoofing and antijamming is antenna nulling or sidelobe cancellation (3). In order to provide a nulling capability, the antenna system needs to be equipped with an array of element antennas and associated electronics for beam forming. At least two spot beam element antennas, each of which can be pointed and controlled independently, are needed. The received signals from all element antennas are phase shifted and amplitude attenuated independently and individually, and then combined to form a single signal. The combination of this array of element antennas is called phased-array antenna.

First, the antenna system tries to sense the presence of a spoofer or jammer within the antenna field of view by sampling the received signal from each element antenna and determining whether there is significant energy outside the ex-

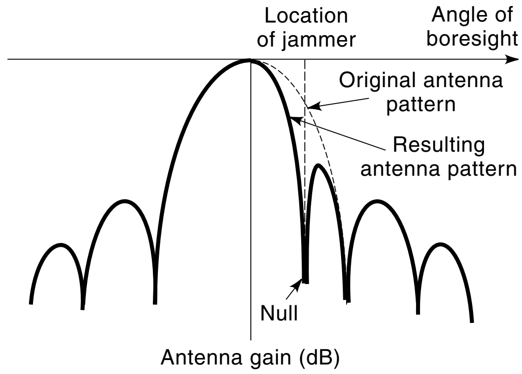

Figure 7. A conceptual antenna pattern of nulling.

pected bandwidth. After the spoofer or jammer is detected, a nuller algorithm processor decides and adjusts accordingly to the phases and attenuation weights of all element antennas. As a result, a null is generated at the direction to the spoofer or jammer so that the interference attack becomes completely ineffective. Figure 7 illustrates a conceptual diagram of forming an antenna null. In most military communications systems, such as the military satellite communications (MILSATCOM) systems, the antenna nulling scheme is required to be implemented on spacecraft.

Forward Error Correcting Code

In general, using a forward error correcting (FEC) code to improve the power efficiency can be also considered as an antispoofing or antijamming technique. Various coding schemes have been included in various systems for this purpose. (7,1/2) convolutional code with Viterbi decoding has been widely used due to its good FEC capability (4). The Reed–Solomon code has been shown to be powerful for correcting burst errors (5). Concatenated code structure with (7,1/2) convolutional code as the inner code and Reed–Solomon code as the outer code has been known to have a significant anti-corruption capability (6). Recently, a newly invented turbo code has demonstrated its ability to provide a near-Shannon-limit coding gain (7).

PROPAGATION CHANNEL CHARACTERISTICS

The term *fading channel* is used when the physical medium affects radio-wave propagation such that the received signal appears to have amplitude fading and/or phase jitter. Three principal fading phenomena are (1) multipath, (2) ionospheric effects, and (3) nuclear-blast-induced plasma.

Multipath Fading

Multipath fading is usually associated with terrestrial communications or low-elevation-angle satellite communications where the transmit and receive signals are subject to reflection from terrain and objects, fixed or moving. Measurement data have been provided from NASA missions (8,9), and Brayer of MITRE also performed several investigations in this area (10,11). In multipath fading, the signal is a composite of the line-of-sight wave and reflections, from the earth's surface, that occur along the propagation channel. Fade condition is dependent on the terrain encountered, such as mountainous, smooth, lake, or oceanic. The received signal is a composite of constructive and destructive interference of the primary and coherent reflections to induce the scintillation behavior. It is convenient to define the single-frequency case after Bullington (12) for the primary and echo without modulation:

$$\nu = 1 + Re^{i(\theta+(n-1)\cdot\pi)} = Le^{-i\cdot\gamma} \tag{17}$$

with

$$\tan\gamma = \frac{R\sin\theta}{1 - R\cos\theta} \tag{18}$$

where R is the instantaneous amplitude and θ is the instantaneous phase of the "composite echo." Experiments have shown that both fades and their duration would be proportional to the combined amplitude L as

$$\mathrm{Prob}[(L_{\min}/L) \le X] = X, \qquad \text{where } 0 \le X \le 1 \tag{19}$$

Figure 8 illustrates a relationship between fade duration and percent of fades for an example of multipath fading at 4 GHz.

Ionospheric Effects

Fading or scintillation occurs in the ionosphere due to the influence of electron densities in the propagation medium. Ionospheric scintillation can be a major factor for satellite communications depending on carrier frequency, satellite to terminal locations, time of day, season, and magnetic activity. Figure 9 indicates the change of ionospheric scintillation as the frequency changes (13).

Equatorial scintillation is caused by electron gradients at altitudes of several hundred kilometers. High-latitude scintillation occurs from the visible aurora region (regions D and E) and from the polar cap to the aurora (14). The electron densities in the ionosphere tend to align with the earth's magnetic field lines. This causes the fading characteristics to be highly geometry-dependent, particularly at high latitudes and at the

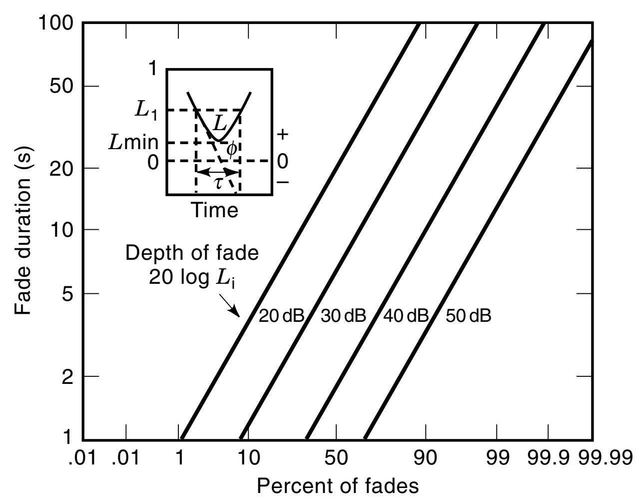

Figure 8. Duration of fading at a 4 GHz on a 30 mile path.

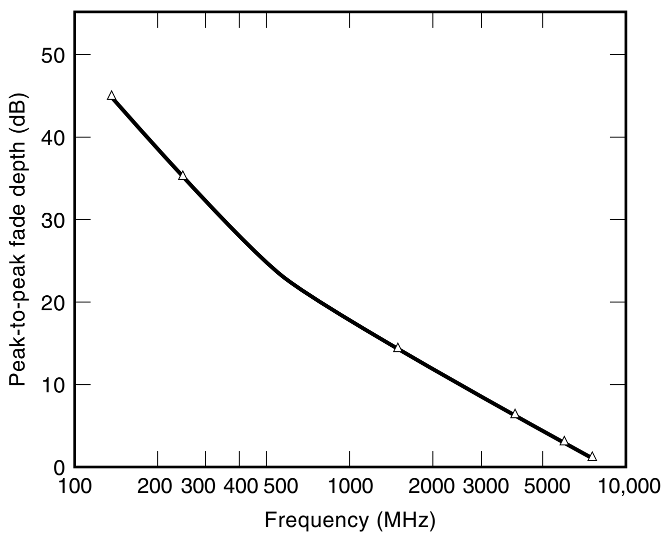

Figure 9. Frequency dependence of ionospheric scintillation fading.

poles. Figure 10 shows the geographic distribution of the ionospheric scintillation (15), in which the darker the region, the severer the fade.

