ELECTRONIC WARFARE

Robert Inkol

Defence Research and Development Canada

1 Introduction

Over the last century, there has been a burgeoning use of the electromagnetic (EM) spectrum for military purposes, including those related to communications, navigation, and targeting.

This dependence is embedded in many modern warfare doctrines and technologies, such as:

- Revolution in Military Affairs;
- Network-centric warfare;
- Information warfare;
- Rapid decisive operations;
- Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR);
- Precision guided weapons.

Given the importance of the EM environment to military operations, there is obvious reason for safeguarding its use by friendly forces, denying its use by enemy forces, and defeating enemy efforts to achieve the same objectives. Electronic Warfare (EW) encompasses the broad and somewhat ill-defined mix of military tactics, techniques, procedures (TTPs), technology and organizational structures that address these concerns [sc99], [po02]. It is also related to some civilian technologies and applications, including spectrum monitoring and radio astronomy.

Historical experience has repeatedly demonstrated the importance of EW as highlighted by an extensive body of declassified information pertaining to operations by both sides in World War II [pr78], [pr84], [jo78], and by more recent accounts concerning the Korean, Viet Nam, Six Day and Yom Kippur Wars, and the campaigns in the Falklands, Lebanon, Kosovo, Chechnya and Iraq [ar85], [pr89], [pr00], [mi07], [ha02].

EW continues to be widely recognized as a powerful force multiplier and the development and application of EW concepts and technologies consequently remains a high priority [ew07], [ja07]. For the greatest effect, its use is regulated by planning structures that tailor it to situational requirements, and procedures intended to deny the enemy as much knowledge as possible relating to its specific capabilities and deployment structures. For this reason, many aspects of EW are highly classified.

Formally, the roles of EW are subdivided into:

1. Electronic Support (ES) - taking advantage of signals emitted by an opponent's systems;
2. Electronic Attack (EA) - degrading the ability of an opponent to use his systems;
3. Electronic Protection (EP) - safeguarding the effective operation of friendly force electronic systems against enemy EA and ES activities.

The following article presents a breakdown of EW in this order, with attention given to both technical system concepts and relevant operational doctrine.

2 Electronic Support

Electronic Support (ES), also known as Electronic Support Measures (ESM), concerns the sensing of communication, radar and other electromagnetic signals of potential interest. ES sensors perform the following technical functions:

1. Signal detection - determining the presence of a signal;
2. Signal classification - associating the signal with a type of modulation or function;
3. Signal parameter and feature extraction - measuring various signal parameters; such as carrier frequency, power, transmission start and end times, and bandwidth;
4. Emitter identification - determining the type of system that the signal is associated with;
5. Signal intercept – recovering the message content from communication signals;
6. EW analysis - inferring the organization and structure of enemy networks, dispositions of forces and operational intent from communications traffic patterns and message content;
7. Geo-location - determining the positions of signal emitters.

Several points concerning ES deserve emphasis. First, its passive nature has the great advantage that valuable intelligence can be produced without an adversary being aware. Second, the mere suspicion of its use can cause an adversary to restrict its use of communication systems and active sensors, thereby reducing their operational value. Finally, radar ES systems are often able to detect a radar transmitter at ranges considerably in excess of the useful range of the radar. The radar must be able to detect the extremely small fraction of the transmitted signal power that the target reflects back to the radar [ea85].

The organization and processing of information provided by ES sensors is a complex problem. Much of the value of ES sensor outputs can be lost if information does not reach the appropriate commanders and other potential users in a timely way. Complicating factors include the volume of information, the difficulty of interpreting it, and the need to protect sensitive information concerning ES capabilities. The last point is a very real concern. During WW2, the decryption of German communication signals coded with the Enigma cipher provided immensely valuable intelligence to the British.

Accordingly, every effort was made to avoid arousing suspicions that the Enigma cipher was anything other than unbreakable. For example, reconnaissance aircraft would be dispatched to "find" an important convoy whose orders had in fact been revealed by the decryption of Enigma messages, thereby giving the impression that the attack that followed was the direct result of routine aerial reconnaissance [jo78].

The diversity of the roles performed by ES systems has resulted in a significant degree of specialization in the design of the systems themselves and their organization and control.

2.1 Tactical ES

Tactical ES is the deployment of an ES capability in direct support of field operations. It typically resides within some form of dedicated Electronic Warfare unit that may be either part of the maneuver force's echelon or assigned to support it under an operational (OPCON) or tactical (TACON) command and control relationship. Examples of tactical ES are found in land, air and sea operational environments, where objectives include:

1. The intercept, direction finding and analysis of battlefield communications signals by ground based assets to determine the composition and geographical distribution of enemy forces and the immediate intentions of its elements, from fighter to commander. When ES is performed by an EW unit native to the maneuver force, 'intentions and warnings' (I&W) tip-offs are reported directly to field unit commanders and their staff. The unit may also acquire and disseminate intelligence for consumption strictly within Signals Intelligence (SIGINT) channels (see below) and generate technical information for internal process refinement;
2. The detection and direction finding of battlefield surveillance radars by ground based radar ES;
3. The detection and analysis by a Radar Warning Receiver (RWR) of radar signals associated with enemy target acquisition, tracking and fire control systems, to provide aircraft pilots with situational awareness and warnings of threats. This information is essential for the timely initiation of suitable countermeasures, which may include a combination of EA and evasive maneuvers;
4. A general surveillance capability by a warship's radar ES systems to track military, merchant or clandestine ships and fishing vessels using the signals received from their navigation radars. These systems also perform the same self protection functions as RWRs used on smaller platforms. On larger platforms, there are usually more provisions for analyzing ES information, fusing it with other intelligence, and distributing it to other platforms, channels and organizations (including SIGINT).

The capability to geo-locate transmitters associated with communication, navigation, and radar systems is particularly important; even approximate indications of the direction of an enemy position or platform provided by direction finding (DF) are valuable from a situational awareness perspective. Estimates of the positions of individual emitters can be determined by obtaining lines-of-bearing from spatially separated sites and solving for the positions where they intersect. Geo-location is particularly important for

communication signals when the message content cannot be extracted because of encryption or other techniques. Appendix 1 provides an overview of various DF techniques that can be used for the geo-location of signal sources by ES systems.

An additional EW Analysis (EWA) capability is often associated with units that deploy ES assets. EWA is a Military Intelligence function that specializes in drawing operational inferences from EW data. Its main purpose is to determine the enemy's 'electronic order of battle', a comprehensive representation of its electronics systems, including their identification, geographical disposition, and where possible the association of this equipment with specific units within a command-control structure. An EW Analysis cell may also be responsible for maintaining communication target lists and selecting information for dissemination to Intelligence organizations.

Tactical Communications ES is a particularly challenging problem in urban environments. Multipath propagation effects can be expected to seriously degrade the accuracy of radio frequency direction finding systems. Furthermore, opposition forces can be expected to make use of the civilian communications infrastructure. This results in a requirement to sift rapidly through a large amount of communications traffic to find the signals of interest.

2.2 Signals Intelligence

Signals Intelligence (SIGINT) is the strategic application of ES performed under the control of national intelligence organizations, such as the National Security Agency (NSA) in the US, and the Government Communication Headquarters (GCHQ) in the UK. The term relates variously to the type of information produced, the systems used to produce it, and to the community that controls the ES systems and the analysis and distribution of their products. SIGINT 'products' are disseminated via highly classified channels and, except in exceptional circumstances, only released for use in the wider national or Military Intelligence communities after being 'sanitized' of any distinguishing elements that could reveal the source. On the battlefield, there may be some overlap between SIGINT and tactical ES activities and platforms, with EW units sometimes tasked to serve both functions simultaneously.

SIGINT comprises Communications Intelligence (COMINT) and Electronic Intelligence (ELINT). COMINT is concerned with the message content of communication signals, information about communication traffic patterns, and the locations of the associated transmitters, with a strong emphasis on determining higher level or 'strategic' command and control structures. ELINT is the collection of technical or 'parametric' information about the radar and other non-communications equipment [wi82].

