Chapter 2
Electronic Defence Systems

2.1 Introduction

Electronic Defence (ED) is defined as the art and science of preserving the use of the Electro-Magnetic (EM) spectrum for friendly use while denying its use to the enemy [157]. The inherent value that the EM spectrum has as a natural resource, which is utilized and/or abused, is a pivotal reason why ED has such a vested interest in preserving its use. ED protects the spectrum by utilizing task specific passive ED receiver systems and ED transmitter systems (i.e. Jammers). ED receiver systems (falling within the sub-category of electronic support (ES)) are designed to detect, monitor and locate EM radiation sources (Friend or Foe), whereas ED countermeasures are designed to reduce the effectiveness of threats (i.e. Enemy EM radiation sources).[1]

Concerning communication operations, the EM spectrum that is utilized commercially and for exclusive military use, occupies large sections/bands of the Electromagnetic spectrum (i.e. FM, AM, GSM, UMTS, LTE, WiFi, WiMax, etc.). As is the case with supportive measures, monitoring/sensing certain bands of interest is a typical technique to ensure that the spectrum usage is preserved. As a consequence other operative tasks become available, allowing for tracking capability and intercepting communications for intelligence gathering.

In this chapter we develop a critical literature review, detailing the context of ES in the domain of ED and its application as well as implementation for communication systems. We deal with a wide range of topics starting from ED passive communication systems (namely Electronic Support (ES) receivers), operations for detection, communication techniques, RF propagation theory to direction finding.

[1]Both ED receiver and transmitter systems are designed by sourcing from multi-disciplinary fields such as radar, communications, digital signal processing, antenna theory, radio frequency systems, high performance computing and computer networks to preserve the EM spectrum with high effectiveness for the user.

A.K. Mishra and R.S. Verster, *Compressive Sensing Based Algorithms for Electronic Defence*, Signals and Communication Technology,
DOI 10.1007/978-3-319-46700-9_2

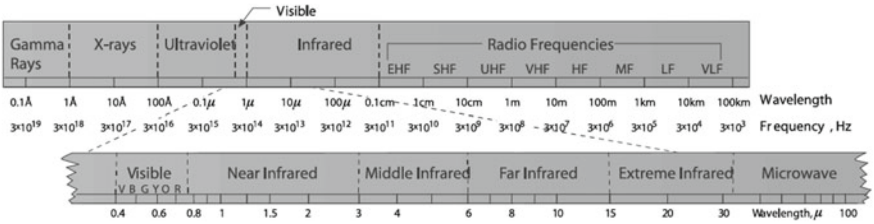

Fig. 2.1 Illustrates the electromagnetic spectrum usage in terms of frequency and wavelength, sourced and adapted from [99]

2.1.1 Electronic Defence Overview

ED systems sense and monitor the EM spectrum. The frequencies that comprise the EM spectrum range from Alternating Current (AC) to Gamma rays, which from a governing and/or controlling entity's (i.e. ED systems) point of view, is an enormous band to sense and determine the usage thereof.

ED domain utilizes full extent of this usable electromagnetic (EM) spectrum namely the radio frequency, infra-red, optical and ultraviolet spectrum [2]. Usability of the EM spectrum is detailed in Fig. 2.1.

Classically, ED has been divided into following three domains.

- Electronic Support Measures (ESM),
- Electromagnetic countermeasures (ECM).
- Electromagnetic counter-countermeasures (ECCM).

However, in recent years these subdivisions were renamed and redefined under the guidance of NATO [2]—now widely accepted in many countries, but not all.

Under the previous definition[2] the ED subdivisions were understood as follows (see Fig. 2.2 for detail).

- **ESM**—Receiver systems, mainly used for intercept purposes in ED.
- **ECM**—Jamming, chaff, flares used for the sole purpose to counter systems such as radars, military communication and weapon systems.
- **ECCM**—Design or operational measures taken to counter radar and communication systems against the effectiveness of ECM.

Under the newly redefined view of NATO, ED subsystems/divisions are now defined as Electronic Support (ES), Electronic Attack (EA) and Electronic Protect (EP) subsystems. These three divisions are detailed below. In Sects. 2.1.2–2.1.4 we shall describe how these divisions include classical definitions which can be correlated to Fig. 2.2.

[2]Definitions sourced and modified from [1, 2].

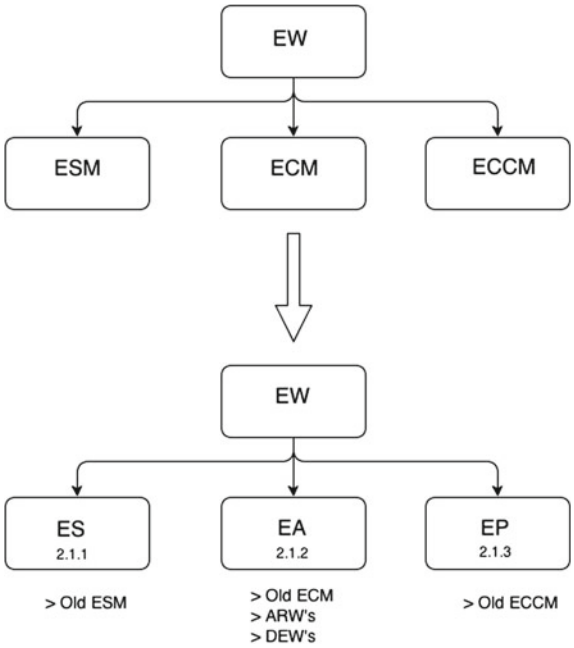

Fig. 2.2 Illustrates the classical definition subdivision of the ED domains for operational tasks

- **ES**—This is the same as the classical definition of ESM.
- **EA**—This is same as the previous ECM including jamming, chaff, and flares. Also including anti-radiation weapons and direct energy weapons.
- **EP**—This is identical to the classical ECCM definition.

For clarity, it is important to distinguish ESM (or ES) from signal intelligence (SIGINT) which contains two streams of intelligent systems, namely communication intelligence (COMINT) and electronic intelligence (ELINT) [2]. Differentiation between these types of signal has become increasingly vague—as signal complexity develops—for the purpose of transmissions received [1].

Purpose of the respective subdivisions:

- **COMINT**—The operational tasks involve receiving communication signals for the purpose of extracting intelligence from the data/information carried by the signals of interest.
- **ELINT**—These operations are interested in non-communication signals (i.e. radar signals) to determine the type of electromagnetic system in use by an enemy, in order to develop a counter measure. ELINT systems typically collect a large amount of data over an extended period of time.
- **ES/ESM**—The modus operandi of ES is to collect, intercept, identify and locate enemy signals [3] in order to execute a specific task relative to the threat level that the received signal holds. The signal can also be employed for situational awareness [1]. In other words, the signal can be used to determine the types and

locations of enemy weapons or electronic capabilities. ES systems typically need to optimize data throughput whilst gathering a considerable amount of real time data. The main objective of such systems is to determine which emitter types are present and where they can be located.

The majority of the objectives, and hence the operational tasks for this monograph, will be focused within the domain of ES. However, due to the nature of exclusively dealing with communication signals, certain aspects of COMINT will be included for a holistic approach of the topic.

2.1.2 *Electronic Support*

In combat or passive scenarios where assets are in the field, it is a high operational priority to gather as much information about the physical environment and communications in the immediate vicinity in order to asses the threat level. This information gathering ensures the safety of people and equipment [3]. ES undertakes this task via electronic interception of communication and other RF signals (i.e. Radar). A typical topology of this is shown in Fig. 2.3.