Nuclear Blast Induced Plasma

Nuclear-induced scintillation is postulated when such ordinance is detonated in the upper atmosphere to cut off communications, particularly via satellite. Corroboration of such characteristics were conducted by the "Starfish" experiments in the 1950s and by STRESS test in which barium clouds were set up in the upper atmosphere through which radiowave propagation was studied.

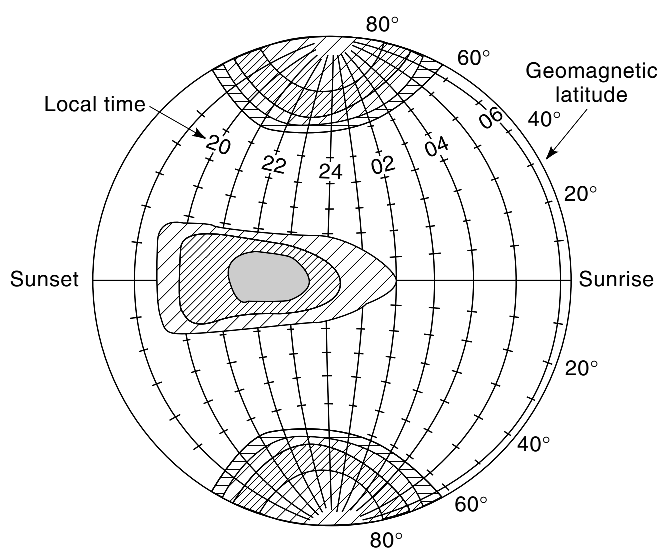

Figure 10. Geographic distribution ionospheric scintillation. The depth of scintillation fading is proportional to the density of cross-hatching.

The generalized power spectrum $\Gamma(f, \tau)$ of the scintillation fading can be characterized by the scintillation decorrelation time τ_0 and the frequency-selective bandwidth f_0 (16).

$$\Gamma(f,\tau) = \frac{1.864\tau_0\delta(\tau)}{[1 + 8.572(\tau_0 f)^2]^2} \tag{20}$$

for $f_0 \cdot T > 1$ with T being the minimum symbol time, where δ is the Dirac delta function. For frequency-selective fades ($f_0T < 1$), we have

$$\begin{aligned}\Gamma(f,\tau) = {} & 2.981\frac{f'\tau_0}{C_1^{1/2}} \exp\left\{-\frac{1}{2C_1^2}[(\pi\tau_0 f)^2 - 2\pi f'\tau]^2 - (\pi\tau_0 f)^2\right\} \\ & \times \int_{-\infty}^{\infty} \exp\left\{-x^4\right. \\ & \left. -2x^2\left[\frac{C_1}{2^{1/2}}\left(1 + \frac{1}{C_1^2}((\pi\tau_0 f)^2 - 2\pi f'\tau)\right)\right]\right\} dx\end{aligned} \tag{21}$$

where

$$\begin{aligned} f' &= f_0(1 + C_1^2)^{1/2} \\ C_1 &= \text{delay parameter } (\approx 0.25)\end{aligned} \tag{22}$$

For both Eqs. (20) and (21), we have

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \Gamma(f,\tau)\, df\, d\tau = 1 \tag{23}$$

In scintillation, there are random time-varying components of the electron density. If the random component is zero mean and normally distributed, Wittwer (13) has given the variance of this component $g(f)$ as

$$\overline{g^*(f)g(f')} = \begin{cases} \delta(f - f')\dfrac{\tau_0(f_c/r_0c)^2}{[a^2 + (2\pi f\tau_0)^2]^{3/2}} & \text{for } f \le f_r \\ 0 & \text{for } f > f_r \end{cases} \tag{24}$$

where

$g(-f) = g^*(f)$
$a^2 = (r_0 \cdot c \cdot N_L(t)/f_c)^{-2}$
r_0 = classical electron radius (2.82×10^{-5} m)
c = light speed (3×10^8 m/s)
$N_L(t)$ = large scale (slow component of electron density)
f_c = carrier frequency
$f_r = 1/(2\pi\sigma\tau_0)$
σ = Rayleigh phase variance, Rayleigh scintillations
= 0 phase-only scintillation

FADING MITIGATION TECHNIQUES

There are five major techniques that can be employed to specifically combat the effects of fading. They are (1) frequency band selection and diversity, (2) spatial diversity, (3) time diversity (interleaving), (4) polarization, and (5) equalization. In addition, coding and frequency hopping (with or without chirp combined), where the hop rate is faster than the data rate, also mitigate fading.

Frequency Band Selection and Diversity

Scattering and scintillation are two major factors that cause fading in communication systems. As was shown in the previous section, the effectiveness of these two factors depends on the operating frequency. Therefore, properly selecting a frequency band for a satellite system to operate becomes very important. Furthermore, transmitting the signal on multiple carriers and employing a diversity combiner is also an effective way to combat the fading loss.

Spatial Diversity

Due to link geometry, the effects of the fading phenomena are spatially selective as well. Fading is more sensitive to spacing with vertical than with horizontal distance by about an order of magnitude. Spacing the transmit/receive apertures to decorrelate fading provides immunity. Providing multiple receptions by utilizing more than one ground station and then combining the received signals can build up a robust system in fading environments.

Polarization

Polarization is the orientation of the plane on which the electric field vibrates when an electromagnetic wave propagates through the medium. The wave can be linearly, elliptically, or circularly polarized. Jordan suggested that multipath effects can be limited by use of circular rather than linear polarization (17). This is due to the nature of the wave propagation and multipath reflections. Therefore, in a fading environment, circular polarization is preferable.

Equalization

Equalization attempts to compensate for the time dispersion effect in the fading channel. The effects of the multipath channel has the effect of time smearing the signal introducing intersymbol interference (ISI). A common equalizer structure is the mean square error (MSE), where the sum of the squares of ISI and noise power is minimized. Lee and Messerschitt (18), Widrow and Stearns (19), and Orfanidis (20) discussed the concept of equalization and adaptive signal processing. A synchronization sequence must be transmitted to aid the adaptation process.

