An Expert System For Threat Analysis In Radar Warning Receivers

Tunu Miah
Research Associate
Department of Computer Studies
Loughborough University
Ashby Road, Loughborough
LE11 3TU
T.Miah@lboro.ac.uk
01509-222881

Omar Bashir
Post Graduate Student
Department of Computer Studies
Loughborough University
Ashby Road, Loughborough
LE11 3TU
O.Bashir@lboro.ac.uk

Abstract

Historically threat analysis were carried out through manual analysis of measured radar parameters in the RWRs (Radar Warning Receivers) and ESM (Electronic Support Measure) systems by techniques as simple as audio analysis of video signal i.e. modulating pulse train (1). As the threat environment evolved, these manual systems started generating extensive workload for the operators. With advancements in analogue and digital electronics, the threat analysers in the EW (Electronic Warfare) receiving systems evolved from simple analogue filter modules to sophisticated computers employing techniques ranging from simple data matching to those based on neural networks (2)(3).

Emitter identification and threat analysis represent the highest level of signal processing in these systems. Usually threat analysis is combined with emitter identification (4). Unidentified emitters are considered to be threatening, even though they may not be operating in the threatening mode.

A simple threat analysis approach based on syntactic pattern recognition and fuzzy logic is presented here. Threat analysis has been performed separately from emitter identification as it is expected that in a hostile environment emitters may operate with unknown parameters. This would result in relatively accurate prioritisation of the threatening emitters.

1.0 Introduction

RWRs (figure 1) intercept electromagnetic signals incident on the platform, measure their parameters, perform signal identification and threat analysis and provide requisite situation awareness to the human operator (5).

Measurements carried out in the ***sensor*** include calculation of signal carrier frequency, pulse amplitude, pulse time of arrival (TOA), angle of arrival (AOA) and pulse width (PW) (6). On the basis of these parameters the ***pre-processor*** calculates pulse repetition frequency (PRF), type of PRF (for e.g. agile, staggered, fixed etc.), frequency type (for e.g. agile, staggered, bi-channel etc.), antenna scan rate (ASR) and antenna scan type (for e.g. fixed, circular, sectorial, fixed, conical scan etc.) by de-interleaving the incident pulse train (3) (7) (8). These parameters, also known as emitter descriptors, are used to track the detected radar in time. The ***processor*** uses these parameters to identify the emitters, assess the threat posed by them and determine their position with respect to the parent platform.

General Architecture Of EW Receivers

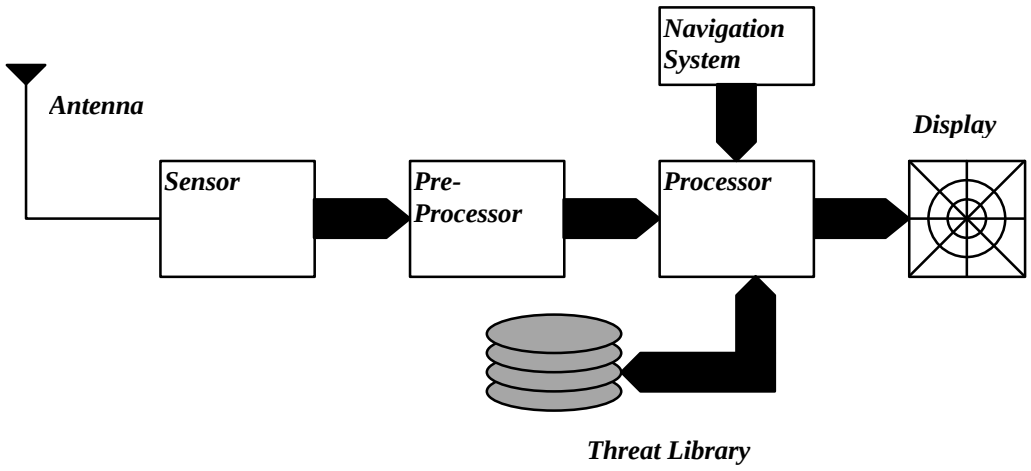

Figure -1

Emitter identification and threat assessment are generally carried out by comparing the parameters in the emitter descriptor with those stored in the threat library (4) (5). Threat library is a database of parameters of various radars and their operating modes. In the simplest case a threat priority level is programmed for each of the operating modes. Once an emitter

and its operating mode have been identified, the pre-programmed threat level is assigned to the emitter descriptor. By default this threat level is the highest for all unknown emitters.