ELINT has several important uses. First, theoretical analysis of the signal parameters allows inferences to be drawn about the functions, capabilities and limitations of the systems associated with the signals, and hence, more broadly, about enemy early warning or targeting capabilities. Second, ELINT data is used to construct emitter libraries or databases that are fundamental to EA and EP operations. For each known type of radar, information is collected on the signal parameters for the various operating modes, the estimated radar performance, its intended function(s), and the platforms the radar is known to be installed on. An ES system on a ship or tactical aircraft correlates the parameters of observed signals with the database entries to identify the radar systems that

transmitted them, and, if an observed signal is associated with a threat, provides the information needed to select and execute the most appropriate countermeasures.

SIGINT operations often involve the use of specialized equipment deployed on either dedicated or multi-use platforms, including satellites, ships and aircraft. During the Cold War, suitable types of aircraft were extensively modified to perform SIGINT. By operating at altitudes of 10 km or higher, useful ranges could be extended to hundreds of km for the intercept of microwave radar signals. Consequently, intelligence could be acquired from aircraft flying at the periphery of the Soviet defense perimeter. For a period, specialized high altitude aircraft were even able to carry out operations over Soviet territory by flying above the effective ceiling of interceptor aircraft and ground based anti-aircraft weapons. After improved Soviet anti-aircraft defenses made overflights impractical, the West hurriedly deployed satellite based systems [mc05].

In recent years, much interest has been aroused by the idea of integrating ES information derived at different levels (tactical, operational, and strategic) by EW and SIGINT units with similar objectives, but possibly different reporting mechanisms. For instance, modern strategies for Netcentric Warfare involve the accumulation of various kinds of data and intelligence at a central point where it can be fused to produce more complete assessments. However, many practical challenges exist in reconciling technical possibilities with doctrine. Complicating factors and risks involved with centralized analysis schemes include:

1. The quantity of data generated by advanced ES systems may tax the analysis systems that must sort through it;
2. Delays in the reporting chain, where key information may take longer to reach its ultimate destination after passing through a central accumulation point;
3. The expense and complexity of deploying communication systems with adequate bandwidth;
4. Standardization issues for technical interfaces, and the complexity of both designing and maintaining interfaces for systems that were originally designed for different purposes and may be based on widely differing technologies;
5. Complications affecting the handling and distribution of information resulting from classification issues and, in the case of multinational environments, the willingness of individual nations to declare and release their information to others;
6. The risks of commanders relying too heavily on the formation of a ‘complete intelligence picture’ in lieu of trusting their judgment and intuition, which can lead to decision paralysis.

2.3 ES System Technologies and Implementation

ES systems are typically comprised of antenna, receiver, and processing systems. Early ES systems were often improvisations based on civilian equipment. For example, receivers developed for radio amateurs had relatively good sensitivity and frequency coverage and were widely used by the Allies during WW2. The National HRO, having excellent frequency resolution, was used to intercept communication signals in the Medium and High Frequency bands. The Hallicrafters S-27, providing contiguous coverage in the lower portion of the Very High Frequency (VHF) band, was widely used

to receive signals associated with German VHF radar, air-to-air communication, and bombing navigation systems. These receivers, while useful, had significant limitations. Their frequency coverage was limited and their effectiveness was heavily dependent on the training and skill of the operators.

The continued evolution of the technologies used by communication and radar systems has contributed to the development of specialized ES receivers. A fundamental issue concerns the differences in the waveforms used by communication and radar signals.

Most communication systems transmit a continuous or near continuous narrow bandwidth signal during the transmission of a message. A primary goal is to make efficient use of bandwidth to transmit information, thereby allowing the available radio frequency bands to be divided between many users. Communication signals have continued to evolve:

1. The bandwidth and channel spacing associated with conventional narrowband signals has decreased due to developments in more efficient modulation formats and accurate frequency references and synthesizers;
2. Digital modulation techniques are being increasingly used to transmit information in the form of binary data;
3. Time division multiplexing access (TDMA) techniques are being used by some systems, such as those based on the GSM cell phone standard, to provide a way of time sharing bandwidth between multiple users;
4. Classes of spread spectrum techniques are being used in some military and civilian communication systems. Frequency hopping (FH) systems superpose periodic changes on the center frequency of a transmitted signal following a predetermined sequence. These changes typically occur at rates that are tens or hundreds of times a second. The portion of a transmission corresponding to a dwell at a single frequency is often referred to as a hop. To minimize interference between FH communication systems, careful co-ordination is needed in the assignment of hop frequencies and/or the codes defining the hop sequences. Direct sequence spread spectrum (DSSS) uses a different approach. In the basic form, a pseudo-random number (PRN) sequence is used by the transmitter to spread the narrowband information content over a much larger bandwidth. The receiver uses the same PRN sequence to recover the information. Multiple systems can share the same bandwidth without seriously interfering with each other if they are assigned different PRN sequences. Code division multiple access (CDMA) cell phone systems are a major application of DSSS techniques. Since the detection of spread spectrum signals often requires special techniques [hi97], these signals are sometimes referred to as low probability of intercept (LPI) signals.
5. Mobile communication systems and networks have proliferated and are widely used. These systems are based on the idea of dividing a geographical area into cells. Each cell has a base station that performs the functions of relaying messages between the short range handset radios within the cell and a communication network interface to other carriers, such as the public telephone system network (PTSN). Cellular telephone systems usually operate in the Ultra High Frequency (UHF) band.

The classic pulsed radar concept, on the other hand, involves the transmission of short duration pulses with relatively large time intervals between successive pulses. This sidesteps the difficult problem of detecting the relatively weak signals reflected from the target during the simultaneous transmission of a high power signal. Requirements for range resolution often dictate the use of pulse widths on the order of a microsecond or less, thereby resulting in relatively large bandwidths on the order of MHz. The waveforms used by advanced radars have increased in sophistication:

1. Coherent radars transmit signals whose waveforms are precisely defined;
2. Frequency or phase modulation may be used to increase range resolution;
3. The time intervals between successive pulses (pulse repetition interval) may be varied in a periodic or random sequence (pulse repetition interval stagger);
4. Multi-function radars select between different waveforms depending on the functionality that is required;[1]

Application requirements for high angular resolution and compact antenna dimensions have motivated the extensive use of frequencies above 8 GHz.

The differences between radar and communication signals have motivated the development of specialized ES equipment:

1. Communication ES receivers feature extended frequency coverage to reduce the need to use different receivers, selective filters for separating signals that are closely spaced in frequency, comprehensive capabilities for demodulating the signal message content, and provisions for the measurement of signal parameters;
2. Radar ES receivers provide microwave frequency coverage and are optimized for the reception of pulse signals;
3. Specialized radar ES receivers have been developed for strategic and tactical applications. For example, electronic intelligence receivers are designed for the precision measurement of signal parameters, whereas radar warning receivers are designed to provide warnings of threat signals, be simple to use and satisfy size and cost constraints;
4. Multi-channel receivers have been developed to process multiple signals from antenna arrays with the accurate phase and amplitude matching needed for applications such as direction finding.

General trends in all systems include the use of precision frequency references and synthesizers to permit accurate and repeatable tuning, progressive reductions in size, and the use of form factors permitting the convenient installation of multiple receivers in standardized rack configurations.

[1] For example, the optimal waveforms for discriminating between a moving target on the ground and the surrounding terrain would be unsuitable for providing extreme range resolution.

2.3.1 Communication ES Signal Processing

The classic communication ES receiver implementation is basically a high quality manually controlled superheterodyne receiver. Signal search was performed by the operator manually tuning the receiver through the frequency range known to be used by the adversary's radios and listening to the outputs of the available demodulator(s) for signals of interest. When such a signal was found, the operator would listen to the demodulated signal and record his observations. If available, a DF system would be tuned to the frequency and measurements obtained for the signal angle of arrival. This process required the attention of a skilled operator and had the further weakness that short duration transmissions on new frequencies could be missed, particularly if the frequency ranges to be covered could not be divided up among multiple systems and operators. Another weakness concerned the size, weight and power consumption of the equipment.