Coding

Using an effective FEC code is an important antifading scheme. Because fading is usually on and off so that the received signal is corrupted only in a small portion of a duty cycle, the errors generally come in bursts. Reed–Solomon code is known to be good for burst error correction. However, in a severe fading environment where the fade duration is long, the concatenated code structure, with a convolutional or turbo code as the inner code and a Reed–Solomon code as the outer code, incorporated with interleaving is required.

Interleaving/Deinterleaving

Interleaving is essentially a permutation among the transmitted channel symbols. Thus, when an interleaving technique is adopted, the continuous data need to be subdivided into blocks. In addition, it generally comes with an FEC code. In the transmitter, the modulated symbols at the output of modulator are permuted before entering the channel. The channel symbols are corrupted in bursts in a fading environment. At the receiver, a deinterleaver rescrambles channel symbols using a reverse permutation pattern so that the order of the originally modulated symbols is preserved. Due to the process of deinterleaving, the burst channel symbol errors are broken into scattered random errors that will be, in turn, easily corrected by an FEC decoder. In order to ensure the randomness of the channel symbol errors after deinterleaving, the interleaving depth should be linearly increased as the fade duration increases.

It should be pointed out that interleaving/deinterleaving results in a delay that depends on the interleaving depth and type. Theoretically, the interleaving pattern can be any format of permutation. Block and convolutional interleavings are the two most commonly used patterns.

- *Block Interleaver.* As shown in Fig. 11, a block interleaver is a regular interleaver in that the input symbols are written in rows and read in columns. For a 5×6 block interleaver, if $I_1, I_2, I_3, I_4, \ldots$ are the input symbols, the outputs are $I_1, I_7, I_{13}, I_{19}, I_{25}, I_2, I_8, I_{14}, \ldots$. It can be seen that the permutation cannot take place until the entire block is filled up with the input symbols. Therefore, a block interleaver of size N suffers a delay of N symbol intervals.
- *Convolutional Interleaver.* Figure 12 illustrates the structure of a convolutional interleaver. For the same input symbols $I_1, I_2, I_3, I_4, \ldots$, the outputs become I_1, X, X, X, X, X, I_7, I_2, X, X, X, X, I_{13}, I_8, I_3, X, X, X, I_{19}, I_{14}, I_9, I_4, X, X, I_{25}, I_{20}, I_{15}, I_{10}, I_5, X, . . ., where X is a dummy symbol. It can be seen that the convolutional interleaver reads out the symbols on diagonals. So, the convolutional

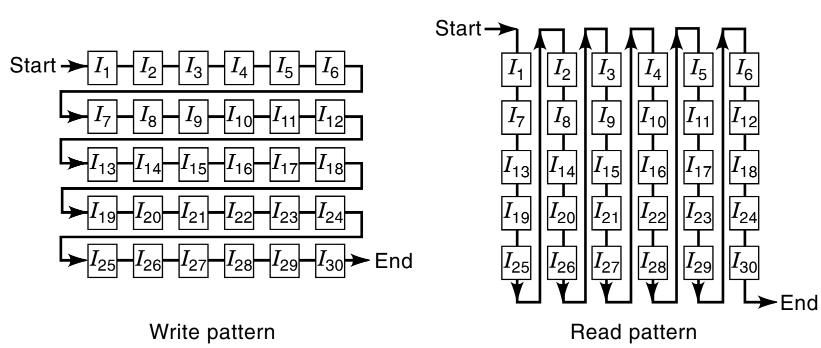

Figure 11. A 5×6 block interleaver.

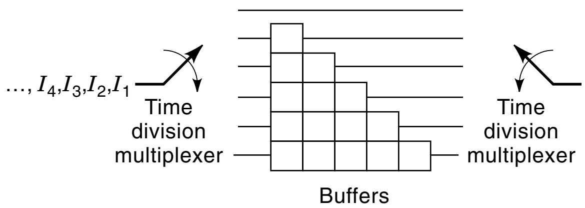

Figure 12. A convolutional interleaver of depth 6.

interleaver can start its output without having the entire block filled up. As a result, the delay is one-half of the interleaver depth.

LOW PROBABILITY OF DETECT/LOW PROBABILITY OF INTERCEPT (LPD/LPI)

In electronic warfare, radio signals from transmitters can be detected by adversaries. As a result, the location of soldiers and command posts can be identified, jeopardizing human lives and success of operations. In order to prevent signals from being intercepted, receivers are designed with good capability of low probability of detect (LPD) or low probability of intercept (LPI).

Detection of Signals in the Presence of Noise

In communication systems, the most commonly used theory is the detection theory. This refers to the technique of making a decision as to whether a radio signal is received in the presence of noise. It is possible that the receiver misdetects a radio signal when it thinks that only the noise is received. On the other hand, the receiver may present a false alarm by declaring that a radio signal is present when no signal actually exists. Hypothesis testing is one of the most important statistical tools for making such decisions (21). The hypotheses are statements of the possible decisions that are being considered. For example, in a radar detection problem we might select two hypotheses—a target is present (H_1) or no target is present (H_0).

The total power radiometer is a commonly used device that detects the existence of a radio signal in the presence of noise. It operates as a square-law device that outputs the average power of the input signal within a certain bandwidth and over a certain period of time T_0. Figure 13 shows the block diagram of a total power radiometer.

The input $x(t)$ to the radiometer includes the signal component $s(t)$ of power P_s and the noise component $n(t)$, which is white with power spectrum N_0. The test statistic z out of the radiometer can be expressed as

$$z = \frac{1}{T_0}\int_{t_0}^{t_0+T_0} (s(t) + n^*(t))^2\, dt \tag{25}$$

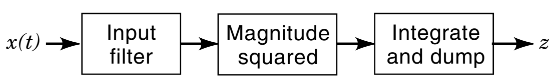

Figure 13. Block diagram of a total power radiometer.

where t_0 is a particular time instant for starting the observation, T_0 is the observation period, and $n^*(t)$ is the band-limited noise component. Let the likelihood function, $p_0(z)$ and $p_1(z)$, be defined as the probability of observable being at z given conditions of H_0 and H_1, respectively. It can be shown (22) that $p_0(z)$ and $p_1(z)$ can be approximated by Gaussian probability density functions with mean values, m_0 and m_1, and variances, σ_0^2 and σ_1^2, respectively, given by

$$\begin{aligned} m_0 &= P_s + N_0 B \\ m_1 &= N_0 B \\ \sigma_0^2 &= (2P_s + N_0 B)N_0/T_0 \\ \sigma_1^2 &= N_0^2 B/T_0 \end{aligned} \tag{26}$$

where B is the bandwidth of the input filter of the radiometer, assuming an ideal filter is used.