The objective of ES is to provide other electronic defence (ED) systems with accurate combat information in order to alert and react appropriately to threats. We refer the reader to the appendix for further information on ED theory and the application of ES systems therein.

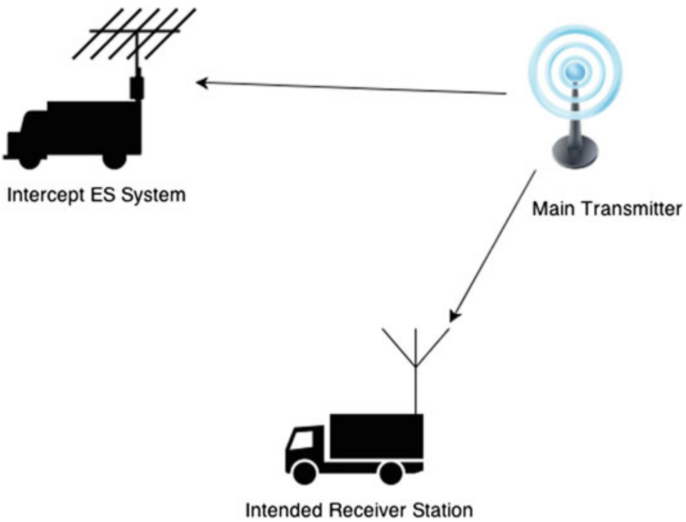

Fig. 2.3 The operation of a possible Electronic Support deployed in the field. This is a typical application of an intercept layout of an ES system, intercepting communication from an adversary's transmissions from a communication node. Adopted from [3] and modified by the authors

ES systems deliver the capability to search, intercept, identify and locate intentional and unintentional sources of electromagnetic (EM) radiation [157]. These tasks involve real-time signal acquisition and processing of combat or friendly information gathered to generate intelligence and pass onto sub-systems. Intercepting communication signals comprise of several steps; namely receiving the signal, identifying the type of signal, and finally locating the source of the radiation which is done by DOA estimation methods. Information gained from a signal to infer the location of the emitter source, namely DOA estimation, is regarded as a pivotal task for ES systems [126].

2.1.3 Electronic Attack

Electronic Attack (EA) has at its core, the objective to restrict enemy signals access in using the EM spectrum for communication, information exchange and/or other illicit activities (i.e. infrared and optical detection and tracking). This denial of information can be categorized into two schemes; firstly, in terms of information protection (protecting your own communication link via deception or encryption), and secondly as information attack (denying the user the use of their own communication link) [3]. For most of the situations in ED, the attack of an adversary's communication systems to deny information exchange is one of the most important task in ensuring a successful control strategy for information dominance.

Typically the denial of an adversary in exchanging information via RF communication is done via jamming. In brief, a communication jammer emits an excess (large amounts) of RF energy in the RF link of the enemy [3, 157]. This in no way reflects the entire scope of EA techniques and technologies. The sophistication of such jammer technology in literature and industry [3, 34, 157] serves as a remainder of how involved this aspect of ED is.

However, as far as the scope of the current work is concerned, more diverse EA systems will not be critically analysed herein. Further investigation of EA systems are left up to the reader (Fig. 2.4).

2.1.4 Electronic Protect

EP Systems are designed to restrict penetration and susceptibility of friendly systems being interfered with by enemy ES and EA systems [1, 157]. This is an involved process. A range of approaches must be adopted in achieving the intended task of protecting friendly forces. EP systems have a focal objective to protect friendly information, usually telecommunication, from being manipulated by an adversary.

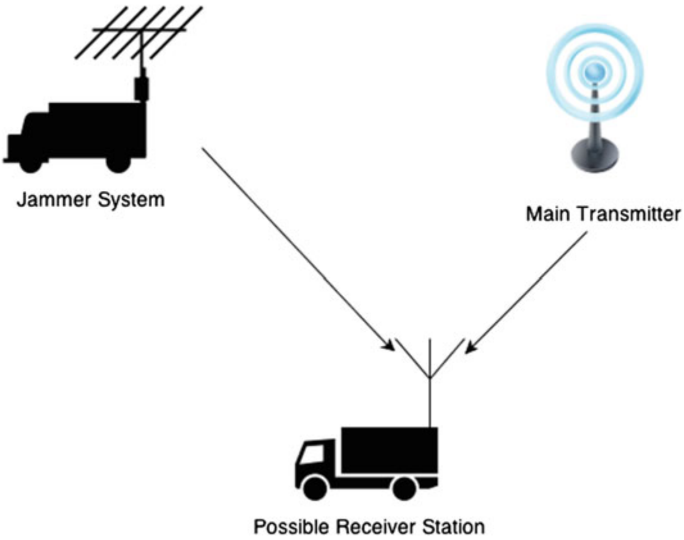

Fig. 2.4 Illustrates the operation of a possible Electronic Attack deployed in the field. This is a typical application of an EA system, whereby a Jammer is used to reduce the efficacy of an adversary's transmissions from a communication node. Adopted from [3] and modified by author

Some of the major kinds of EP measures are detailed below.

- Emission Control (EMCON) is the intelligent control that coordinates friendly transmissions for a period of time. In particular, it limits access of certain transmission sources at critical junctures as to not risk exposure for detection by enemy ES and EA systems [3].
- Low Probability Intercept *LPI* (spread spectrum) signals is the use of deliberate spreading of the transmitted data over frequency, and hence bandwidth. This is intentional, so as to prevent any attempt of adversary ES and EA systems to intercept, locate and jam signals [2].
- Screen Jamming is a clever, yet simple, technique to introduce RF energy between friendly communication networks and the SIGINT systems of enemies to impede the interception of transmission [3]. This is done by user specific jammer systems, much the same as the EA jammer systems, but with a different objective.
- Encryption is the classical technique to ensure the fidelity of data transmission, in cases where transmissions are intercepted and extracted for intelligence gains.

All these techniques are utilized to protect friendly communications being intercepted or susceptible to adversary electronic tactics.

The discussion of EP serves as part of the overview for the ED domain, whereas our focus will be restricted to ES systems and hence little more will be detailed on EP herein this work.

2.2 Electronic Support Communication Applications

The application of our work incorporates both ES and COMINT (a sub section of SIGINT) tasks, as detailed in Sect. 2.1.2, with a focus on implementing the new signal processing techniques using compressive sensing. As a result, the question of which equipment platforms such techniques can be implemented on (i.e. digital or analog), becomes a focal point.

In fact the typical equipment platforms that are used to perform ES and COMINT tasks are communication electronic support (CES) and communication intelligence (COMINT) equipments. The distinction between the two systems varies in terms of both equipment architecture and purpose.

In this section we highlight the equipments needed for both systems, their applications and purpose. We also include common signal processing techniques used as part of the processor unit. Then, we review how certain techniques such as emitter identification, feature extraction, and classification are typically implemented for communication ES purposes. Lastly, we discuss the implementation of spectrum monitoring and direction finding techniques that are pertinent to our work.

2.2.1 Communication Electronic Support—CES

Communication Electronic Support systems provide immediate emitter signal information to troops and other operators in order to make informed decisions in the battlefield [139]. The functions that are tasked to CES equipment include:

- Search,
- Interception,
- Classification,
- Identification, and
- Direction Finding.