Modern purpose-designed communication EW receivers provide significant enhancements:

1. Computer controlled operation via standard digital interfaces;
2. Accurate high speed tuning and reduced phase noise resulting from the use of high quality crystal oscillators as frequency references and sophisticated frequency synthesis techniques;
3. Provisions for phase coherent operation of multiple receivers to allow commonality of hardware between systems used for signal search and DF;
4. Built-in-test functionality;
5. Reduced size, weight and power consumption.

Digital signal processing techniques are being adopted for advanced ES systems. Digital filter bank concepts based on the Fast Fourier Transform (FFT) algorithm allow a single wideband receiver to process and detect the individual signals present within a large instantaneous bandwidth. Also, if the system dwells on a fixed center frequency, digital downconverters (DDCs) can be used to extract the narrowband signals within the receiver bandwidth and software demodulators used to recover the message content from each signal.

Advanced wideband communication ES sensors based on digital filter bank techniques have some very desirable advantages:

1. A large frequency range can be scanned quickly; the tuning frequency step size can be orders of magnitude larger than the required frequency resolution. This substantially reduces or eliminates the likelihood that a short duration transmission will be missed and can provide some capability for detecting at least some of the hops transmitted by a frequency hopping radio;
2. The use of Constant False Alarm Rate (CFAR) techniques allows the system detection processing parameters to be automatically adjusted to achieve the best possible sensitivity without incurring erroneous signal detections at a rate exceeding a set value, even if the environmental noise is frequency dependent and time variant [in07];
3. Algorithms can be implemented to determine the type of modulation used by a signal and the modulation parameters;

4. Raw signal data can be acquired and stored for off-line analysis;
5. Demodulators implemented in software can accommodate a wide range of modulation types;
6. DF functionality can be integrated into the system to provide a measurement of the angle of arrival for each signal that is detected;
7. Reports of signal detections and the measured signal parameters can be automatically stored in a database and transferred to EW analysis and intelligence systems for subsequent processing;
8. Remote controlled or autonomous operation of ES systems is feasible.

However, wideband signal processing techniques also incur disadvantages. Early implementations tended to be expensive and have significant performance limitations. A major problem concerns dynamic range, a measure of the ability of a system to process strong and weak signals simultaneously. This is an issue of considerable importance for wideband communications ES systems since weak signals of interest and strong signals will often coexist in the same frequency range. The dynamic range of a practical system is dependent on the noise and spurious signals, which are generated in the system by various mechanisms. One of the most important of these mechanisms, third order intermodulation distortion (IMD), occurs when two or more signals present within the system bandwidth interact due to non-linearities in the system signal processing. The spurious signals that result remain within the system bandwidth and, depending on the size of the input signals and the nature of the system non-linearities, can be large enough to be detected and interpreted as actual signals in subsequent processing. To avoid this undesirable result, the detection processing must be adjusted to reduce the effective system sensitivity. Thus, the presence of strong input signals tends to degrade the ability of the system to usefully detect and process weak signals. The problem is further aggravated as the system bandwidth is increased since the number of strong signals within the system bandwidth can also be expected to increase. Fortunately, progressive advances in radio frequency components, analog-to-digital converters (ADCs), and digital processor hardware have substantially resolved these issues, particularly when careful system design choices and tradeoffs are made. Nevertheless, a well designed narrowband receiver may still offer advantages with respect to usable sensitivity and selectivity in a dense signal environment that includes strong signals.

In addition to its message content, a communication signal contains information which can be used to classify the type of signal, and, with some limitations, to identify individual emitters.

The measurement of the modulation type and parameters is an important topic for communications ES systems. Conventional communication systems use modulation techniques to embed information on a sinusoidal carrier signal. The choice of modulation type and implementation parameters is dependent on application requirements and various factors, such as the need for interoperability with other radio systems as well as technology and cost constraints. Advances in communication theory coupled with the availability of low cost digital signal processing hardware has motivated the use of sophisticated digital modulation techniques to provide favorable trade-offs between bandwidth efficiency, sensitivity to propagation effects, and hardware implementation costs. At the same time, simple classical modulation techniques, such as analog

frequency modulation, remain in widespread use, in part to maintain interoperability with older systems.

Knowledge of the modulation type and parameters associated with a signal is of considerable practical value. Requirements for interoperability have led to the standardization of the modulation types used by military radios. For example, the tactical VHF radios used in ground operations typically support analog FM and digital FSK modulations in accordance with standards such as MIL-STD-188-242. If a signal has a modulation type and parameters associated with a communication system known to be used by an adversary, it can be flagged as a potential signal of interest and prioritized to receive further attention. Also, since emitters that are communicating with each other will generally use the same modulation type, this knowledge can be used to support or reject hypotheses concerning the membership of a given emitter in a network. Finally, knowledge of the modulation type and parameters facilitates the selection of an appropriate demodulation technique to recover the message content.

Due to the diversity of modulation standards and the effects of multipath propagation and non-ideal radio system implementations, the modulation recognition problem is non-trivial. Algorithms for modulation recognition have been described in various papers, of which [ch89], [na98], [bo00] and [do07] are representative examples.

A related idea is based on the observation that the signal waveforms generated by practical radio transmitters will differ in subtle ways depending on implementation details and component tolerances, and that these differences can be sufficient to distinguish between transmitters that are very similar or even nominally identical. Various techniques have also been proposed to extract and measure appropriately selected features from a signal and use statistical tests to determine if the feature measurements match those of previously observed signals. [ta03], [te04].

2.3.2 Radar ES Signal Processing

Various analog and digital approaches have been used in radar ES receivers to detect signals and measure their parameters. Descriptions and performance analyses of the more common ones have been published [ts95], [ea97], [ma97]. The radar ES receivers used for current radar ES systems deployed for the self-protection of platforms such as aircraft and surface ships generate pulse descriptor words (PDWs) for each radar pulse that is received. Each PDW consists of digital data representing the principal signal parameters, typically frequency, power, time of arrival, pulse duration, and if available, angle of arrival and modulation type (phase or frequency). Early implementations made extensive use of analog techniques to generate PDWs, but more recent implementations are making increasingly extensive use of digital techniques.

Pulse train deinterleaving is required since the pulses that are received from the various radars in the signal environment will be interleaved in time (*i.e.*, in a sequence of received radar pulses there is no certainty that for a given pulse in the sequence, the previous or next pulses in the sequence will be from the same radar). Deinterleaving is typically performed in a two stage process. First, clustering is performed as pulses are received to form clusters or groups of pulses having similar characteristics. A subset of the signal parameters contained in the PDWs, typically frequency, angle of arrival, and pulse duration, are used in this stage. The second stage involves analyzing the time

relationships (Pulse Repetition Interval (PRI) deinterleaving) between the pulses collected in each cluster to identify patterns that are consistent with the hypothesis that they were transmitted by a single radar. In addition to the radar PRI behavior, the radar scan pattern can be inferred by examining the time history of the measured power of received pulses in a deinterleaved pulse train. For example, a radar that is performing a circular scan will illuminate the platform carrying the ES system with its main beam response at uniform intervals in time.

Emitter identification involves comparing the various parameters that have been measured for each of the resultant deinterleaved pulse trains with those in an EW library and identifying the best match.

In practice, there are many potential difficulties. The Pulse Description Words generated by the receiver will contain errors resulting from various sources. At least some of the clusters formed in the first stage will have broad ranges. For example, a large frequency range may be needed to accommodate a frequency agile radar. Consequently, some of the clusters may overlap. Accurate PRI deinterleaving can be very difficult to perform with limited signal data sets; many modern radars have complex PRI staggers (*i.e.*, the time intervals between successive pulses transmitted by a radar vary randomly or follow patterns that repeat only over a long period). Deinterleaving errors can result in the pulse train transmitted by such a radar being fragmented into two or more partial pulse trains. Finally, EW databases can have errors, be incomplete, or as a result of ambiguities, may be unable to provide a unique identification.