It should be pointed out that the design of the front-end filter bandwidth of a receiver is based on the requirement of adjacent channel interference (ACI). For example, a system may require the ACI at the edge of the input-filter bandwidth to be at least -20 dB of the center carrier power so that the system can provide a good link quality to the customer. In this case, the bandwidth of the input filter, assuming to be ideal, has to be at least 1.8 times the R_s for QPSK signaling (23), where R_s is the channel symbol rate. On the other hand, if the receiver is simply used to detect the presence of a radio signal, the bandwidth of the input filter can merely match the 3 dB bandwidth of the power spectrum of the signal. In this section, we assume that the input filter bandwidth of the radiometer is equal to R_s of the $s(t)$, which is close to the 3 dB bandwidth.

When a single fixed-length packet is transmitted with a packet duration less than the observation time T_0, we will replace the above P_s by μP_s, where μ is the duty cycle of the packet within T_0, assuming that the entire packet is to be observed within the observation period T_0. This is a practical assumption as long as T_0 is much larger than the packet duration.

To decide whether it is H_0 or H_1, the observable z is compared against a threshold. The signal is declared to be present if z is above or equal to the threshold, and absent if z is below the threshold. Let us define the probability of detection P_d as the probability that the signal is declared to be present (z is above or equal to the threshold) when the signal indeed exists, while the probability of false alarm P_{fa} is defined as the probability that the signal is declared to be present when no signal is actually transmitted. It can be seen that the sensitivity of the detection (interception) depends on the threshold set. If it is set too low, although the signal will not be likely missed, the P_{fa} will be high, which is not desirable. To the contrary, if the threshold is set too high, the radiometer will not be able to effectively detect the presence of a signal. Therefore, for any specified values of P_{fa} and P_d there is a corresponding threshold. In this type of detection problem, the Neyman-Pearson criterion (21), which maximizes the likelihood ratio $p_1(z)/p_0(z)$ for a given P_{fa}, is generally adopted for setting up the threshold.

In order to be effective, a channelized total power radiometer is used, in that a bank of filters and integrate-and-dump circuits are implemented, each of which matches with the frequency band of each channel so that the radiometer can detect the entire transmitted frequency band. Because different communication systems may allocate different bandwidths for the entire system, for the sake of fairness, the LPD/LPI capabilities for different systems should be compared based on the same length of observation period T_0 and the same specification of false alarm rate (FAR). FAR is defined as the number of false alarm declarations within a unit of time and for a unit of bandwidth. Hence, P_{fa} (for each channel) = T_0[FAR][channel bandwidth]. For example, for a FAR = 1/h/MHz and T_0 = 1 s, P_{fa} (for each channel) = (channel bandwidth in MHz)/3600.

Let us consider a case where the threshold of the radiometer is set such that the probability of correctly detecting a radio signal, P_d, exceeds 50% (with FAR = 1/h/MHz). Based on the Neyman-Pearson criterion, the normalized threshold, defined as

$$\eta = \frac{\text{mean difference}}{\text{standard deviation}} \tag{27}$$

is such that

$$P_{fa} = \frac{1}{\sqrt{2\pi}} \int_{\eta}^{\infty} \exp\left(-\frac{x^2}{2}\right) dx \tag{28}$$

Thus, the threshold η depends on only P_{fa}, which may vary for different systems. From Eq. (26), it can be seen that

$$\eta = \frac{\mu P_s}{N_0}\sqrt{\frac{T_0}{B}} \tag{29}$$

Using this threshold and the fact that $B = R_s$, the received signal-to-noise ratio (SNR), defined as P_s/N_0B, required for this detection is

$$\text{SNR}_{\text{detection}} = \frac{\eta}{\mu\sqrt{R_s T_0}} \tag{30}$$

When a very sensitive detection device is implemented so that the radiometer can detect the signal given a very small amount of energy, a much finer integration time can be used for detection. As a result, this so-called intelligent radiometer is able to pinpoint the time at which each received packet starts and ends. In this case, the total observation time can essentially match with the actual packet duration. Therefore, the duty cycle is always 1. Accordingly, the $\text{SNR}_{\text{detection}}$ used in the intelligent radiometer will be different under the same specifications of P_d and P_{fa}.

Range of Vulnerability

The range of vulnerability, which is defined as the range from the adversary within which a radio can be detected, is used to quantify the capability of the LPI/LPD of a system. From above, it was shown that the sensitivity of detect (intercept) of a radiometer depends on the threshold set. This implies that the range of vulnerability is dependent on the level of threshold. The lower the threshold, the longer the range for a radio not being detected. Thus, the range of vulnerability is meaningful only under specified values of P_{fa} and P_d.

It is well known (24) that the received power of a radio signal at the receiver can be represented by

$$P_r = P_t G_t G_r / L \tag{31}$$

where P_t is the transmitting power, G_t is the transmit antenna gain, G_r is the receive antenna gain, and L is the loss during propagation. The received noise power can be represented by

$$N = N_0 B = kTB \tag{32}$$

where k is Boltzmann's constant ($=1.379 \times 10^{-23}$ J/K), T is the receiver system temperature in kelvin, and B is the bandwidth of the input filter in hertz. Combining Eqs. (31) and (32), the receiving SNR at the radiometer can be expressed as

$$\text{SNR} = (\text{EIRP})(G_r/T)/(LkB) \tag{33}$$

where EIRP ($=P_tG_t$) is the transmitted equivalent isotropic radiated power from a radio and G_r/T is defined as the figure of merit of the receiving antenna.

The range of vulnerability can be studied under two categories, ground collection and airborne collection. The ground vulnerability range is associated with an adversarial radiometer, which is on or near the ground. In this case, the dominant loss of the radio-wave power is due to the reflection from the terrain. The airborne vulnerability range is associated with radiometer placed on the aircraft, in which case the free space loss is only considered in determining the received radio power.

Ground Collection. Blake showed that when a radio wave is reflected from the ground, the received signal is subject to a loss of $L = R^4/(h_t^2 h_r^2)$, where R is the distance between a radio and the radiometer, h_t is the radio's transmit antenna height (from ground), and h_r is the radiometer antenna height (24). Therefore, from Eq. (33), the vulnerability range for the ground collection can be expressed as

$$R = [(\text{EIRP})(h_t^2 h_r^2)(G_r/T)/(kR_s)/\text{SNR}_{\text{detection}}]^{1/4} \tag{34}$$

Airborne Collection. For airborne collection, L is simply the free-space loss that is equal to $(4\pi R/\lambda)^2$, where λ is the wavelength of the carrier. Therefore, the vulnerability range becomes

$$R = [(\text{EIRP})(\lambda/4\pi)^2(G_r/T)/(kR_s)/\text{SNR}_{\text{detection}}]^{1/2} \tag{35}$$

Plugging Eq. (30) into both Eq. (34) and Eq. (35), it can be illustrated that

$$R \propto \left(\frac{\text{EIRP}\cdot\mu}{\eta}\sqrt{\frac{T_0}{R_s}}\right)^e \tag{36}$$

where e = 1/4 for ground collection and 1/2 for air collection.