Tracked emitters are then displayed to the operator in a suitable manner. Figure 2 shows one of the most common displays used by RWR systems. Symbols on these displays represent different radars being tracked by the RWR system. The orientation of these symbols from the centre of the display represent the angle of arrival of emissions from the corresponding radars. The distance of these symbols from the centre of the display approximately represent the threat posed by the corresponding radars irrespective of their physical locations. Thus the symbol closest to the centre of the display represents a radar posing the maximum threat.

RWR displays generally have limited space. Emitter densities as well as the complexities of their emissions (for e.g. agility in carrier frequency and PRF, complex antenna scan patterns etc.) in a typical threat environment are also increasing (3) (7) (8) (9) (10). Additionally a radar may operate with totally different (and unknown) parameters during hostilities, i.e. WAR time Modes or WARMs (3). Thus if suitable threat analysis is not carried out in a dense electromagnetic environment, there is a significant possibility that a RWR processor and display will be saturated with unknown emitters categorised as threats.

Radar Warning Receiver Display

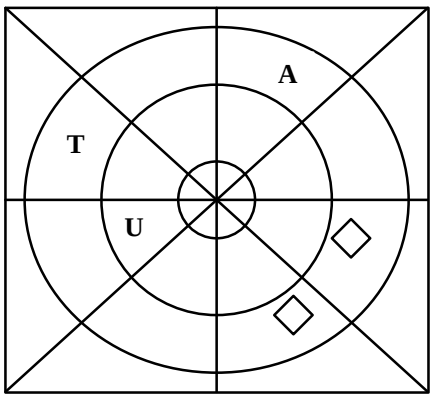

Figure 2

This paper demonstrates the application of a simple syntactic pattern recognition approach to classification of radar emitters. This classification is carried out in three broad categories of threats or threat levels. These categories are ***TRACK***, ***HF_SCAN*** and ***LF_SCAN. TRACK*** represents the category of tracking radars, ***HF_SCAN*** represents the category of scanning radars operating at a high radio frequency and ***LF_SCAN*** represents the category of scanning radars operating at a low radio frequency. This classification is carried out by converting the measured radar parameters to suitable symbols and analysing the combination of these ***terminals*** or constants by appropriate linguistic techniques (11) (12).

Emitters classified as being from ***HF_SCAN*** or ***LF_SCAN*** categories may also represent varying degrees of threat to the platform. It may therefore be desirable that individual emitters within these categories be assigned ***threat levels***. These threat levels provide numerical values to each emitter. The higher the threat level, more threatening is the emitter and visa versa. Assignment of these threat levels is carried out by a ***fuzzy expert system***. It is expected that this simple approach can provide accurate and effective analysis of the electromagnetic threat environment.

This paper proceeds with explaining some other techniques that can be applied to threat analysis and emitter classification. Section 3 discusses some ***rules of thumb*** that are used by radar systems analysts and Electronic Intelligence (Elint) operators to classify unknown emissions. Section 4 explains the proposed system and this paper is concluded after presenting an example that highlights the threat analysis process within the proposed system.

2.0 Techniques Used Currently for Threat Analysis

The effectiveness of the threat analysis approach based on simple data matching (as explained in the previous section) depends upon the accuracy of the data in the threat library. However the accuracy of this data cannot be guaranteed with absolute certainty as the threat environment may change significantly soon after the threat library has been updated.