More sophisticated approaches are being investigated for the extraction of features that can be used to provide additional information for the classification and identification of radar signals. For radars that use frequency or phase modulation to improve range resolution, knowledge of the type of modulation waveform and its parameters is useful for classification purposes. Also, the waveforms transmitted by radar systems often have distinctive features, sometimes referred to as Unintentional Modulation on Pulse (UMOP). Various techniques have been proposed for the extraction and processing of waveform features for signal identification.

3 Electronic Attack

Electronic attack (EA), also known as Electronic Countermeasures (ECM), involves actions intended to degrade the ability of an adversary to make use of the electromagnetic spectrum. It may be active or passive in nature.

3.1 EA Against Communication Signals

EA against communication signals can be carried out as deception operations or jamming.

Deception operations involve the transmission of signals to intentionally mislead the enemy. For example, after a ground formation has been redeployed for operations elsewhere, simulated radio traffic may be maintained to give the impression that the formation is still in its original location. Another technique involves the transmission of messages that contain misleading information in the expectation that the message content

will be recovered and used by the adversary. Deception operations must be carefully designed and organized to be convincing; the information provided to the intended recipient should be consistent with other information that the intended recipient believes to be true. Large scale deception operations involving carefully co-ordinated activities can influence an adversary's strategic planning with decisive effect. Several accounts of highly successful Allied deception operations in WW2 have been published [jo78], [br76].

Jamming is intended to prevent an adversary from reliably receiving his communication signals by the transmission of signals that interfere with their reception. In the simplest form, a jammer consists of an antenna, power amplifier and signal generator programmed to produce a signal with an appropriately chosen waveform. It is also possible to use a conventional transmitter or radio as an improvised jammer. Jamming systems are often deployed with an adjunct ES capability in order to ascertain the frequencies of signals worth jamming, and to assess the effects of the jamming operation.

To be effective, jamming requires that the ratio of jammer and communication signal powers (J/S ratio) at the victim radio receiver be sufficient to adequately degrade communication activity. This may require the use of high power transmitters in combination with directional antennas, and the judicious positioning of the jammer near the area where jamming coverage is desired.

There are several distinct types of communication jamming techniques:

Narrowband jamming. Individual communication signals can be attacked by transmitting an appropriately designed narrowband jamming signal on the frequency used by the target signal. To determine whether the target signal is still being transmitted, the jamming may be periodically stopped and an ES capability used to check for the presence of the signal. This method of attack has several advantages. First, the jamming range is maximized since the full jamming power is focused on a single signal. Second, the likelihood of interference with own side communication is minimized since only a small part of the radio spectrum is affected. If the jamming signal can be switched rapidly between frequencies, a single transmitter may be able to jam two or more narrowband signals on a time shared basis.

A follower jammer is a special case of narrowband jammer used to jam a frequency hopping signal. The practical implementation of the concept is challenging; each hop transmission must be detected, its frequency measured by the ES functionality integrated with the jammer and, before more than a fraction of the hop is transmitted, the jamming transmitter must be tuned to the hop frequency [bu04]. One difficulty is that the jammer must be able to reliably discriminate between the hops from the target transmitter and any other frequency hopping communication systems that may be operating in the environment. A more fundamental issue concerns the propagation delays associated with, first, the path from the transmitter to the jammer, and, second, the path from the jammer to the victim receiver. If the end result is that the overall delay, including the jammer

response time, approaches the hop duration, the effectiveness of the jamming will be degraded.[2]

Barrage jamming. A wideband jamming signal is used to degrade communication activities over a relatively wide range of frequencies. A high power jammer may be needed to provide a useful range. A partial-band jammer is a variation on the barrage jammer concept. The aim is to jam a bandwidth that is sufficiently large to include a sufficient proportion of the hops transmitted by a frequency hopping radio to make it unusable. The idea is that, by not attempting to jam the full bandwidth used by the frequency hopping radio, the jammer power within the hop bandwidth can be kept higher, and provide an increase in the effective range of the jammer.

Many issues must be considered with respect to communication jamming:

1. Jamming often interferes with own side communication;
2. The value of information that is obtained by ES may be considered to be of greater military value than the effect of disrupting communication;
3. An adversary can infer the presence of enemy forces with EW capabilities from the observation of jamming signals and, if given time, may find ways of countering its effects.

Consequently, aside from some specialized applications, the decision to carry out communication jamming is usually made at a relatively high level and closely co-ordinated with operational plans.

The deployment of communications jammers on aircraft provides several advantages. The jammer is mobile and can be quickly positioned to affect the desired area while minimizing the effect on friendly forces. Also, the required transmitter power can be reduced since, for a given range, the propagation losses are normally much lower than they would be for the signals from a ground based jammer. Recently, serious interest has been expressed in the idea of using low power communications jammers on small UAVs to provide localized jamming coverage in the direct support of small unit operations [go07].

3.2 EA Against Radar Signals

EA against radar signals is often concerned with degrading the performance of surveillance, target acquisition and target tracking radars to protect platforms such as aircraft and surface ships. The value of these platforms and the potential effectiveness of radar guided weapons has led to much emphasis being placed on EA.

Active EA techniques are used to create false targets or otherwise degrade the operation of the victim radar:

1. A noise jammer transmits wideband noise in the frequency ranges used by radar systems of potential concern. This makes it difficult for the radar to detect the target and get a range measurement;

[2] This problem can be avoided if the hop frequency sequence can be predicted using observations of the hop frequencies and *a priori* knowledge of the algorithm used to generate the hop sequence.

2. A range gate pull-off (RGPO) jammer attempts to create a false target that appears to move away from the jammer platform. The jammer first creates a false target at the jammer platform by transmitting a pulse timed to coincide with the arrival of each pulse transmitted by the victim radar. The timing of successive pulses is gradually shifted so that the jammer pulses received by the victim radar correspond to a target that is moving away from the jammer platform. The digital radio frequency memory (DRFM) improves the technique by storing and transmitting a replica of the radar pulse waveform. This makes it more difficult for the radar to discriminate against the jammer signal.

There are several practical problems in the deployment of jammers. The operation of jammers used for the self protection of platforms, such as aircraft, is usually restricted to the jamming of threat signals as required. This minimizes several risks, including the possibility of interference with other systems on the platform, and that the presence of the platform can be inferred by the detection and direction finding of signals transmitted by the jammer. In this situation, an integrated ES capability for performing the detection, characterization and assessment of threat signals is required to provide information needed for the control of the jammer. One way of sidestepping this issue is to deploy jammers on specialized platforms, and if possible perform the jamming outside the defended air space. Other solutions include the towing of jammers behind the platform to be protected, or deploying jammers on unmanned air vehicles (UAVs).

Passive EA techniques attempt to degrade the effectiveness of enemy radars without transmitting signals. A widely used idea is to create false targets by dropping chaff (typically metal coated plastic strips) from aircraft to confuse tracking radars associated with anti-aircraft defense systems. Chaff can also be dispersed via rockets or shells fired from platforms such as ships as a countermeasure to radar guided missiles. Another approach is to tow decoys behind an aircraft or ship. The use of passive EA to confuse the guidance systems of anti-aircraft or anti-ship missiles is often combined with maneuvers designed to position the platform to minimize the likelihood that the missile guidance system will be able to reacquire its target or that the missile will fortuitously pass near its target. Another form of passive EA concerns the use of stealth techniques to reduce the reflected energy returned to a radar transmitter by a platform (*i.e.*, reduce the apparent radar cross section of the platform). The effectiveness of this technique is increased if combined with active EA from other platforms.