As pointed out earlier, the large frequency coverage as well as the congestion of the RF spectrum requires a receiver system that can cope with the demand of complete coverage of the intended spectrum. In the case of CES equipment, this is either implemented by a wide-band channelized receiver or with a number of wide-band Super-Heterodyne (SH) channelized receivers, coupled with the number of receiving antennas, that rapidly scan over the RF bands [107]. These bands are known as the instantaneous bandwidth (IBW) corresponding to the SH receiver channel width, typically 40 MHz wide [139]. This receiver architecture is the most commonly used one in practice for CES equipment [107] and serve as motivation for its review. We refer the reader to the work done in [1, 8, 139] for further study on the working details of different available architectures.

CES equipment typically comprise of the following sub systems (sourced from [8, 107]). See Fig. 2.5 for the CES system block diagram.

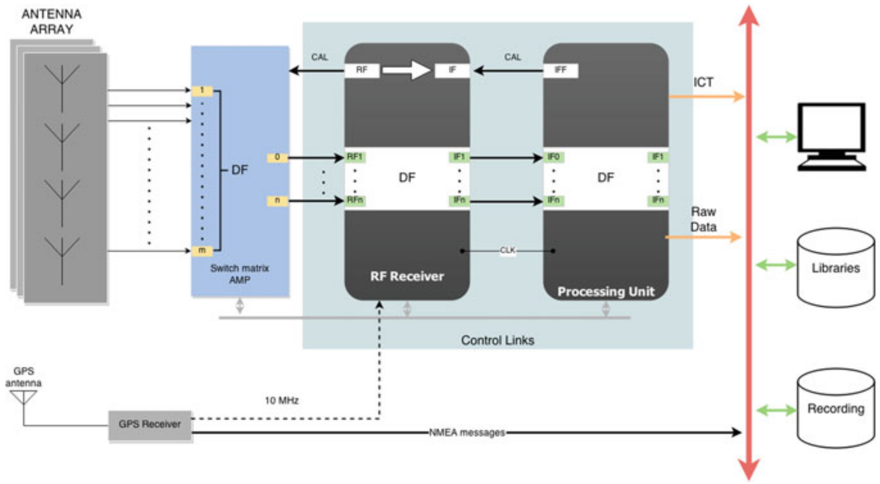

Fig. 2.5 System block diagram for a typical CES system and equipment requirement. Sourced from [107] and modified by the authors

1. **Antenna array**, composed of different sub-band antennas typically covering the VHF, UHF and SHF bands
   - These arrays typically form a sub-band circular array (UCA) useful for DF methods [156], especially correlative methods. Further discussion of these methods are detailed in Sect. 2.4.
   - The UCAs are made up of an odd number of vertical poles to reduce the phase ambiguities.
   - An additional antenna used as a GPS antenna and receiver which provides information about its global position, necessary for ground deployment, as well as synchronizing a CES receiver with other systems in a CES sensor network.
2. **Antenna front-end (AFE) and sub-band array switching matrix**
   - Provides pre-selector filtering and low noise amplification of the received RF signal before being passed to the RF receiver
   - The switch matrix selects between the different sub-array of antennas in order to perform DF measurement as the number of UCA channels are limited.
3. **RF receiver**
   - The CES monitoring equipment exploits the SH architecture and channel nature to do stepwise sweeping over the entire frequency spectrum. The IBW is usually 40 MHz (as previously suggested).
   - The sweeping speed is determined by the tuning time, typically in the order of 10 s of microseconds.

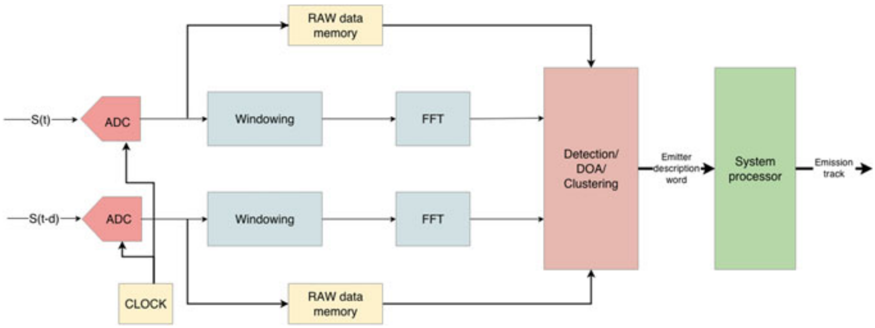

Fig. 2.6 A two channel DRx shown performing detection and differential phase measurement using two antenna channels from the IBW equipment. Sourced from [107]

- Adjusting the IBW tuning speed can be used to either increase/reduce the frequency resolution for a specific purpose, such as detecting and locating frequency agile signals, better known as frequency hopping (FH) signals.
- The required instantaneous dynamic range (IDR) is usually IDR > 60 dB, with a signal-to-noise (SNR) ratio between 8 and 10 dB.

4. **Processing Unit**

- The IF signal from each channel of the RF receiver is then converted via a 12–14 bit ADC (providing the needed 60 dB IDR). All the channel data then gets processed via FPGAs, which provide the DSP capability such that detection using a filter bank implementation and phase measurement algorithms can be accomplished.
- The processing of these channels is shown in terms of processing blocks in Fig. 2.6, which shows two channels from the UCA. The processing tasks, shown as system blocks (i.e. Windowing, FFT, Detection etc.), are executed by the FPGA. The blocks are merely system descriptions describing the processing steps.
- Windowing applied to the data stream reduces the sidelobe response of frequencies for Fast Fourier Transform (FFT) detection.

5. **Axillary Units** i.e. Human Machine Interface (HMI), computer, databases, libraries and storage

- After preliminary detection, direction of arrival (DOA) and clustering are performed. The auxiliary units use this information to perform classification and feature extraction.
- Classification and feature extraction techniques are discussed in Sect. 2.2.4.

2.2.2 Communication Intelligence—COMINT

Communication Intelligence systems are used to analyse signal over an extended period of time giving sufficient processing time to provide accurate intelligence about signal characteristics and content [139]. Signal intelligence includes emitter location, signal structure and the level of electronic counter counter measures (ECCM) employed by an enemy to evade detection. These characteristics are then used to compile and support mission control plans and provide insight to generate the appropriate waveforms used in jamming enemy signals [40]. In this respect COMINT is vital for jamming and protecting RF supremacy. The main functions ascribed to COMINT are as follows.

- Signal Acquisition and feature extraction;
- Signal Classification;
- Signal demodulation;
- Voice signal demodulation, decryption and listening;
- Signal Recording; and
- Decoding, transmission standard recognition and speech recognition.

Furthermore, use for COMINT equipment extends to civilian application for spectrum monitoring, whereby surveillance of the spectrum use is monitored to determine if users are broadcasting within the legal specified bands [12]. Any RF emitter broadcasting in a defined civilian area must comply with the regulatory body licensing agreement that defines the broadcasting standards within a specific geographical location. The Independent Communications Authority of South Africa (ICASA) is an example of such a body. However, as far as DF tasks are concerned, COMINT equipment typically does not include omnidirectional antennas and sub-systems needed to perform DF. The DF (360°) antennas are substituted for high gain directional antennas in order to improve sensitivity and provide higher SNR for signal parameter estimation [1].

It is worth mentioning that the architecture for COMINT equipment share similarities with CES equipment including similar AFE, UCA, RF receiver, DRx (Dual Receiver) channels, and processing units. However, as mentioned before, the DF antennas are replaced by high-gain directional antennas and as a consequence the DOA processing steps are omitted and additional number of processors, recording systems (i.e. storage devices), and software tools are added.