Operating mode of a radar or its type may be determined by using a rule based system. For example consider the following rules (***frequency*** is measured in ***megahertz***, ***pulse repetition frequency*** in ***hertz*** and ***antenna scan rate*** in ***RPM***)

IF ***frequency*** **<** ***4000*** **AND** ***antenna_scan_type*** **=** ***"circular"*** **AND** ***antenna_scan_rate*** **<** ***20***
AND ***pulse_repetition_frequency*** **<** ***1000*** **THEN**
radar_type **=** ***"scanning"***
ELSE
radar_type **=** ***"tracking"***
IF ***radar_type*** **=** ***"scanning"*** **THEN**
threat_level **=** ***0***
ELSE
threat_level **=** ***1***

These rules classify a radar as being threatening (***threat_level = 1***) or not threatening (***threat_level = 0***). This rule base has to be expanded to handle more threat levels. Moreover errors in measurement of radar parameters may cause mis-classification of a radar type. Thus a pure rule based system may require an extremely large rule base to provide adequate threat analysis. Such systems may also require frequent maintenance so that the rules conform to the current threat scenario.

Vaccaro (3) explains the application of Bayesian Statistics and Shafer Dempster theory in RWRs and ESM systems to provide situation awareness. Bayesian approach requires a precise probability to be estimated for each possibility. Shafer Dempster theory however addresses the problem of objective uncertainty, which is the problem of assigning specific value of probability (confidence) to a proposition, where that assignment is based on insufficient evidence. These techniques require data regarding the operating characteristics of the radars in the environment, which may not be available.

Techniques based on neural networks have also been applied to situation awareness in threat warning systems (2)(3). Although neural networks are capable of processing noisy, incomplete and ambiguous information, they are known to make ***bad guesses*** (3). Moreover use of conventional computing elements increases the computational time excessively thereby necessitating the use of specialised neural computers.

The ability of fuzzy set theory to describe vagueness, ambiguity or lack of precision make them suitable for application in threat analysis and situation awareness. Fuzzy sets aim to quantify linguistic variables such as ***high threat*** or ***low threat*** etc. thus providing a mechanism for numerical manipulation of these variables. Moreover assignment of characteristic functions to quantify these linguistic variables is subjective (not arbitrary) in nature. Fuzzy expert systems may be developed to provide a relative grade or value of threat a particular emitter poses on the basis of its measured parameters.

3.0 Human Decision Making Process in a Threat Environment

Traditionally the threat level associated with a particular operating mode of a radar is determined by human Electronic Intelligence (Elint) operators. Even today in large platforms like warships, RWR data can be viewed by an operator. This operator decides, with the assistance of a computer, which emission poses a greater threat than the others.

Elint analysis requires some calculations to be carried out on the observed parameters that may indicate the identity and/or possible operating mode of the radar (13). However in the field, i.e. in tactical situations, this classification has to be carried out as quickly as possible. Electronic warfare systems operators have generally developed some basic ***rules of thumb*** to counter such situations. On the basis of these rules this categorisation is performed almost as a cognitive process. Some of the most well known rules are listed below.

3.1 Beware of Continuous Wave (CW) Signals

CW radars are generally used for Doppler airborne navigation systems and radio altimeters (14). However some potentially lethal applications for such radars are illuminators for tracking radars as well as proximity fuses in weapon systems (14).

3.2 To Hit You, They Have to Aim at You

Aiming here means tracking. When a radar switches from a search or surveillance mode to tracking mode, an attack is imminent and the threat level increases considerably. Tracking may be characterised by the following antenna scan patterns

- ***Fixed*** antenna scan type determined by the pre-processor. This scan pattern has no amplitude modulation on the intercepted pulses due to the radar antenna scanning (13).

- ***Conical*** scanning (14) (15) is also considered to be threatening.

- Electronic scanning systems can generate ***complex*** scan patterns (4) which may be dependant on the system characteristics as well as the number of targets being tracked by them (13). As RWRs generally perform relatively coarse measurements and calculations on the intercepted emissions (3) (9), characteristics of complex scan patterns cannot be determined by such systems. Complex scan patterns are therefore also considered as threatening.

3.3 High Frequency may Present Substantial Threat

At frequencies higher than 4 GHz i.e. ***c***, ***x*** and ***k*** bands (16), size of microwave components and devices reduces considerably. As a result radar systems designed to operate in these bands can be carried in mobile platforms, for e.g. warplanes (16) and guided weapons (17). Radar systems for information gathering like precise target location and tracking can also be found in these bands. Skolnik (16) refers to ***s*** band as a compromise for medium range aircraft detection and tracking when a single radar must be used for both functions. Lower frequency bands are generally more suitable for long and medium range surveillance radar systems.