Other forms of EA are also important. Radar systems can be destroyed by missiles designed to home in on the signals transmitted by the radar. Conventional military operations against deployed systems identified by EW sensors or other intelligence are also possible. Recently, the concept of using directed energy or electromagnetic pulse (EMP) to damage or disrupt the operation of electronic equipment has received attention.

4. Electronic Protection

Electronic protection, also known as electronic-counter-counter measures (ECCM), concerns techniques and technologies intended to preserve the ability of defense electronic systems to operate in hostile electromagnetic environments.

Active EP includes measures taken to enhance the ability of defense electronic equipment to operate without hindrance by enemy EW.

Protection against intercept and jamming of communication signals can be provided in various ways:

1. Equipment can be designed to operate over wide frequency ranges. This offers improved opportunities for a system to switch to quieter frequencies if interference or jamming is encountered;
2. Directional antennas can be employed to make the interception of a signal difficult for a receiver outside the main beam response of the transmitting antenna. Jamming resistance can be achieved if the direction that the jamming signal is coming from corresponds to a null in the receiving antenna directional response.
3. Careful choices of sites may be able to take advantage of terrain masking of areas potentially usable by jammers or ES systems;
4. Power management allows the transmitter power to be set at the minimum level required for reliable communication. Low power operation is desirable for short range communication since the range at which the signal can be detected and intercepted is reduced. High power levels can be used to provide reliable operation over longer ranges and/or overcome jamming;
5. Low Probability of Intercept (LPI) techniques can be used to render DF and intercept difficult. Frequency Hopping (FH) techniques are widely used by modern tactical radios;
6. Redundancy can be achieved by design and/or tactical procedures to limit the damage caused by the effects of enemy EA; for example, different types of communication systems can be networked and managed to ensure that the disruption of one system does not prevent the communication of important information.

Similar techniques are applicable to radar systems with several differences:

1. A radar system may be able to search over a restricted range of angles and still perform its mission requirements. An ES system outside the search area will not be illuminated by the mainbeam of the radar antenna and may have difficulty detecting the signals;
2. Radar antennas are generally designed to be highly directive to provide angle resolution. However, antenna designs that also achieve low sidelobe levels are desirable for several reasons. First, sensitive ES systems can usefully detect pulses corresponding to the antenna sidelobes if these are sufficiently large. Second, some jamming techniques make use of signals that are received through sidelobes in the radar antenna response and therefore confuse the radar into showing a target at an angle offset from the jammer;
3. Frequency agility involves changing the transmitter frequency pulse to pulse or between groups of pulses. It has some similarities to the use of frequency hopping by communication systems, though the primary ideas are to complicate the task of an ES system in interpreting whether the received pulses are from one or more radars, and to reduce the effectiveness of single frequency jammers.

4. LPI radars tend to use continuous wave (CW) signals with frequency or phase modulation to provide the desired range resolution. Technical considerations generally restrict the average transmitter power with the result that they are most suited to applications where long range is not required. Against these signals, conventional radar ES systems are usually limited to very short detection ranges due to the low transmitter power and the effect of receiver optimizations for the processing of short duration pulse signals.[3]

Passive EP generally places considerable emphasis on training and operational procedures. Some of the most spectacular EW successes, such as the decryption of messages ciphered by the German Enigma machine in WW2, resulted, at least in part, from the failure of radio operators to follow correct procedures. There are many possible ways in which the security of communication systems can be compromised. Examples include the transmission of unimportant or unnecessarily long messages, the repeated transmission of the same message with and without encryption, the failure to use code words and available EP capabilities, such as power management, frequency hopping, and encryption, and the failure to safeguard encryption equipment and keys. The likelihood of such lapses can be substantially reduced by the institution of suitable procedures followed by training under realistic conditions.

Emission Security (EMSEC) is policy defining procedures and techniques for minimizing the possibility of sensitive information being obtained from the intercept of RF signals that are unintentionally generated in the operation of computer or other electronic systems.

In field or operational environments, tactical EP strategy is set by Emission Control (EMCON) orders, which define specific rules for the management of electromagnetic emissions [ew07] during a military operation. These rules attempt to strike a balance between various requirements:

1. Maintaining command and control capabilities;
2. Limiting mutual interference between friendly systems;
3. Limiting the useful information that enemy ES can provide;
4. The execution of deception operations.

EMCON rules include

1. Restrictions on transmit power times and use of radio black-out policy;
2. Guidelines, such as frequency allocations and approved system configurations;
3. Restrictions on the type of information that can be transmitted (and thus denied to the enemy);

5. Additional Topics

[3] An interesting idea is to use commercial FM radio stations as a transmitter in a bistatic radar system. The receivers are located some distance from the transmitter and the signal processing is designed to measure the relative time shifts between the signal that propagates directly from the transmitter to the receiver and the signal that arrives via a reflection from the target.

5.1 EW and Navigation Systems

Before WW2, specialized direction finding systems were developed for navigation purposes. By determining the angles to radio stations or beacons at known locations, it was possible to obtain position estimates, that while of limited accuracy, were still very useful, particularly at night and in bad weather. During WW2, more sophisticated systems were developed and deployed. Examples include Knickebein, X-Gerat, Y-Gerat, Decca Navigator, GEE, G-H, and Oboe.

Various efforts were made to jam the signals associated with these systems, particularly those used for bombing navigation.[4] Luftwaffe attempts to use the Knickebein, X-Great, and Y-Gerat navigation systems to guide bombers to targets in the UK were successfully countered by jamming, though a series of damaging raids was conducted using the X-Gerat system before effective jamming techniques were devised [jo78]. German attempts to jam allied systems, such as GEE and Oboe, were generally less successful.

For example, by the time successful jamming was achieved against Oboe signals at 200 MHz, the Mark III version had moved to 3 GHz, a frequency where the technical capabilities of the Germans were inadequate for the implementation of effective countermeasures.

In addition, both sides made efforts to interfere with enemy radio beacons, sometimes with the result that aircraft got lost or were even captured after landing in unfriendly territory.

After WW2 various navigation systems were developed and deployed. More recently, the GPS system has become very important, particularly in Western countries, due to the availability of world-wide coverage and the high accuracy that can be achieved. This has led to the widespread use of GPS for the guidance of precision weapons and defining target locations. The military importance of GPS has motivated the development and marketing of GPS jammers. At the same time, recognition of the potential impact of GPS jamming has resulted in serious efforts to develop and implement anti-jam features in military GPS systems [ro04].

5.2 EW and IFF Systems

Identification Friend Foe (IFF) systems are used to provide a means of quickly and positively identifying friendly aircraft. When an unknown aircraft is observed, the IFF system transmits a specially coded signal and looks for the transmission of an appropriate signal in response from the IFF system in the unknown aircraft.

After early IFF systems were deployed in British bombers during WW2, the Germans discovered that the bombers could be tracked by transmitting signals to trigger their IFF systems and observing the IFF signals transmitted in response. Significant losses of aircraft resulted until it was realized that the IFF signals were being exploited and the systems were removed from the aircraft [jo78]. Since then, significant efforts have been made to reduce the vulnerability of modern IFF systems to EW.

[4] Investigations in the UK revealed that bombing attacks carried out at night were often ineffective without the use of electronic navigation aides [jo78].

5.3 Countermeasures Against IR Sensors

Passive Infrared (IR) sensors have important military applications [hu75]. Anti-aircraft missiles using IR guidance systems have proven to be very effective in the absence of effective countermeasures, particularly for low altitude air defense. Other important applications include ground-to-air and air-to-ground target acquisition, fire control, and night vision. In ground combat, the use of IR sensor technology has greatly increased the effectiveness of operations at night and under conditions of bad weather and haze. The usefulness of IR sensors has been progressively enhanced by technical advances in IR detectors and the processing of their outputs. IR sensors have been evolved to operate in both the long wave infrared (LWIR) and mid-wave infrared (MWIR) bands. These dual-band sensors can provide robust performance over a wide range of environmental conditions.