2.2.3 Signal Processing Techniques

Any intelligent receiver system requiring classification and/or identification of signal are highly dependent on some form of signal processing unit, and/or HMI (i.e. computer) [68, 167]. Moreover, signal processing techniques—specific to transforms—play a pivotal role in generating a representative base that allows different digital methods to classify, identify, and extract features from RF signals in ES communication systems [42]. Some transforms that are integral to ES equipment include the Fast Fourier Transform (FFT), Wavelet Transform (WT), Walsh Hadamard Transform (WHT), and the Hilbert Transform (HT). A few of these tasks are described below.

1. **Filtering Methods** based on cyclostationary signal properties [63] using an FFT accumulation technique. A lower level implementation that does not involve feature detection, as cyclostationary techniques do, involve FIR filters that are quite commonly seen as part of digital receiver systems to perform digital filtering of signals.
2. **Time-Frequency Analysis** which is either implemented via a Wavelet Transform or else, in some systems, via the Wigner-Ville distribution coupled with a quadrature mirror filter (QMF) method. Time-frequency analysis of signals, especially for ES systems, are vital to determine if a signal is frequency agile.
3. **Signal Detection** using a strip spectral correlation analysis (SSCA) [138] that comprises of FFT blocks to achieve detection. Detection is ubiquitous with signal processing of RF signals within ED. However, elementary detection techniques such as *threshold detection* simply do not suffice for some kinds of signal. Hence is the need for more probabilistic detection methods such as the SSCA and cyclostationary signal processing that provide improved detection performance with more deterministic parameters [7, 138].

2.2.3.1 Transforms

A transform, for the discrete case, is the process where an input signal is mapped from one domain represented as real discrete values to another vector space. This mapping process is the basis on which any transform is based. Transforms are ubiquitous in signal processing. Herein we have selected the most frequently used and prominent transforms used as part of the ES signal processing block. However many more transforms exist and can be applied to ED, but such a discussion merits a study on its own (Tables 2.1, 2.2 and Fig. 2.7).[3]

2.2.4 Signal Classification

Classification techniques in the equipment mentioned earlier serve to recognize specific characteristics about a received communication signal [139]. These are known as classifiers of the system, whereby the output parameters from the receiver unit of a CES or COMINT system (i.e. DF, frequency carrier and detection) are used as

[3] See the following literature on the advances [165] and implementation of different transforms for the uses in ES [32, 73, 110].

Table 2.1 A table detailing the expressions for the transforms and the associated complexity

Transforms	Definition	Fast algorithm		Complexity
		Name	Complexity	
Discrete Cosine Transform (DCT)	DCT-II: $X_k = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}(n+1/2)k\right]$	(FCT)	$O(N\log_2(N))$	$O(N)$
Discrete Fourier Transform (DFT)	$X_k = \sum_{n=0}^{N-1} x_n e^{-j2\pi kn/N}$	(FFT)	$O(N\log_2(N))$	$O(N)$
Discrete Short Time Fourier Transform (DSTFT)	$X(m,w) = \sum_{n=-\infty}^{\infty} x[n]w[n-m]e^{-jwn}$	(WFFT)	$O(N\log_2(N))$	$O(N)$
Walsh Hadamard Transform (WHT)	$(H_m)_{k,n} = \frac{1}{2^{m/2}}(-1)^{\sum_j k_j n_j}$ where $k = \sum_0^{i<m} k_i 2^i$ and $n = \sum_0^{i<m} n_i 2^i$	(FWHT)	$O(N\log_2(N))$	$O(N)$
Wavelet Transform (WT)	$\left[W_\psi, f\right](a,b) = \frac{1}{\sqrt{\lvert a\rvert}} \int_{-\infty}^{\infty} \overline{\psi\left(\frac{x-b}{a}\right)} f(x)dx$	(FWT)	$O(N) - O(N\log_2(N))$ per scale	$O(N)$ per scale

Table 2.2 A table detailing the advantages and disadvantages associated with different signal processing transforms used to facilitate electronic support processing tasks

Transforms	Application	Advantage	Disadvantages
(FCT)	• Spectral methods • Lossy compression (i.e. MP3, Image processing)	• Efficient representation of signals • Smaller data length • Multiple DCT variants (i.e. I-VII-DCT)	• Single basis to represent signals • No phase information
(FFT)	• Spectral methods (i.e. Filter banks) • Demodulation • Broad application to RF detection, identification, and classification	• Magnitude & Phase information • Efficient representation of frequencies	• Assumption of periodicity causes spectral leakage • No time information (exclusive to frequency domain) • Only two representative basis (sin & cos)
(WFFT)	• Non-periodic signal analysis • Sidelobe reduction	• Provides time-frequency information • Major reduction in spectral leakage	• Computationally intensive (Let time slots be M then complexity is $O(MN\log_2(N))$ • Equal resolution for time and frequency transformations
(FWHT)	• Frequency signal processing • Digital signal detection/estimation • Used when signals are choppy	• Less computationally expensive than FFT, as only 2 discrete states exist (i.e. 2 bits) for addition and subtractions • Reduction in Bit depth needed	• Reduction in true frequency representation • Representative basis leads to different frequency interpretation
(FWT)	• Time-Frequency signal processing analysis • Signal detection, estimation, and classification	• Varying resolution for time-frequency transformations • Numerous wavelet basis (i.e. Haar, Daubechies, Coifman, Symmlet) [37] • Provides adequate signal approximations that have sharp discontinuities	• Prior knowledge of the signal must generally be known • Computationally more expensive

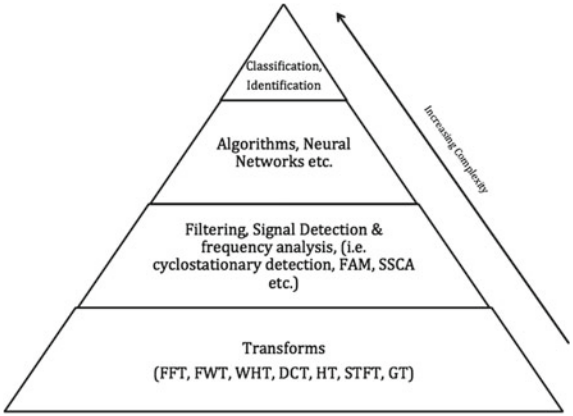

Fig. 2.7 Illustrates how signal processing in the context of ES maintains a hierarchy, in that the lower level signal processing techniques all add up and aid the upper, more complex levels, in order to accomplish the ultimate task of classification and identification of emitters

input to another system processor to classify the signal. Signal classification of the signals include one or more of the following.

- Signal type recognition (i.e. Analog or Digital),
- Analog modulation recognition (i.e. AM, FM, PM),
- Digital Modulation recognition (i.e. FSK, PSK, ASK), and
- Type of multiplexing recognition (i.e. FDM, PPM).

Classifiers above are vital for emitter identification tasks.

In practice there are two major perspectives on classification for communication signals that have been adopted in military applications [139]. These are based on two algorithmic approaches, namely pattern recognition processing and decision theoretic approach, sourced from [107, 139]:

- **Pattern Recognition Processing**—uses signal feature knowledge processed by an artificial neural network type of algorithm [121]. Two major works that have contributed to classification processing using neural networks include:

  1. the **Nandi-Azzouz** classifier [121], that proved to be successful in distinguishing between 13 analog and digital modulation types, namely AM, FM, FSK2-4, ASK2-4, DSB, LSB, VSB, USB, PSK2-4, and combined (amplitude and phase) modulation, and
  2. the **Assaleh-Farrell-Mammone** classifier used to discriminate between different digitally modulated signals [10] (The modulation types include CW, BPSK, QPSK, BFSK, and QFSK.).