From Eq. (36), it can be seen that a radio with higher channel symbol rate R_s is less vulnerable to the radiometer detection. That is why the LPI/LPD capability is significantly improved when a CDMA system is utilized. Note that adopting

TDMA in a system will reduce the duty cycle μ and increase the R_s by the same factor of γ, resulting in a reduction of range of vulnerability by a factor of $\gamma^{3/2}$. This implies that a TDMA system also has a good LPI/LPD property. Furthermore, Eq. (36) also explains why the radio is more vulnerable to an intelligent radiometer than a basic radiometer. This is due to the fact that when an intelligent radiometer is used, the observation time is reduced by a factor of $1/\mu$ (T_0 becomes μT_0; $\mu < 1$) and the μ in Eq. (36) is replaced by 1, resulting in an increase of vulnerability range R by a factor of $\sqrt{1/\mu}$. Thus, a TDMA system becomes vulnerable when an intelligent radiometer is utilized.

CRYPTOGRAPHY

One of the more important elements that differentiates military communications from commercial communications is secrecy. Without appropriate safeguards, the transmitted data are susceptible to unauthorized interception, deletion, addition, and modification. Such unwanted exposure of data may jeopardize national security. Cryptography is a practical method of protecting transmitted information from being intercepted.

Classical Cryptology

When a transmitter generates a plaintext or unenciphered message to be communicated over an insecure channel to a legitimate receiver, an eavesdropper can easily intercept it. In order to prevent the eavesdropper from learning it, in the classic cryptography system, the transmitter operates on the plaintext with an invertible transformation to produce a ciphertext or cryptogram. The inverse transformation (or called "key") is either already known by or transmitted via a secure channel to the legitimate receiver. Therefore, the receiver can decipher the received ciphertext by applying the key and recover the original plaintext. This system requires exchanges of the secret keys among communicators.

Public Key Cryptosystems

The public-key cryptosystem is the first secrecy system that does not rely on exchanges of secret keys to obtain its security from cryptanalysis (25). This system employs a public directory in that each subscriber places a key to be used by other subscribers for encrypting their transmitted messages addressed to each recipient. All subscribers keep secret their corresponding decryption keys for decrypting their received messages.

Methods of Encryption

In any cryptosystem, the most important thing is to design a means of encryption so that it is practically impossible for cryptanalysis to break it. Wang developed an algorithm of generating a significantly long pseudo-random number (PN) sequence using exponentiation in finite fields (26). This PN sequence can be used as an encryption/decryption code that is applied to the plaintext by the same way as in the direct sequence (DS) spread spectrum system. Diffie and Hellman used the finite field exponentiation as the operation for encipher or decipher (25). Merkle and Hellman designed a so-called trapdoor knapsack n-vector as the public encryption key (27). McEliece suggested using a linear error-correcting code, Goppa code, for the encryption algorithm (28).

TARGET RECOGNITION OR CLASSIFICATION

Identifying a target in a sense with object distortions and background clutter present is a challenging problem for military applications. Two basic mechanisms, optics and electronics, can be adopted for target image collection. Lens, laser, and infrared light are commonly used for optical sensing, while the classic radar and synthetic aperture radar (SAR) (29) are used for electronic sensing.

After the image is collected, an extensive amount of processing is required. In general, there are five levels of processing required to complete a target recognition. They are (1) detection, (2) image enhancement, (3) segmentation, (4) feature extraction, and (5) identification.

Detection

Detection is the most computationally demanding stage. It must handle every pixel in the input scene, accommodate target distortions, reject clutter, and locate all candidate regions of interest (ROIs). It does not attempt to recognize the object from the background; it merely attempts to locate ROIs. Because it conceivably must process every pixel in every image, it must contain simple and fast algorithms to avoid long processing time. Various types of correlator (detection filter), such as hit-miss (H-M), rank order H-M, etc., were developed (30).

Image Enhancement

Once ROIs have been located, each ROI must be further enhanced to reduce background noises, and fill in holes and sharp edges. These processes will help remove false alarms and achieve identification. Optical morphology (31) is a technique used to enhance the optically collected images.

Segmentation

Segmentation refers to the inference about objects within each ROI and includes rejection of clutter, omission of false alarms, and identification of macroclass (large-sized) target. Early rule-based inference systems such as MYCIN used certainty factors and developed a simple calculus to compute an overall certainty factor for a hypothesis (32). More recently the Dempster–Shafer theory of evidence was developed and refined to address the evidence accumulation issue in target recognition (33,34). Currently, a popular approach to evidence accumulation is via Bayes nets (35). Bayes nets are graphs, primarily tree-structured but not necessarily so, that use Bayes's rule to lay out all of the conditional probability relationships in assessing the probability that a given hypothesis is true.

Feature Extraction

The next step for target recognition is to examine the ROI and extract features that would support the inference. In optical sensing systems, computer generated hologram filters can be used (36). In SAR, the extracted features might be the locations of scattering centers, the shape of the diffuse return of the object, or the location of shadows. The concept is that appropriate features be detected, located, and characterized so that they can be matched against predicted features in the final stage, identification.

Identification

The K-nearest neighbor (K-NN) is a classic algorithm for target identification or classification (37). The problems of this method are selecting the threshold and requiring the number of classes that were known a priori. This process is also slow since it uses a feedforward unsupervised learning method (38). In recent years, feedforward neural networks have been used for target identification (39). This algorithm is fast, less noisy, and more accurate. It can also classify multitarget and multibackground images (40).

GLOBAL POSITIONING SYSTEM

In military applications, ranging and navigation are essential. To achieve them, a space-based navigation system, global positioning system (GPS), has been developed and launched (41). The objective of GPS is to provide accurate, continuous position location information in three dimensions anywhere on or near the earth in all weather conditions. The concept involves measuring the times of arrival of radio signals transmitted from satellites whose positions are precisely known. This gives the ranges to the known satellites, which, in turn, establishes the user's position. To be effective, atomic clocks are installed onboard each satellite, which must be synchronized with a master system clock. Transmission frequencies are selected to minimize timing errors caused by the earth's ionosphere and to be unaffected by rain and weather. By measuring the distance to four GPS satellites, it is possible to establish the three coordinates of a user's position (latitude, longitude, and altitude), as well as GPS time.