The importance of IR sensors has motivated the expenditure of considerable effort on the development of technology and techniques designed to reduce the effectiveness of IR sensors and their associated weapon systems. This work is very comprehensive and includes modeling and experimental measurements of the IR radiation emitted by platforms, such as ships and aircraft, and the behavior of threat IR sensors.

Flares have been widely used as decoys to distract the IR sensor based missile guidance systems for the protection of aircraft. The use of flares is often combined with evasive action to help ensure that the missile guidance system continues to track the flare and that the missile's path towards the flare does not take it near the aircraft. Infrared Counter Measures (IRCM) systems generate an IR signature whose power is modulated in a way that is intended to confuse the tracking system associated with typical IR sensor based guidance systems. Directional Infrared Counter Measures (DIRCM) systems extend the IRCM concept further by directing the modulated IR energy towards the threat sensor. Another idea is to use a laser to blind the IR sensor.

IR deception techniques for aircraft have achieved significant successes against more basic IR sensors. However, the development of increasingly sophisticated IR sensors has necessitated continued work on the development of IR countermeasures.

Improvised IR deception measures have been used with some success to simulate ground targets.

The reduction of IR signatures associated with platforms, such as surface ships and aircraft, can significantly improve their survivability. Various measures have been used:

- Cooling visible exhaust duct metal surfaces with air or water;
- Shrouding visible exhaust duct metal surfaces;
- Cooling engine exhaust plumes by mixing them with cool ambient air;
- Cooling exposed surfaces heated by the sun with water;
- Coating exposed surfaces with low emittance materials;
- Covering ground based assets with IR camouflage netting.

6. Future Trends in EW Technology

The evolution of EW technology and concepts is driven by various factors, including changing operational requirements and technology advances. Future systems will provide significant capability enhancements and other benefits:

1. The development and widespread deployment of capable cell phone networks and their adoption for military purposes means that ES, even at the tactical level, cannot be limited to explicitly military communication systems;
2. Requirements to shorten development cycles and reduce cost will favor increasing use of commercial-off-the-shelf technology and open standards; The implementation of digital signal processing algorithms in software and hardware based on Field Programmable Gate Array (FPGA) technology and general purpose processors provides flexibility and performance advantages;
3. Specialized systems will tend to be replaced by multi-function systems. The concept of integrating ES and EA functionality with communication and radar systems will receive increasing attention [ta05];
4. Networking of EW assets and technical advances will tend to blur the distinction between tactical and strategic EW;
5. Simulators and other aids are being developed to provide realistic scenarios for EW training without requiring large scale exercises and/or expensive equipment;
6. Models and simulations will be increasingly used to assess EW effectiveness with the aim of determining appropriate system design trade-offs and contributing to the development of EW doctrine;
7. Automated ES and EA systems will be added to the sensors carried by UAVs and platforms such as reconnaissance vehicles;
8. Smart antennas will improve the robustness of communication systems in a jamming environment;
9. The future development of aircraft and naval platforms will place increasing emphasis on signature management;
10. Decoys will be increasingly used for platform protection.

In practice, the application of technical advances will be moderated by various practical issues: There are always competing priorities for personnel and funding. Sophisticated EW systems are often very expensive to develop and deploy and can be quickly rendered obsolescent by technology advances and changing application requirements. The development of sophisticated defense electronics systems presents formidable challenges. Many systems fall far short of initial expectations for various reasons, ranging from faulty technology or trade-off analyses, the failure of anticipated technical advances to materialize, and changing application requirements. The problems involved with the introduction of advanced technology systems into service are considerable:

- Integration into platforms;
- Integration with other systems;
- Provisions made for maintenance;

- Development of suitable doctrine;
- Provisions for interoperability with allied forces;
- Training of users.

It is very easy to underestimate some of these issues. An otherwise capable system may be completely unsuitable for service use if the user interface is poorly thought out. A system may work well in the hands of skilled engineers who have an intimate understanding of its operation, but, in an operational environment, be virtually unusable by service personnel, even if they have substantial training and experience. Another common problem is that the networking of battlefield sensors tends to require considerable communications capacity. This may not be available, or if provided by communication satellites, be prohibitively expensive.

References

[ar85] M. Arcangelis, *Electronic Warfare: From the Battle of Tsushima to the Falklands and Lebanon Conflicts*, Blandford Press, Dorset, United Kingdom, 1985.

[bo00] D. Boudreau, C. Dubuc, F. Patenaude, M. Dufour, J. Lodge, R. and Inkol, "A fast automatic modulation recognition algorithm and its implementation in a spectrum monitoring application," Proceeding of MILCOM 2000, October 2000.

[bu04] K. Burda, "The Performance of the Follower Jammer with a Wideband-Scanning Receiver," Journal of Electrical Engineering, Vol. 55, NO. 1-2, 2004.

[ch82] P. C. Chestnut, "Emitter Location Accuracy Using TDOA and Differential Doppler," IEEE Transactions on Aerospace and Electronic Systems, March 1982.

[ch89] Y. T. Chan and L. G. Gadbois, "Identification of the modulation type of a signal," Signal Processing, vol. 16, no. 2, February 1989.

[do07] O. A. Dobre, A. Abdi, Y. Bar-Ness, and W. Su, "Survey of automatic modulation classification techniques: classical approaches and new trends," IET Communications, Volume 1, Issue 2, April 2007.

[ea85] P. W. East, "ESM Range Advantage," EE Proceedings, Vol. 144, Pt. F, No. 4, July 1985.

[ea97] P. W. East, "Microwave Intercept Receiver Sensitivity Estimation," IEE Proceedings, Radar, Sonar and Navigation, Vol. 132, No. 4, August 1997.

[el06] D. Elsaesser, "The Discrete Probability Density Method for Target Geolocation," Canadian Conference on Electrical and Computer Engineering, May 2006.

[es07] D. Eshel, "EW in the Yom Kippur War," Journal of Electronic Defense, Vol . 30, No. 10, October 2007.

[ew07] Joint Publication 3-13.1, Electronic Warfare, 25 January 2007.

[go07] G. Goodman, "New Challenges for Ground EW – Democratized Jamming," Journal of Electronic Defense, Vol . 30, No. 10, October 2007.

[ha02] R. J. Hanyok, "Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975," Center for Cryptologic History, National Security Agency, Volume 7, 2002.

[hi97] P. Hill, E. Adams, and V. Comley, Techniques for Detecting and Characterizing Covert Communications Signals," European Conference on Security and Detection, April 1997.

[hu75] R. D. Hudson, "The Military Applications of Remote Sensing by Infrared," IEEE Proceedings, Vol. 63, Issue 1, January 1975.

[in07] R. Inkol, S. Wang, and S. Rajan, "FFT Filter Bank-Based CFAR Detection Schemes," Proceedings of Midwest Symposium on Circuits and Systems, August 5-8, 2007.

[ja05] M. Streetly (editor), *Janes Radar and Electronic Warfare Systems 2005-2006*. Jane's Information Group, 2005.

[jo78] R. V. Jones, *Most Secret War*. Hamish Hamilton, 1978.

[ki87] N. King, I. Pawson, M. Baker, R. Shaddock, and E. Stansfield, "Direction Finding," US Patent 4,639,733, January 27, 1987.

[li03] S. E. Lipsky, *Microwave Passive Direction Finding*. SciTech Publishing, 2003.

[ma97] D. E. Maurer, R. Chamlou, and K. O. Genovese, "Signal Processing Algorithms for Electronic Combat Receiver Applications," John Hopkins APL Technical Digest, Volume 18, Number 1, 1997.

[mc05] R. A. McDonald and S. K. Moreno, "Raising the Periscope … Grab and Poppy: America's Early ELINT Satellites," Center for the Study of National Reconnaissance, National Reconnaissance Office, Chantilly, VA , September 2005.

[mi07] P. Mihelich, "Jamming Systems Play Secret Role in Iraq," http://www.cnn.com/2007/TECH/08/13/cied.jamming.tech/index.html.