- **Decision Theoretic Approach**—depends on likelihood or probability to determine the modulation of a signal. Two of these decision-based methods include:

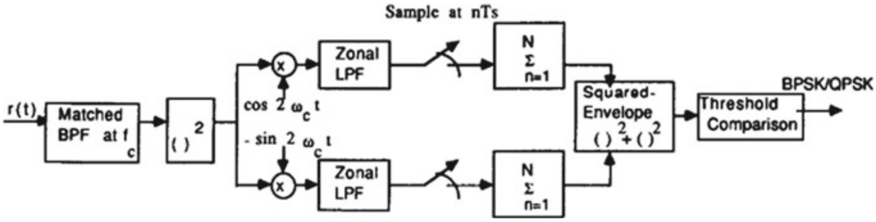

Fig. 2.8 Functional system block diagram describing the qLLR classifier used in the work by Kim and Polydoros, taken from [135]

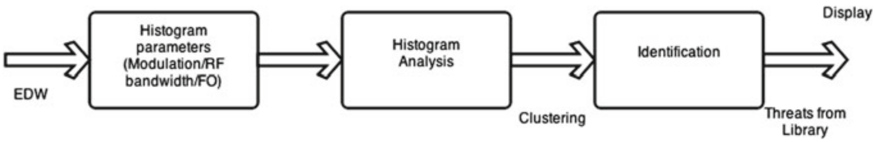

Fig. 2.9 System block describing the processing steps involved for emitter sorting process. Compiled by author, but sourced from [107]

1. the **Sills** classifier [161], which can discriminate between the three different types of PSK (BPSK, QPSK, PSK-6) and three types of Quadrature Amplitude Modulation (QAM) signals (i.e. 2^4QAM, 2^5QAM, 2^6QAM) (The classifier implements a maximum-likelihood (ML) algorithm for coherent classification and validate the findings using a noncoherent ML version of the algorithm.); and
2. the **Kim-Polydoros** classifier [141] which is an efficient means to discriminate between modulation, relying on a quasi-log-likelihood ratio (qLLR) rule to base decisions (Fig. 2.8).

2.2.5 Signal Feature Extraction

Signal feature extraction is a critical step, used after a signal has been classified, to extract and catalogue the features that are assigned to the signal in order to identify the emitter type [2], see Fig. 2.9. The process for feature extraction is similar to the process used for emitter deinterleaving[4] and sorting of radar warning receiver (RWR) systems within ES [113].

Although the tasks are similar, to deinterleave and to sort the features based on classifiers, the fundamental difference depends upon the emission description of the signals [156]. In communication scenarios, emission descriptor words (EDW) that are

[4] "*Deinterleaving is a kind of clustering analysis, which clusters inter-weaved pulses—intercepted by a scout or by other means—into distinct groups belonging to respective emitters, according to the pulses' features.*" [88].

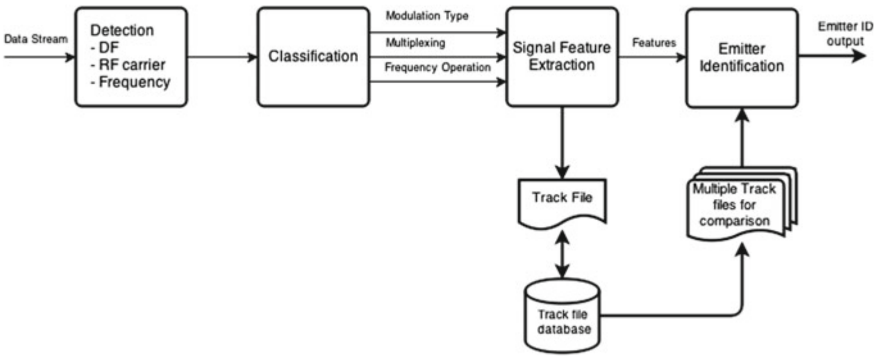

Fig. 2.10 System block diagram describing the processing steps involved to identify a RF emitter

assigned to communication signals are different in nature to that of radar signals (i.e. RWR systems), as they are primarily pulsed [88]. Nevertheless, the process remains similar, although the features assigned to signals differ. Typical features associated with communication signals [139] which serve as an input to the clustering analysis process (i.e. deinterleaving) are:

- Signal classification
- Frequency of operation
- RF bandwidth
- Modulation type
- Power Levels.

The features assigned to a particular signal are transformed into a digital word, which is then passed onto the clustering analysis process based on a knowledge-based algorithm which is mostly a histogram analysis method [88] (see Fig. 2.10 for the sorting process). A key component of the feature extraction is to sort the EDW into a subspace based on the parameters of the feature in order to generate a track file of the emitters that are catalogued. This track file is then used as an input to identify the emitter. The process of generating the track file is discussed in the following section. Furthermore Fig. 2.10 adeptly contextualizes how the processing of an RF communication signal, by means of detection, classification, and feature extraction, enables an emitter to be identified. We refer the reader to the following literature [13, 145, 163] for further discussion.

2.2.6 Emitter Identification

Once the features of the signal emitter has been sorted and the accompanying track file generated as depicted in Fig. 2.10, the following process takes over in identifying

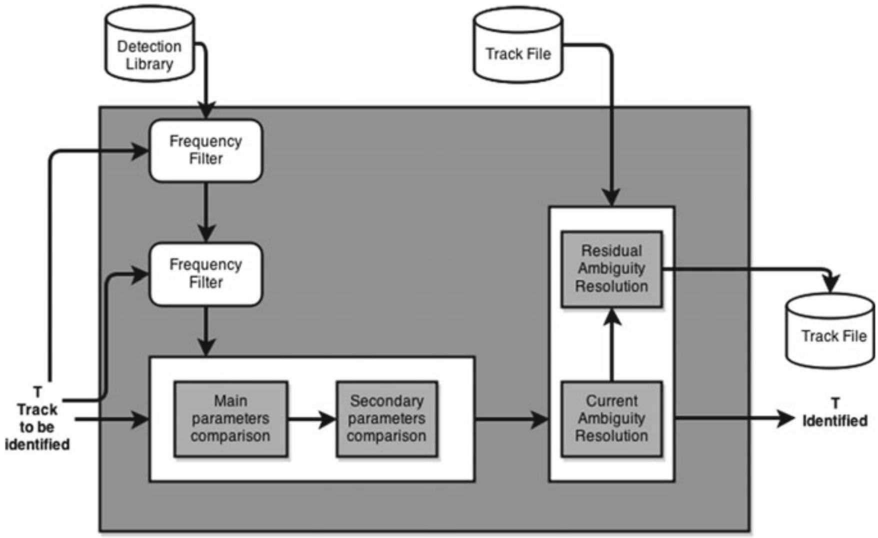

Fig. 2.11 System block diagram describing the flow process for emitter identification. Compiled by author, but sourced from [107]

the most likely emitter based on a history of emitters as well as the database that stores relevant parameters that comprise the details of a specific emitter [107].