3.4 If They Are Interested In You, They Will Keep In Touch

Tracking is the operation of locating a target and following its movement in range, elevation and in azimuth (13) (15). Tracking modes of most tracking radars can be characterised by a fixed amplitude pattern of pulses received by the RWR. One notable exception is the tracking of targets carried out by computers in modern search radar systems (14). Potentially dangerous systems amongst these are characterised by high antenna scan rates thereby providing a relatively rapid update regarding target characteristics.

These rules are derived from the information captured from the operators, the technical documentation of various radar systems and electronic intelligence procedures. Rule base threat analysers are expected to be simpler and more efficient than present systems, even though they are limited to classifying radars in a finite number of classes. Due to the subjective nature of threat assessment and the uncertainty involved in its determination, simple rule based systems have to be augmented with techniques that can provide reasonably accurate results.

4.0 A Threat Analysis Subsystem Based on Rules and Fuzzy Logic

The threat analysis subsystem described here consists of two major components i.e. the ***classifier*** and the ***prioritiser*** (figure 3). The classifier uses the measured frequency, emission type and antenna scan type to classify the emitter as being a tracking (***TRACK***), high frequency scan (***HF_SCAN***) or a low frequency scan (***LF_SCAN***) radar.

All tracking radars are assigned the highest priority i.e. 1.0 . Threat levels or priorities are calculated separately for scanning radars of ***HF_SCAN*** and ***LF_SCAN*** radar classes. These priorities are calculated by applying a fuzzy expert system to the measured values of PRF and antenna scan rate.

Threat Analysis Sub-system

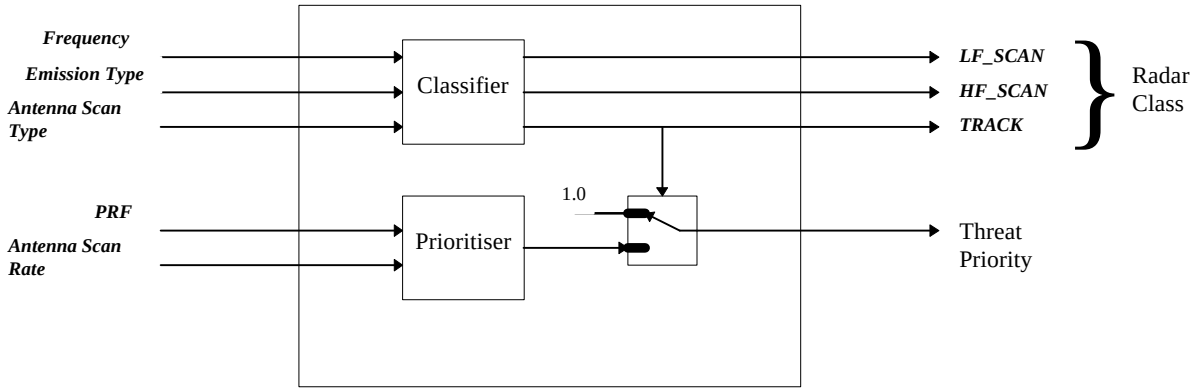

Figure - 3

Following paragraphs describe the classifier and the prioritiser in detail.

4.1 Classifier

As mentioned previously, threat analysis involves high level recognition and classification. Classification at this level may conveniently be carried out by employing linguistic computation (18). Contrary to the pattern recognition techniques applied at lower processing levels, relationships between various primitives need to be investigated (19). These relationships between various primitives may then be classified using appropriate grammar (11) (12). A syntactic classifier is employed to classify the intercepted emissions as being from either one the following classes (decreasing order of threat)

- ***TRACK*** : Tracking radars
- ***HF_SCAN*** : Radars operating at high radio frequency
- ***LF_SCAN*** : Radars operating at low radio frequency

The classifier uses only the measured frequency, emission type and antenna scan type to classify the intercepted emission.