Space Segment

The complete GPS space segment consists of 24 satellites. The satellites travel in 12 h circular orbits 11,000 nautical miles above the earth. They occupy six orbital planes, inclined 55°, with four operational satellites in each plane. The satellites are positioned so that six are observable nearly 100% of the time from any point on the earth. Each is equipped with a combination of rubidium or cesium atomic clocks, which are accurate to within 10 ns. By 1994, the GPS had already completed its full 24-satellite constellation.

Control Segment

The worldwide GPS ground control segment includes monitor stations, ground antennas, and a master control station. Receivers at the monitor stations track the GPS satellites, record their positions and status, and relay information to the master control station. There the data are processed to establish the satellites' clock correction factors and current orbital elements for transmission back to the satellites via the ground antennas. Currently, the master station is at Falcon Air Force Base, Colorado. The GPS monitor stations are located in Kwajalein, Hawaii, Diego Garcia, Ascension Island, and Colorado. Ground antennas are located at Kwajalein, Diego Garcia, Ascension Island, and Cape Canaveral.

User Segment

GPS receiver equipment, unique to each application, can be placed onboard aircraft, ships, submarines, trains, cars, trucks, or other vehicles, or it can be hand carried. The receivers detect, decode, and process the GPS satellite signals. GPS can determine a user's position with an accuracy of better than 16 m. Greater accuracy, less than 1 m, can be obtained by using corrections sent from another GPS receiver at a known location, and used as a reference.

Today, there are more than 100 different receiver models in use for a wide variety of military and civilian applications. The typical hand-held receiver is about the size of a cellular phone, and is getting smaller. The hand-held units distributed to U.S. armed forces personnel during the Persian Gulf war weighed only 28 ounces.

MILITARY SATELLITE COMMUNICATION SYSTEMS

Military satellite communication systems of the U.S. have been developed to support communication beyond line of sight and to provide global dispersed forces and global power protection (42–44). The system can also support polar regions and oceans. The systems have been designed to have both interoperability and compatibility features so that they can support users of all types of platforms such as land, ship, shore, submarine, air, transportable, and mobile. The choice of frequency bands is critical in designing the MILSATCOM systems. Three basic frequency bands, namely, ultrahigh frequency (UHF), super high frequency (SHF), and extremely high frequency (EHF), are available and each provides different advantages. UHF with frequency ranging from 300 MHz to 3000 MHz is suitable for mobile systems, which can work in bad weather conditions and dense foliage. Moreover, UHF systems are inexpensive. Since the operating frequencies for SHF systems range from 3 GHz to 30 GHz, they can support higher data rates and hence provide more jam resistance than UHF (because we spread the signals wider than UHF). EHF frequency bands provide the highest data rates and are the most jam-resistant of the three bands because the operating frequencies are allocated in the range of 30 GHz to 300 GHz. Designed systems are also required to provide maximum flexibility for situations such as unpredictable conflicts in location, time, and operation duration and intensity. The systems are able to support voice, text, data, imagery, and video. Figure 14 shows a typical MILSATCOM system.

In the following section we will briefly describe the current MILSATCOM systems and Milstar architecture.

Current MILSATCOM Systems

Based on the frequency bands allocated to the MILSATCOM systems, one can classify the current systems into three categories, namely UHF, SHF, and EHF systems.

UHF Systems. UHF systems consist of two types of satellites:

- *FLTSATCOM and AFSATCOM.* The FLTSAT serves Navy surface ships, submarines, aircraft, and shore sta-

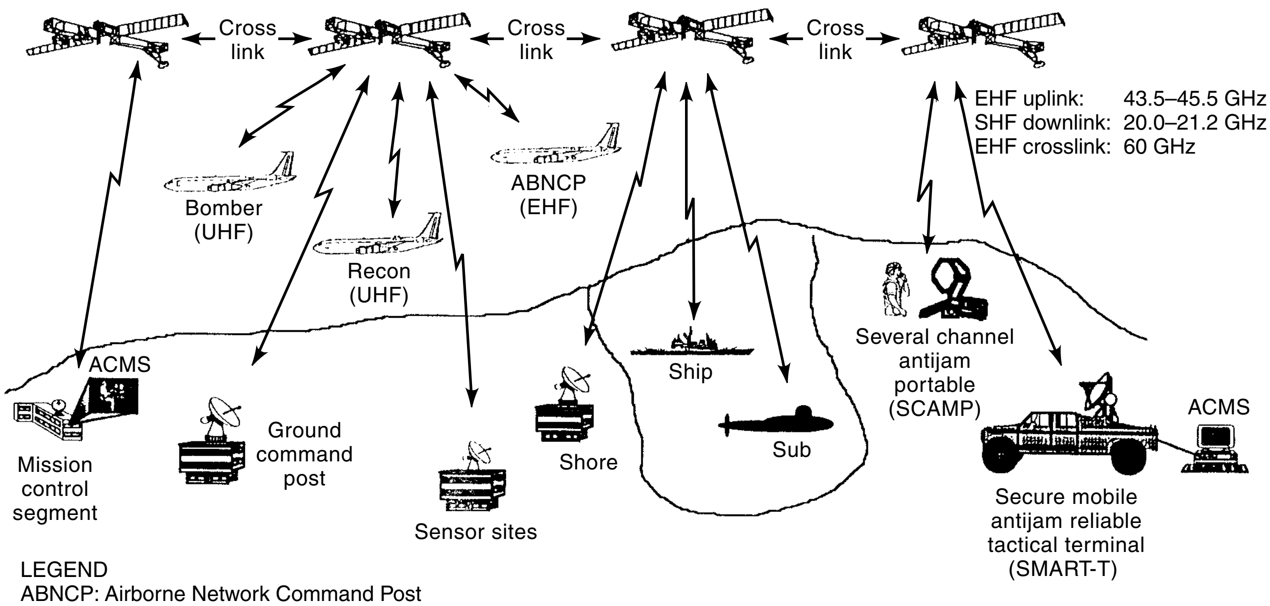

Figure 14. MILSATCOM system.

tions. The AFSAT serves Air Force strategic aircraft, airborne command posts, and ground terminals. The two systems share a set of eight satellites in synchronous equatorial orbits. The Air Force also has communications payload on several satellites in high inclination orbits to provide coverage of the north polar region, which is not visible from the equatorial satellites. These satellites were built by TRW with a design life of 5 years and a weight of 1860 kg at launch. The satellites operate in the frequency ranges of 240 MHz to 400 MHz with on-board signal processing for SHF uplink. The FLTSATs 7 and 8 have fleet EHF packages.

- *UFO.* UFO stands for UHF follow-on satellites, which are built to replace the FLTSAT. The program is managed by the Navy as a lead service with a plan for 10 satellites, with two satellites in each of five coverage areas. These satellites are built by Hughes Aircraft Company with a 14-year design life. These satellites also have EHF on-board signal processing packages.