Every parameter that is defined in the track file based on the EDW from the signal features are used as a comparison to the measured values of an incoming track. As depicted in Fig. 2.11 the process of identifying an emitter is based on scoring the specific parameters based on the correlation from past emitters in the database. Consider an emitter signal that has been received with a specific frequency operation (FO) modulation type and signal power. The input signal is assigned with a score based on the correlation measured of each of the values against emitters in the database [108]. Then, the sum total score is calculated and if the total score exceeds a selected threshold, the received signal can be identified with a probability relative to the score, which is known as the confidence level [109].

2.3 Direction of Arrival Methods Used for Electronic Support Tasks

DOA systems determine accurate estimates, within probabilistic bounds, of the direction from where a signal of interest (SOI) is received—also known as the line of bearing (LOB). Once an accurate estimate of the signal DOA is determined a second DOA must be acquired from a different geographical location, which can either be done from a second receiver or a mobile intercept receiver. When two estimates from varying locations are acquired the location of a communication signal can be accurately determined, which is known as direction finding (DF).

It is important to distinguish between the signal processing task which constitute DOA estimation methods and the operational task of DF. As explained, DF is the operational objective in ES to use DOA estimates from multiple receivers to find the direction of an EM source with high accuracy. In other words, DOA forms a part of DF.

Main requirements of a DOA system are:

- High accuracy i.e. resolution less than 1°;
- High sensitivity;
- Real time data capturing and processing;
- Short minimum requirement signal duration;
- Immunity to field distortion and polarization errors.

Both azimuth and elevation characteristics can be considered to provide a three-dimensional estimate of a signal DOA. However, as elevation DOA is common in air-to-ground scenarios, we do not continue the 3D discussion herein,[5] we only consider the case for azimuth DOA methods as we are interested in ground-to-ground scenarios.

In this section we review conventional and modern DOA techniques used in ES, and discuss why only phase interferometry is considered for our ES application, especially communication DOA estimation. We then discuss modern DOA algorithms used for ES systems and their associated performance to estimate the DOA of a signal. Thereafter, we review the scalability of existing DOA estimation using compressive sensing in the open literature.

2.4 DOA Methods

The two main DOA methods used in ES are amplitude comparison and phase interferometry [37]. Table 2.3 details the comparison of the two DOA measurement methods and their associated benefits and drawbacks.

Amplitude comparison methods, as the name suggests, compare the amplitude of a measured signal from multiple antennas [126] or in some instances a single rotating antenna [107], in order to determine the DOA of a signal. Although amplitude comparison DOA is widely used, with adequate directional resolution and bandwidth coverage, it is generally designed for pulsed transmissions. That is why they are predominantly used for radar warning receivers. Subsequently, the use of amplitude comparison DOA in ES equipment is almost non-existent, except for some electronic intelligent (ELINT) equipment where rotating antennas are used [107]. As a consequence, we do not develop amplitude comparison methods further in this work.

[5]We refer the reader to the following literature for further reading on the subject of DOA and elevation direction finding techniques [61, 21, 107, 126].

Table 2.3 DOA measurement method comparison, sourced from [37]

	Amplitude comparison	Phase interferometer
Sensor configuration	Typically 4–6 equispaced antenna elements for 360° coverage	2 or more RHC or LHC spirals in fixed array
DF accuracy	$\text{DF}_{\text{ACC}} \approx \frac{\theta_{BW}^2 \Delta C_{dB}}{24S}$ (Gaussian Shape)	$\text{DF}_{\text{ACC}} = \frac{\lambda}{2\pi d \cos\theta} \Delta\theta$
DF accuracy improvement	Decrease antenna BW; Decrease amplitude mistrack; Increase squint angle	Increase spacing of outer antennas; Decrease phase mistrack
Typical DF accuracy	3°–10° rms	0.1°–3° rms
Sensitivity to multipath/Reflections	High sensitivity; Mistrack of several dB can cause large DF errors	Relatively insensitive; Interferometer can be made to tolerate large phase errors
Platform constraints	Locate in reflection free area	Reflection free area; Real estate for array; Prefers flat radome
Applicable receivers	Crystal video; Channelizer; Acousto-optic; Compressive	Superheterodyne

ΔC_{dB} = Amplitude monoipulse ratio in dB; S = Squint angle in degrees; θ_{BW} = Antenna beamwidth in degrees

Phase interferometry on the other hand, is widely used in ES equipment [37]. Phase interferometry is dependent on using multiple antennas, typically an array of uniform spacing. The received signal's phase between the individual receiving antennas, is correlated to provide an estimate of the DOA based on the phase difference [176]. Due to the breadth of implementation of this DOA method for ES, a review of phase interferometry follows.

2.4.1 Phase Interferometry

Phase interferometry is considered as one of the best suited technique for communication signal DOA estimation [126]. If a scenario demands higher accuracy, in the order of 0.1°–1°, the antenna spacing distance $d = \lambda/2$ (referred to as the baseline width) can be decreased as it is relatively insensitive to phase errors [139]. Moreover, one can reduce phase mistrack by increasing the spacing of the outer antennas in the array. Phase interferometry is relatively responsive, but requires complex RF circuitry and processing when compared to other methods.

DOA phase interferometry system consists of the following components:

- an array of equidistant antennas which take various configuration—linear, circular or lattice;

- front end channelized receiver circuitry, including mixers and analog-to-digital converters (ADC); and
- digital signal processing back-end.

A typical configuration of this architecture is shown in Fig. 2.13.

Phase interferometry works on the following principle. Consider a plane wave incident on a linear antenna array at an angle Φ, as shown in Fig. 2.12. Then based on the geometry of the configuration the time difference of the signal being received at every antenna can be expressed as phase difference. The phase difference can then be be expressed in terms of the angle of arrival as shown in Eq. 2.1. Following the notation in Fig. 2.12 gives:

$$\Phi = \omega \frac{d}{dt} = 2\pi f(\frac{\Delta s}{c}) = 2\pi(d \sin\theta)/\lambda, \qquad (2.1)$$

where

- Φ phase of the signal,
- ω angular frequency of the signal,
- s vector component of the antenna separation distance,
- f frequency of the signal,
- θ angle of arrival,
- d the antenna separation,
- λ the wavelength of the RF signal,
- c speed of light (3×10^8).

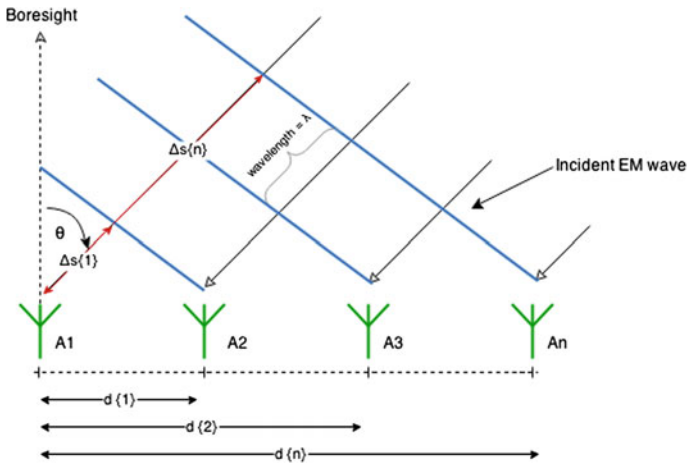

Fig. 2.12 An n length linear antenna array showing the 2 dimensional dynamics of phase interferometry, using phase representation of the time difference to solve the angle θ of an incident RF wave. (Compiled by the authors.)