Let V_T be the set of terminals or primitives that are extracted from the measured radar data

$$V_T = \{ p , l , s , c , x , k , cw , pul , fxd , cpx , cs , sct , cir \} \quad [1]$$

where

p , l , s , c , x , k : different carrier frequency bands (Table 1). This is a standard classification of emissions on the basis of radio frequency (12).

cw , pul : carrier frequency type i.e. continuous wave radar or pulsed radar. Here ***pul*** is used to identify all types of pulsed radar even those operating in agile and staggered prf modes

fxd , cpx , cs , sct , cir : antenna scan types in azimuth (Table 2) (13)

Carrier Frequency Bands

Band Designation	Thresholds (in GHz)
p	$0.7 \leq f < 1.0$
l	$1.0 \leq f < 2.0$
s	$2.0 \leq f < 4.0$
c	$4.0 \leq f < 8.0$
x	$8.0 \leq f < 12.5$
k	$12.5 \leq f < 18$

Table 1

A suitable set of ***non-terminals*** or expressives may be given as follows

$$V_N = \{TRACK, HF\_SCAN, LF\_SCAN, SCAN\} \quad [2]$$

where

TRACK, ***HF_SCAN*** and ***LF_SCAN*** are different classes of radars whereas ***SCAN*** is a general class for all scanning radars.

P: ***TRACK*** → ***cw*** [3]

TRACK → ***cs*** [4]

TRACK → ***fxd*** [5]

TRACK → ***cpx*** [6]

SCAN → ***cir*** [7]

SCAN → ***sct*** [8]

HF_SCAN → ***SCAN.k*** [9]

HF_SCAN → ***SCAN.x*** [10]

HF_SCAN → ***SCAN.c*** [11]

LF_SCAN → ***SCAN.s*** [12]

LF_SCAN → ***SCAN.l*** [13]

LF_SCAN → ***SCAN.p*** [14]

Bottom up parsing (11) can be applied conveniently. Primitives extracted from various radar parameters are applied to the production rules successively till the emission is classified into a suitable class.

Other measured parameters that can be used in emitter classification are measured emission amplitude variation and measured emission angle of arrival (AOA) variation. These parameters can be used to provide an indication of mobility of the emitter being tracked. If the emitter is mounted on a mobile platform, then the motion of the platform would vary the peak signal amplitude differently as compared to emissions from static emitters. Moreover relative Angle of Arrival (AOA) of the incident radar pulses also varies for emitters mounted on a mobile platform. This is detected only if the platform on which the radar is mounted has a tangential component of the velocity.

Antenna Scan Types

Designation	Description	Characteristics
fxd	Fixed Scan Type	Radar locked on to the target i.e. tracking
cpx	Complex Scan Type	Scanning parameters could not determined, characteristic of electronic scanning radars
cs	Conical Scanning	Characteristic of conical scan tracking radars
sct	Sectorial Scanning	Limited Area Search
cir	Circular Scanning	Conventional Search Pattern

Table 2

Classification of emission on the basis of amplitude and AOA variations may be complex and may require data from several scan cycles before a reasonable decision may be taken. The output power of the emitter may also be varied after target detection in a manner so as to confuse the RWR on a target in believing that the emitter is static (20).

4.2 Prioritiser

Prioritiser analyses other emission parameters measured (antenna scan rate and pulse repetition frequency) by the RWR to provide a threat level or priority to each emitter in the ***HF_SCAN*** or ***LF_SCAN*** class. Pulse repetition frequency (PRF) provides an indication of the maximum unambiguous range of the radar whereas the antenna scan rate (ASR) may considered to be directly proportional to the rate at which the radar updates its internal representation of the environments. A radar operating at high PRF and ASR therefore poses a higher level of threat than a radar operating at a lower PRF and ASR.

Classification of radars on the basis of PRF or ASR is largely subjective. There are no standards for such classification as compared to the one mentioned in table 1 for frequency. Moreover assessment of threat posed by an emission is also subjective in nature and depends upon a number of factors for e.g. order of battle or the combat scenario and the type of conflict (full scale war, cold war, insurgency etc.).