SHF Systems. The Defense Satellite Communication System (DSCS) has been developed to provide the Department of Defense (DoD), other government agencies, and U.S. allies with global communications services. DSCS provides required national security and maintains thorough communications during crisis and conflict. The DSCS provides services that cannot be provided by other media. The services are provided for both stressed and unstressed environments. Stressed environments contain jamming, nuclear scintillation, and tactical antijam (AJ). Unstressed environments include ATM, dedicated voice and data, high-speed computer to computer, wideband and high capacity during peace and precrisis. These satellites are built by TRW for Air Force Space Systems Division with a design life of 5 years and operating frequency ranging from 7200 MHz to 8400 MHz.

EHF Systems. EHF systems can be classified into two systems:

- *Milstar.* This system, which is the latest addition to and the most advanced in the MILSATCOM architecture, provides service for mobile users for both strategic and tactical missions. The tactical missions are command and control using a low data rate communication (LDR) mode, tactical intelligence dissemination using both LDR and medium data rate (MDR) modes, Army mobile subscriber equipment using an MDR mode, and Navy task force connectivity also using an MDR mode. The strategic missions include strategic intelligence relay, tactical warning/attack assessment data relay, force management, and force report back.

  The Milstar system and satellites are built to be survivable throughout all levels of conflict. The satellites are hardened to resist the effects of nuclear radiation. The Milstar communication links have high threat mitigation features such as LPI, LPD, exploitation, antijam, and antiscintillation capabilities. Other salient features associated with Milstar include LDR and MDR communication services using robust signal waveform, flexible network configuration, and interoperable terminal base.

  Milstar is a joint MILSATCOM program consisting of a six-satellite constellation operating at UHF (225 MHz to 400 MHz), SHF (20.2 GHz to 21.2 GHz), and EHF (43.5 GHz to 45.5 GHZ). Milstar satellites can provide narrow coverage spot beams and MDR nulling antenna capabilities.
- *UFO/E.* This is the ultrahigh frequency follow-on/EHF with operating frequencies in the range of 43.5 GHz to 45.5 GHz for the uplink and 20.2 GHz to 21.2 GHz for the downlink. The UFO/E does not support the crosslinks, and it provides LDR capability only. However, UFO/E provides high-speed fleet broadcast capability.

Milstar Architecture

The Milstar system consists of three segments and the support facilities. The three segments are space, mission control, and terminal segments.

Space Segment. The space segment includes orbiting satellites with satellite bus, LDR and MDR payloads, and crosslinks. Milstar satellites are placed in geosynchronous orbits that can provide coverage up to $\pm 65°$ latitude. Satellites use EHF and SHF for the uplink and downlink, respectively. There are two Milstar I satellites in orbit today with the LDR payload only. The first Milstar II was expected to be launched in early 1999.

- *LDR Payload.* This provides UHF uplink with 2 GHz bandwidth and SHF downlink with 1 GHz bandwidth. It also provides fleet broadcast services. The payload has onboard signal processing, and routing provides interconnections from EHF/SHF links to UHF uplinks and downlinks. The following are some of the features associated with the LDR payload:
  - Data rate: 75 bps to 2400 bps.
  - Frequency hopping with either low hop rate (LHR) or high hop rate (HHR).
  - Multiplexing: TDM/FDM on the uplink and TDM on the downlink.
  - Modulation: FSK on the uplink and DPSK/FSK on the downlink.
- *MDR Payload.* This supports EHF uplink with 2 GHz bandwidth and SHF downlink with 1 GHz bandwidth. It provides crosslink processing of MDR data. The payload has onboard signal processing and resource control. The following are some of the features associated with the MDR payload:
  - Date rate: 4.8 kbps to 1.544 Mbps.
  - Multiplexing: TDM (up to 70 channels)/FDM (32 channels) on the uplink and single TDM on the downlink.
  - Modulation: Filter symmetrical DPSK on the uplink and DPSK on the downlink.
  - Capacity: Maximum throughput of about 45 Mbps.
- *Crosslink Payload.* This simultaneously allows LDR and MDR communication data transmissions and reception between satellites. The crosslink payload also allows for command and telemetry to and from all satellites from a single ground station.

Mission Control Segment. The mission control segment consists of satellite control subsystem and three mission elements, namely, mission support, mission development, and mission planning elements.

- *Satellite Control Subsystem.* This provides distributed command and control via multiple satellite mission control subsystems (SMCS) and preplanned response to satellite. This subsystem uses LDR terminal EHF/SHF communications to control Milstar satellites.
- *Mission Support Element (MSE).* This provides software and databases to control Milstar satellites. This element also supports launch, satellite initialization, and resolution of complex satellite anomalies.
- *Mission Development Element.* This provides a software tool for building SMCS and MSE database, and system simulation supports training and software/database validation.
- *Mission Planning Element.* This provides communications planning software and generates satellite and terminal database information. This element also supports communication resource apportionment, conflict resolution, contingency planning, and detailed communications network planning.

Terminal Segment. The terminal designs and communications protocols are required to provide for interoperable communications among Army-, Navy-, and Air Force–developed terminals. LDR terminals provide survivable tactical and strategic user communications, voice, teletype, and data. LDR terminals also provide force direction/report back, tactical command and control, and emergency message dissemination. MDR terminals can provide all of the features that LDR can provide, including imagery, targeting updates, and mobile subscriber equipment range extension. There are three basic types of terminals: Air Force Milstar, Navy, and Army terminals.

- *Air Force Milstar Terminals.* These include EHF/UHF command post-ground and transportable, as well as UHF force element (also referred to as AFSATCOM dual modem upgrade II).
- *Navy Terminals.* These include ship, shore, submarine, and MDR upgrade program.
- *Army Terminals.* These include secure mobile antijam reliable tactical terminal (SMART-T) and single/multiple channel antijam portable terminal (SCAMP) Block I and II.

Support Facilities. The two basic support facilities are Milstar auxiliary support center and on-orbit test facility.