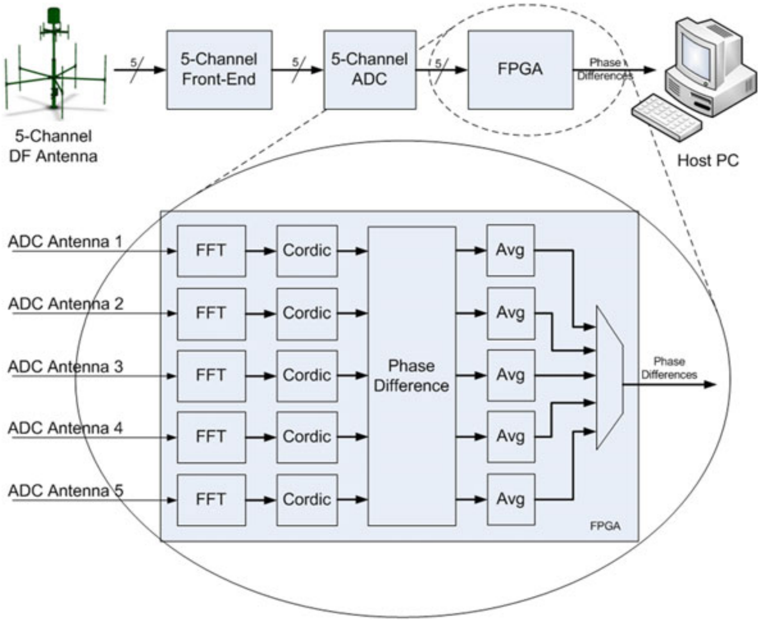

Fig. 2.13 5-channel DF antenna processing architecture, taken from [144]

The phase information of the signal received at every branch of the receiver is used by estimation algorithms to resolve the DOA. Before we review estimation algorithms it is important to mention system considerations of phase interferometry systems deployed in the field. Some of the system considerations restrict accurate DOA estimation, and an awareness of them provide insight to which estimation algorithm to choose.

A typical phase interferometric system using a uniform circular array (UCA) dipole antennas is shown in Fig. 2.14. The processing back-end is shown in Fig. 2.13 implementing an FPGA back-end processing unit to perform correlative interferometric estimation. This architecture and processing implementation in most cases is considered as the standard approach for DOA tasks on modern ES equipments [176].

2.4.1.1 System Considerations

To deploy phase interferometry techniques in the field, there are several considerations that have to be made, namely antenna spacing, coning error, system noise, and signal-to-noise ratio (SNR).

Phase interferometric systems require minimal phase ambiguities as they distort the accuracy of the field of view. When the antenna spacing is less than $\lambda/2$ the field of view is 180° wide, which results from solving $\theta = 2\sin^{-1}(\pi/2d)$ [37]. Therefore, the spacing must match the highest frequency (i.e. smallest wavelength)

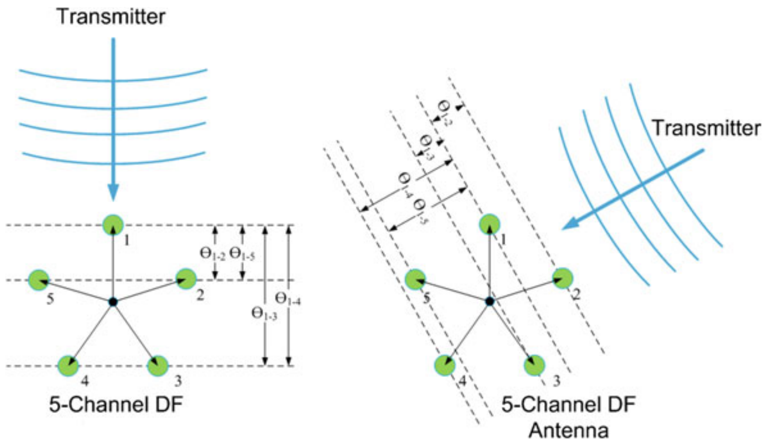

Fig. 2.14 Phase differences shown for two different incident waves for a 5-channel DF antenna system, taken from [144]

of the received signal in the bandwidth of interest [149]. The restriction on the antenna array for higher frequency cases (i.e. UHF/VHF communication) results in ES DOA systems adopting multiple antenna arrays for various bandwidths of interest, or resolving phase ambiguities with correlative algorithms; the latter solution being more computationally expensive than the former.

When an EM source is elevated, for example an air-to-ground scenario, the elevation of the incoming signal in relation to the receiver on the ground introduces discrepancies in azimuth estimation for 2-Dimensional DOA task, which is known as the coning error function [37]; adequately named because of the shape the locus points create, which share the same phase delay.

Coning error adds to phase ambiguities when a signal is incident on the receiver array at an elevated position, which in some cases can be large. Coning error can be calculated by equating the ideal 2-D case $\phi = 2\pi(d \sin\theta)/\lambda$ with the 3D case $\phi = 2\pi(d \sin\theta \cos\varphi)/\lambda$ (with azimuth θ and elevation φ) which gives:

$$\theta^* = \sin^{-1}(\sin\theta \cos\varphi). \tag{2.2}$$

For cases when the emitter location is either on the horizon and/or restricted to ground-to-ground application, the coning error is almost negligible [139] as elevation increases. Fortunately for our application these effects are negligible.

The noise effects due to sensitivity and thermal noise contribute to the accuracy in determining the DOA. The relationship for standard deviation of phase θ_ϕ relative to noise is given as

$$\sigma_\phi = \frac{1}{\sqrt{2SNR}}, \tag{2.3}$$

which is then used to determine the common expression for angle accuracy using interferometric techniques:

$$\sigma_\theta = \frac{c\,\sigma_\phi}{2\pi\ d_i\ f\cos\theta} = \frac{c}{2\pi\ d_i\ f\cos\theta\sqrt{2SNR}}. \tag{2.4}$$

The restriction in the width between antenna elements in the array d_i, in order to mitigate incorrect DOA estimation, requires a higher SNR of the system to process and estimate the DOA of a SOI accurately. In some cases the required SNR could be up to, and above 50 dB, which is unrealistic as interception systems operate in low sensitivity environments [8].

Given such a high SNR demand, for certain tasks phase interferometry cannot be used for ES. However, to overcome SNR demand, phase interferometric methods in ES systems make use of circular harmonic (base-lengths are $d_i = 2^{i-1}d_1$) and non-harmonic (prime number multiples of base-length) antenna array with wider baselines, which result in a lower SNR level requirement [37].

There are a variety of DOA estimation algorithms in the literature that are capable of performing accurate DOA estimation given phase interferometric data. Several estimation algorithms have seen successful implementation for ES systems, namely the correlative interferometer algorithm (most widely used method) [15], multiple signal classification (MUSIC) algorithm [158] and the estimation of signal parameters via rotational invariance techniques (ESPRIT) algorithm [153].

2.4.2 DOA Estimation Algorithms

2.4.2.1 Correlative Interferometer [15]

The correlative interferometric method is based on a two step process. Firstly, the respective phase differences between the antenna's, respective to a primary antenna (e.g. θ_1 as shown in Fig. 2.14), are measured according to a known predefined bearing.

Then, based on a phase-history acquired during the system calibration of known transmitter angles, the method performs a correlation between the different phase measurements of the n-channel antennas and the stored phase history. The best corresponding phase set is chosen for the phase of the received signal which results in the correlative interferometric estimate of a incoming signal DOA.

The reliance on calibration history of some parameters make it susceptible to elevation ambiguities and lower SNR, as well as lower resolution compared to MUSIC and ESPRIT.