[na98] K. Nandi and E. E. Azzouz, "Algorithms for Automatic Modulation Recognition of Communication Signals," IEEE Transactions on Communications, Vol. 46 NO. 4, April 1998.

[po02] R. Poisel, *Introduction to communications electronic warfare systems*. Artech House, 2002.

[po05] R. Poisel, *Electronic Warfare Target Location Methods*. Artech House, 2005.

[pr 00] A. Price, *The History of US Electronic Warfare, Volume III, Rolling Thunder Through Allied Force, 1964 to 2000.* Artech House, 2000.

[pr78] A. Price, *Instruments of Darkness: The History of Electronic Warfare*. Encore Editions, November 1978.

[pr84] A. Price, *The History of US Electronic Warfare, Volume 1, The Years of Innovation – Beginnings to 1946*. Artech House, 1984.

[pr89] A. Price, *The History of US Electronic Warfare, Volume II, The Renaissance Years, 1946 to 1964.* Artech House, 1989.

[re99] W. Read, "An Evaluation of the Watson-Watt and Butler Matrix Approaches for Direction Finding," DREO Technical Report 1999-092, September 1999.

[ro04] S. Rounds, Jamming Protection of GPS Receivers, GPS World, January 1 and February 1, 2004.

[sc86] R. O. Schmidt, "Multiple Emitter Location and Signal Parameter Estimation," IEEE Transactions on Antennas and Propagation, Vol. AP-34, March 1986.

[sc99] D. C. Schleher, *Electronic Warfare in the Information Age*. Artech House, 1999.

[st47] R. G. Stansfield, Statistical theory of DF fixing, Journal of IEE, December 1947.

[ta03] K. I. Talbot, P. R. Duley, and M.H. Hyatt, "Specific Emitter Identification and Verification," Northrop Grumman Technology Review Journal, Spring/Summer 2003.

[ta05] G. C. Tavik et al, "The Advanced Multifunction RF Concept," IEEE Transactions on Microwave Theory and Techniques, Vol. 53, No. 3, March 2005.

[te04] O. H. Tekbas, N. Serinken, and O. Ureten, "An experimental performance evaluation of a novel transmitter identification system under varying environmental conditions," Canadian Journal of Electrical and Computer Engineering, vol. 29, no.3, July 2004.

[to84] D. J. Torrieri, "Statistical theory of passive location systems," IEEE Transactions on Aerospace and Electronic Systems, vol. 20, March 1984.

[ts95] J. B. Tsui, *Microwave Receivers with Electronic Warfare Applications*. Wiley, 2005.

[wi06] R. G. Wiley, *ELINT: The Interception and Analysis of Radar Signals*. Artech House, 2006.

Appendix 1 - Geo-location of Signal Sources for Communications and Radar ES

1 General Concepts

Several fundamental properties of electromagnetic waves can be used for the geo-location of signal sources:

- the signal propagates at a constant known velocity;
- the phase surfaces are perpendicular to the direction of propagation;
- the electric and magnetic field vectors are perpendicular to the direction of propagation.

In free space, the signal appears to spread out radially from a source and arrive at a receiver via a line-of-sight path. Various techniques have been developed to exploit these properties to obtain lines of position for the transmitters associated with radio, radar and navigation systems. Using measurements from a sufficient number of sites, the locus of positions for an emitter can be uniquely solved. In practice the problem can often be usefully simplified by the assumption that the source and sensor sites are located on a plane. If errors can be neglected, the resulting lines of position (LOPs) pass through the position of the signal source, thereby resulting in an unambiguous position estimate. The process of solving the location of a signal source from the LOPs is known as triangulation. In practice, various error sources will affect the estimated LOPs and, with multiple lines of position, the intersections of the LOPs will occur at multiple points or, in some cases, fail to occur. Many sources of error are present in practice:

1. Environmental noise and interfering signals;
2. Thermal noise and spurious signals generated within the sensor;
3. Mutual coupling between the pairs of elements in an antenna array;
4. Gain and phase mismatches in cables and receivers used in systems that use multiple receivers to measure gain or phase differences;
5. Uncertainties in the positions of the sensors;
6. Propagation effects;
7. Geometric factors due to the relative location of the emitter and sensors.

In a ground-based environment, propagation effects are very important. The received signal will usually arrive at the sensor via multiple paths (multipath propagation) caused by reflections from terrain features and man-made structures. Many of these error mechanisms will result in systematic bias errors which cannot be removed by averaging. However, various possibilities exist for minimizing the effects of error sources:

1. Careful positioning of sensor sites to minimize terrain masking of areas of interest and local reflections, and provide favorable source-sensor geometries;
2. The elevation of the sensor antenna on a suitable mast;
3. Increasing the number of sensors.

The statistical behavior of errors arising in estimating the position of a source, and their sensitivity to measurement errors, has been extensively analyzed for various geo-location techniques [st47], [ch82], [to84]. Algorithms for making the best use of available information from sensor arrays have been developed [po05], [el06].

2 Direction Finding Techniques

Direction finding (DF) is based on the idea of directly measuring the direction that the signal wave front is propagating. Extensive research has been applied to the development of DF techniques. Moreover, there are many design variables and available implementation technologies. Consequently, the design of practical DF systems reflects the trade-offs that are relevant to the specific application requirements. The most common ideas [li03], [ch07], [po05] are summarized in the following sections.

2.1 DF Techniques Based on Amplitude Measurements

The most basic form of direction finding is to perform an angular search using a directional antenna whose directional characteristics are known and find the angle at which the received power is either a maximum or a minimum. The choice depends on whether a well defined maxima or null in the directional response exists. The antenna can be continuously rotated and a suitable electro-mechanical system used to display the angle corresponding to the minimum received signal power. One limitation of this scheme concerns the difficulty of measuring the DF of a signal that is present for a short duration. Nevertheless, some DF systems for radar ES are based on the use of a rotating parabolic reflector antenna. The relative simplicity, coupled with the capability against weak signals provided by the high antenna gain partly compensates for the other limitations.

Amplitude comparison DF is a more sophisticated idea. The desired angular coverage is divided into sectors and each sector is associated with a directional antenna having a beam width comparable to the angular width of the sector and a receiver that is designed to measure the amplitude of an observed signal. The angle of arrival is determined in two stages. First the pair of receivers associated with the largest signal power measurements is found. A coarse estimate of the angle of arrival is defined as the mid-angle between the angles that each of the antennas is pointed. Second, the angle of arrival estimate is refined by computing the ratio of the amplitudes, and using a look-up table, or a calculation based on a model of the directional gain of the antennas, to produce a fine angle estimate. There is a trade-off between the number of antennas and the achievable accuracy. This technique is often used in radar ES systems; it is relatively straightforward to implement, and, for microwave frequencies, the antennas are relatively compact. RWRs used in fighter aircraft often use four antennas to provide 360 degree angular coverage, whereas ES systems for naval craft often use six or eight antennas.

Many Communications ES systems use amplitude comparison DF techniques based on the Adcock pair antenna. This consists of two adjacent vertical monopole or dipole antenna elements whose output signals are combined to provide the vector difference of

the two output signals. The result is a figure 8 gain pattern with the null occurring for signals that propagate across the baseline of the antenna elements. The separation of the antenna elements involves a compromise depending on the frequency range to be covered. Too close a spacing reduces the sensitivity whereas too large a spacing results in a distorted gain pattern. The Watson-Watt DF system, in its simplest form, consists of two Adcock pairs oriented at right angles. The angle of arrival of a received signal can be directly determined from the ratios of the signal powers measured from the two Adcock antenna pairs. With some additional processing, an unambiguous DF measurement can be obtained. At the cost of increased size and complexity, improved performance and frequency coverage can be obtained by using four Adcock pairs.