BIBLIOGRAPHY

1. M. K. Simon et al., *Spread Spectrum Communications,* Vol. I, Rockville, MD: Computer Science Press, 1985.
2. R. C. Dixon, *Spread Spectrum Systems,* New York: Wiley, 1975.
3. R. Nitzberg, *Adaptive Signal Processing for Radar,* Norwood, MA: Artech House, 1991.
4. A. J. Viterbi and J. K. Omura, *Principles of Digital Communication and Coding,* New York: McGraw-Hill, 1979.
5. W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes,* Cambridge, MA: MIT Press, 1971.
6. R. F. Rice, *Channel Coding and Data Compression System Consideration for Efficient Communication of Planetary Imaging Data,* Tech. Memo. 33-695, Jet Propulsion Laboratory, Pasadena, CA, 1974.
7. C. Berrou, A. Glavieux, and P. Thitimajshima, Near Shannon limit error-correcting code: Turbo code, *Proc. 1993 IEEE Int. Conf. Commun.,* Geneva, Switzerland, 1993, pp. 1064–1070.
8. J. J. Lemmon and R. W. Hubbard, *Multipath Measurements for the Land Mobile Satellite Radio Channel,* MSAT-X Report, **126**, Jet Propulsion Laboratory, California, 1985.
9. V. Jamnejad, *A Study of Multipath Propagation in Land Mobile Satellite Systems,* MSAT-X Report, **135**, Jet Propulsion Laboratory, California, 1986.

10. K. Brayer, Error Patterns Measured on Transequatorial HF Communications Links, *IEEE Trans. Commun.,* **COM-16**: 215–221, 1968.
11. K. Brayer, Error Correction Code Performance on HF, Troposcatter and Satellite Channels, *IEEE Trans. Commun.,* **COM-19**: 781–789, 1971.
12. K. Bullington, Phase and amplitude variation in multipath fading on microwave signal, *Bell Syst. Tech. J.,* **50**: 2039–2053, 1971.
13. A. Johnson, The Effect of Ionospheric Scintillation on Aircraft-to-Satellite Communications, AFAL Report AFAL-TR-78-171, US Air Force Wright Aeronautical Laboratories.
14. A. Johnson, Advisory Group for Aerospace Research and Development, AGARD Conf. 1980.
15. J. Aaros, Global morphology of ionospheric scintillations, *Proc. IEEE,* **70**: pp. 360–378, 1982.
16. L. A. Wittwer, A Trans-Ionospheric Signal Specification for Satellite C^3 Applications Robust Communication Links, 1980 Wescon Professional Program, Anaheim, CA, 1980.
17. K. L. Jordan, Jr., *Multipath Characteristics in a Satellite-Aircraft Link at 230 MHz,* Lincoln Laboratory, **MS-2605**, MA, MIT: 1969.
18. E. A. Lee and D. G. Messerschitt, *Digital Communications,* Boston, MA: Kluwer Academic Publishers, 1988.
19. B. Widrow and S. D. Stearns, in A. V. Oppenheimer (ed.), *Adaptive Signal Processing,* Englewood Cliffs, NJ: Prentice-Hall, 1985.
20. S. J. Orfanidis, *Optimum Signal Processing—An Introduction,* 2nd Edition, New York: Macmillan Publishing, 1985.
21. A. Whalen, *Detection of Signals in Noise,* New York: Academic Press, 1971.
22. H. Urkowitz, Energy detection of unknown deterministic signals, *Proc. IEEE,* **55**: 523–531, 1967.
23. J. Omura and M. Simon, *Modulation/Demodulation Techniques for Satellite Communications; Part I: Background,* JPL Publication 81-73, 1981.
24. L. V. Blake, *Radar Range-Performance Analysis,* Norwood, MA: Artech House, 1986.
25. W. Diffie and M. Hellman, New Directions in Cryptography, *IEEE Trans. Inf. Theory,* **IT-22**: 644–654, 1976.
26. C. C. Wang, *Exponentiation in Finite Fields,* Ph.D. Dissertation, University of California, Los Angeles, CA: 1985.
27. R. Merkle and M. Hellman, Hiding Information and Receipts in Trapdoor Knapsacks, *IEEE Trans. Inf. Theory,* **IT-24**: 525–530, 1978.
28. R. J. McEliece, A Public Key Cryptosystem Based on Algebraic Coding, *DSN Progress Report,* **42–44**, Jet Propulsion Laboratory, California, 1978.
29. R. O. Harger, *Synthetic Aperture Radar Systems Theory and Design,* New York: Academic Press, 1976.
30. D. Casasent, R. Schaefer, and R. Sturgill, Optical Hit-Miss Morphological Transform, *Appl. Opt.,* **31** (29): 6255–6263, 1992.
31. D. Casasent, Optical Morphological Processors, *Proc. SPIE—Int. Soc. Opt. Eng.,* **1350**: 380–394, 1990.
32. J. B. Adams, in B. G. Buchanan and E. H. Shortliffe (eds.), Probabilistic Reasoning and Certainty Factors, *Rule-Based Expert Systems,* Reading, MA: Addison-Wesley, 1988, pp. 263–271.
33. G. Shafer, *A Mathematical Theory of Evidence,* Princeton, NJ: Princeton Univ. Press, 1976
34. J. Gordon and E. H. Shortliffe, in B. G. Buchanan and E. H. Shortliffe (eds.), The Dempster–Shafer Theory of Evidence, *Rule-Based Expert Systems,* Reading, MA: Addison-Wesley, 1988, pp. 272–292.
35. J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference,* San Mateo, California: Morgan Kaufmann, 1988.
36. D. Casasent, Computer Generated Holograms in Pattern Recognition: A Review, *Opt. Eng.,* **24**: 724–730, 1985.
37. R. D. Scott et al., Sensor Fusion Using K-Nearest Neighbor Concepts, *Proc. SPIE—Int. Soc. Opt. Eng.,* **1383**: 367–378, 1991.
38. G. Parthasarathy and B. N. Chatterji, Class of New KNN Method for Low Sample Problems, *IEEE Trans. Syst., Man Cybern.,* **20**: 715–718, 1990.
39. S. K. Rogers et al., Artificial Neural for Automatic Target Recognition, *Proc. SPIE—Int. Soc. Opt. Eng.,* **1294**: 2–12, 1990.
40. R. Mamlook and W. E. Thompson, A Multi-Target and Multi-Background Classification Algorithm Using Neural Networks, *Proc. SPIE—Int. Soc. Opt. Eng.,* **1955**: 218–225, 1993.
41. The Institute of Navigation, *Global Positioning System,* Vol. I and II, Washington DC, 1984.
42. D. H. Martin, Communication Satellites, 1958–1992, 1991, The Aerospace Corporation, El Segundo, CA.
43. MILSATECOM, JETO, Milstar Training, Part I, Milsatcom Joint Terminal Eng. Office.
44. MILSATECOM, JETO, Milstar Training, Part II, Milsatcom Joint Terminal Eng. Office.

CHARLES C. WANG
TIEN M. NGUYEN
GARY W. GOO
The Aerospace Corporation

MILLIMETER-WAVE COMPONENTS, FINLINE. See FINLINE COMPONENTS.

MILLIMETER-WAVE INTEGRATED CIRCUITS. See MICROWAVE INTEGRATED CIRCUITS.