2.4.2.2 MUSIC [158] and Root-MUSIC [148]

The method of MUSIC as it applies to DOA was first formalized in [158] with beamforming [159] and maximum likelihood [191] DOA methods as seminal components preceding its development. The algorithm is based on a probabilistic spectral search method over all the angles in the subspace, using eigen decomposition methods to

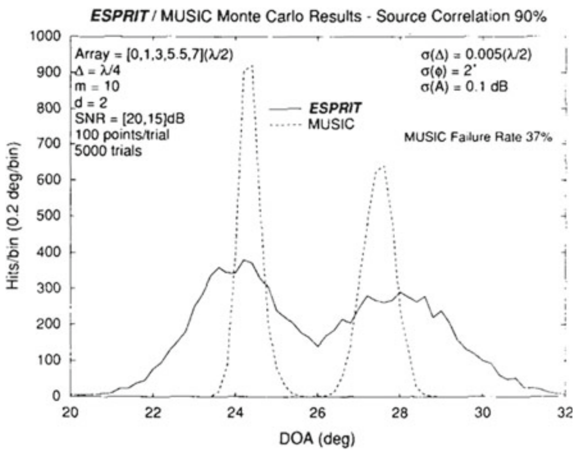

Fig. 2.15 Histogram of MUSIC and ESPRIT results-random IO-element linear array, source correlation 90 %, small array aperture ($\Delta = \lambda/4$), taken from [153]

resolve the DOA estimate. The search technique is computationally demanding and therefore can be very expensive for some real-world applications. Developments such as the alternative root-MUSIC algorithm [148] has shown to reduce the computational complexity and improve estimation accuracy [137].

The conventional MUSIC algorithm, although computationally expensive works for any antenna array configuration and multiple simultaneous RF signals. But it remains vital for the algorithm to have knowledge—in terms of the spatial model—of the positions of the antennas relative to one another. Furthermore, it is sensitive to position, gain errors, and phase. Therefore careful consideration must be applied for calibration.

2.4.2.3 ESPRIT [153]

ESPRIT is another estimation algorithm used for DOA estimation closely following the MUSIC DOA method. The algorithm is based on a similar correlation matrix generation and steering vector method as in MUSIC. The main difference is that by using a non-singular matrix subject to the eigenvector noise subspace, a single execution approach can be taken to determine the DOA instead of a search method. This is sometimes referred to as a "one shot" approach.

Based on this single step process the computation for this algorithm is significantly less as compared to MUSIC. However, due to the constraints imposed on the signal model and matrix rank, the amount of antennas needed for ESPRIT is double that of MUSIC which increases system cost. Furthermore, the use of total least square instead of previous least square (LS) ESPRIT method reduces the error when SNR is low as well as reducing error. The resolution of ESPRIT is reduced as compared to MUSIC. Figure 2.15 shows the difference in DOA estimations for these two algorithms.

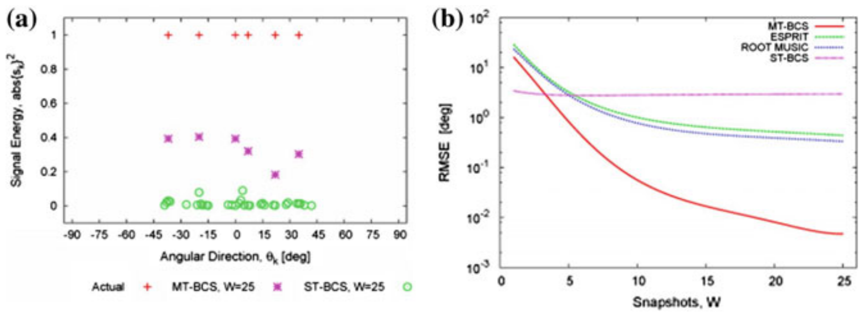

Fig. 2.16 In **a** showing the actual and estimated DOA using both BCS snapshot methods as well as the **b** error in terms of RMSE of the estimates with varying number of snapshots compared to other DOA estimation methods. Courtesy [31]

In summary, where sub-space DOA estimation algorithms are considered for our Compressive Sensing (CS) approach, MUSIC is the preferred DOA estimation algorithm due to the lower requirement on the number of antennas compared to ESPRIT, and higher resolution outcomes for DOA estimation.

2.5 Existing Compressive Based Direction-of-Arrival Methods

In many respects compressive sensing (CS) based techniques used for DOA methods are still in their infancy, which is interesting as CS theory is based on seminal works from beamforming and super resolution [62] techniques.

In the open literature there are several CS methods used for DOA estimations, which apply CS algorithms at various points in the processing chain. Majority of the literature do not include CS sampling techniques for DOA estimation, rather, only focus on applying CS recovery techniques. Such methods include the following major work.

Bayesian CS based DOA estimation [31] develops a single and multi snapshot approach using Bayesian compressive sensing (BCS) to estimate the DOA of a narrowband signal. Rather than relying on compressive sampling, BCS determines the estimates for DOA based on Nyquist-sampled voltage outputs directly from the antenna elements. It was shown that by adopting this method, computation of the covariance matrix for voltage outputs is not needed (as is the case with MUSIC [158] and ESPRIT [153]). Also, robust and accurate estimates were determined without the need for a-priori knowledge of the number of incident angles. However, the magnitude estimates were somewhat degraded due to estimation error, but no such effect to boresight-direction estimates were observed (see Fig. 2.16).

Radius	6.3 λ
Search area	$\sqrt{u^2+v^2} \leq 0.5$
Grid spacing in u, v−plane	0.02
Signal-to-noise ratio	30 dB
Number of elements	$M = 40$
Number of elements for $\lambda/2$−array	500
Number of grid points	$N = 2000$

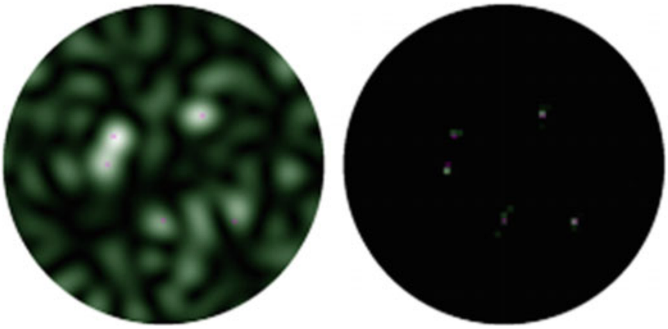

Fig. 2.17 DOA estimation of five simulated aeroplanes crossing the observation area. *Left* DOA estimates from beamforming methods. *Right* amplitude distribution estimates by means of CS methods. The true target position is highlighted by *violet* ‘x’ marker, whereas the estimates are shown in *green* intensity points. Sourced from [52]

CS based radar DOA estimation [55] is another attempt to investigate the application of CS for DOA estimation, specifically for radar (Fig. 2.17).

Even though this approach is successful in theory and has been shown to have favourable results, the application value for implementation lacks system benefits in terms of computational performance or sample reduction. In fact, it adds more complexity to the system and requires additional processing time.

In summary, based on the open literature, there have been minimal investigations as to how CS acquisition and recovery can be developed and applied to DOA estimation tasks in ES resulting in optimized memory and computational use. This puts the work of this monograph well in context.

Springer
http://www.springer.com/978-3-319-46698-9

Compressive Sensing Based Algorithms for Electronic Defence
Mishra, A.K.; Verster, R.S.
2017, X, 184 p. 106 illus., 59 illus. in color., Hardcover
ISBN: 978-3-319-46698-9