2.2 Interferometric DF Systems

The basic interferometric DF system consists of a pair of monopole or dipole antenna elements that are separated by less than half a signal wavelength and the means for measuring the phase difference between their output signals. Using the measured signal frequency, the known signal propagation velocity and the antenna separation, the signal angle of arrival with respect to the antenna baseline can be computed. The angle of arrival measured for this arrangement is ambiguous; the signal can arrive from either side of the baseline. This limitation can be resolved by adding one or more antennas to form a two dimensional array, computing the angles-of-arrival for each antenna pair and determining the value for an unambiguous angle of arrival that is most consistent with the individual results. One implementation uses an array of five antennas positioned in a regular pentagon to form ten antenna pairs, five of which correspond to the faces of the pentagon and the other five to the diagonals [ki84].

The interferometric direction finding technique is expensive in hardware. Each antenna in the array requires a dedicated channel from a multichannel receiver having accurate phase matching between the channels. Digital signal processing techniques facilitate the implementation of such systems, one point being that phase matching errors can be corrected by measuring them with a suitable calibration signal, storing their values in a table, and using the stored calibration data to correct subsequent measurements. The correlative DF techniques used by some systems are a further development of this concept. Well designed interferometric DF systems have a relatively good reputation for accuracy, particularly when a large antenna array is used.

2.3 Single Channel DF Systems

To minimize size, cost, weight and power consumption, several DF system implementations have been developed that require only a single channel receiver. The pseudo-doppler DF technique is distinguished by the use of a circular array of uniformly spaced antennas with a commutator switch that sequentially connects one antenna in the the array at a time to the receiver. The effect is analogous to moving a single antenna element on a circular track and contributes a sinusoidal phase modulation to the received signal. An estimate of the angle of arrival is obtained by measuring the relative phase

shift of this modulation component. The Watson-Watt technique has also been successfully applied to single channel DF systems.

Single channel DF techniques are widely used for low cost portable systems. However, a relatively long observation time is needed compared to the conventional Watson-Watt and interferometric techniques.

2.4 Other DF Techniques

Other DF techniques are possible and have some advantages. Circular antenna arrays using the Butler matrix network can provide unambiguous DF with a receiver having as few as two channels. A theoretical comparison of their performance with other techniques is given in [re99]. Super resolution techniques, such as the multiple signal classification (MUSIC) algorithm [sc78], have the ability to resolve multiple signal sources in angle, even when their signals overlap in frequency. However, the large antenna arrays and the cost of the associated receiver and processing hardware are difficult to justify for most applications.

Attempts have been made to use power measurements to provide an indication of range. This presents some difficulties. The actual power radiated by a transmitter is dependent on various factors including the antenna configuration, height and the selected transmitter output power (if this functionality is available). Furthermore, in a ground environment, propagation losses depend on the nature of the terrain. The usefulness of power measurements increases if measurements are available from multiple sites.

3 Time Difference of Arrival and Frequency Difference of Arrival Geo-location Techniques

The basic concept of geo-location using time difference of arrival (TDOA) measurements can be illustrated by considering a pair of spatially separated receivers and a signal source at an unknown location. Given the assumptions of line of sight propagation paths and fixed signal propagation velocity, the signals observed at the receivers arrive at the receiver sites with delays proportional to the distances from the signal source to the receivers. The difference in delays corresponds to the TDOA.

Given a TDOA measurement and knowledge of the signal propagation velocity, and the receiver locations, the locus of possible transmitter positions can be solved. If the problem is simplified to two dimensions by assuming the signal source and receivers lie on a plane, the resulting line of position is a hyperbola. Given three or more receivers, the hyperbolic lines of position obtained for the different pairs of receivers will intersect at the signal source location if sources of error can be neglected.

There are two basic approaches for measuring TDOAs. The first is applicable if there is a time domain feature of the signal waveform that can be easily identified. For example, the time of arrival (TOA) of a pulse modulated signal can be measured by performing amplitude demodulation to obtain the pulse waveform and measuring the absolute time corresponding to a suitable reference point on the leading edge of the pulse waveform,

such as the point where the pulse reaches a fixed fraction of the peak power level. The TDOA can then be obtained by taking the difference between the corresponding TOAs observed at two locations. The second requires that the signals from the receiver sites be relayed to a single site where the relative time differences are measured using signal processing techniques, such as cross-correlation.

TDOA based geo-location techniques involve several complications. The requirement for the accurate measurement of very small relative time delays necessitates carefully designed and engineered systems. If the signals received at the separate sites must be relayed to a common site for processing, the requirements for suitable data links may involve issues of cost and practicality. Nevertheless, TDOA geo-location techniques have some attractive advantages:

- specialized receiving antennas are not required;
- the orientation of the receiving antenna is not critical;
- there are ways of confirming that a signal received at different sites is from the same transmitter;
- the accuracy is relatively unaffected by multipath propagation occurring in the immediate vicinity of the receiver sites.

The differential frequency shifts resulting from relative motions of the transmitters and receivers complicates the signal processing needed for TDOA estimation. With suitable processing, these frequency differences can be estimated and used to define lines or surfaces on which the signal source lies. FDOA based techniques are primarily applicable to airborne or satellite platforms and can be combined with geo-location based techniques based on TDOA measurements.

4 Minimization of Error Sources

The performance of practical geo-location systems can be improved in several ways.

4.1 DF Techniques

The performance of DF systems can vary widely, depending on the implementation and choice of deployment sites:

1. System design choices and trade-offs need to be carefully considered. Antenna arrays with large baselines tend to have performance advantages, but are generally undesirable for tactical applications. Conversely, attempts to cover a large frequency range with a single antenna array involve significant performance compromises;
2. Gain and phase mismatches contributed by the receiver hardware and the cables between the antenna and receiver can be corrected by measuring the errors and subtracting them from future measurements. The errors can be measured by using a suitable signal source and radio frequency switch to

apply a calibration signal at the point where the cables connect to the antenna. Gain and phase mismatch errors can be measured at suitably chosen test frequencies and used to construct a calibration table containing the amplitude and phase correction factors required at each of the test frequencies;

3. Systematic errors contributed by the antenna can be corrected using a calibration table to provide correction values to be subtracted from the measurements. A one dimensional calibration table can be constructed by carrying out controlled tests using signals transmitted from a fixed angle at frequencies spaced through the frequency range covered by the system and measuring the discrepancy between the actual and observed angles. Since the errors will generally have be angle dependent, the use of a two dimensional calibration table is desirable. This can be constructed by the repeating the procedure for angles distributed around the full 360 degree interval. Interpolation can be used to generate calibration values for intermediate frequencies and angles.
4. The choice of sites for the deployment of DF systems is critical. Ideally, the site should be free of features contributing to multipath propagation and line of sight propagation should be possible over the area of interest. In these respects, the elevation of the antenna is an important factor. Another consideration is to that the sites should be selected to provide favorable sensor-target geometries for geo-location via triangulation.
5. Geo-location performance improves as the number of sites from which DF information is available increases.

4.1 TDOA and FDOA Techniques

The performance of TDOA and FDOA geo-location systems is sensitive to system implementation choices, the nature of the signals of interest, and various aspects of the system deployment:

1. If the system operation is dependent on the relaying of signals received at the sensor sites to a common site for processing, the system must be able to perform this function without significantly degrading the quality of the signals.
2. Provisions must be made to account for the delays contributed by the relaying of the signals observed at the sensor sites to a common site must be removed or accounted for.
3. The performance of TDOA estimation processing depends on the signal-to-noise ratio and the presence of suitable information contained in the signal modulation. Narrowband signals may require higher signal-to-noise ratios and/or longer observation times to achieve the desired accuracy;
4. Frequency shifts resulting from relative motions of the receivers and transmitter affect TDOA measurement processing. If, for scenarios of interest, they are sufficiently important, provisions must be made in the TDOA estimation processing to remove them. If FDOA information is

used for geo-location, the most favorable results will be obtained when the sensors move rapidly since this increases the relative frequency shifts and a given error in frequency measurement becomes less significant. Also, this reduces the effects of frequency shifts contributed by the movement of the signal source.