Prioritiser thus attempts to determine the threat level posed by a particular emission with a fuzzy expert system. Membership values for PRF and ASR are calculated from their ***membership functions*** (21)(22)(23). These membership values determine the degree of truth for each rule in the fuzzy rule base. ***MIN inferencing*** and ***MAX composition*** is used to generate the fuzzy subset for the output variable i.e. threat level. The threat level is determine by appropriately ***defuzzifying*** the output fuzzy subset.

Fuzzy subset for ASR can be represented as

$$asr = \{(asr, m_{asr\_l}), (asr, m_{asr\_m}), (asr, m_{asr\_h})\} \quad [15]$$

where

m_{asr_l} : is the membership function for low antenna scan rate

m_{asr_m} : is the membership function for medium antenna scan rate

m_{asr_h} : is the membership function for high antenna scan rate

Membership functions for ASR may subjectively be represented as follows

$$m_{asr\_l} = \begin{cases} 1 & ; \quad asr \le 5 \\ 0 & ; \quad asr \ge 15 \\ 1.5 - \dfrac{asr}{10} & ; \quad 5 < asr < 15 \end{cases} \qquad [16]$$

$$m_{asr\_m} = \begin{cases} 1 & ; \quad 15 < asr \le 20 \\ 0 & ; \quad 5 \ge asr > 30 \\ \dfrac{asr}{10} - 0.5 & ; \quad 5 < asr \le 15 \\ 3 - \dfrac{asr}{10} & ; \quad 20 < asr < 30 \end{cases} \qquad [17]$$

$$m_{asr\_h} = \begin{cases} 0 & ; \quad asr \le 20 \\ 1 & ; \quad 30 < asr \\ \dfrac{asr}{10} - 2 & ; \quad 20 \le asr \le 30 \end{cases} \qquad [18]$$

Membership Functions for Antenna Scan Rate

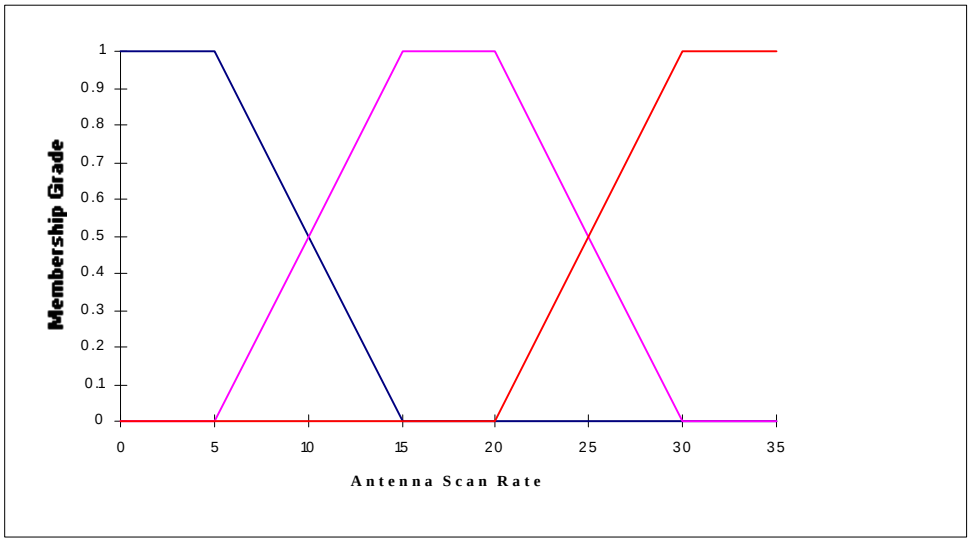

Figure 4

Similarly the fuzzy subset for PRF may be represented as

$$prf = \{(prf, m_{prf\_l}), (prf, m_{prf\_m}), (prf, m_{prf\_h})\} \quad [19]$$

where

m_{prf_l} : is the membership function for low prf

m_{prf_m} : is the membership function for medium prf

m_{prf_h} : is the membership function for high prf

Membership function for PRF may subjectively be represented as follows

$$m_{prf\_l} = \begin{cases} 1 & ; \quad prf \le 250 \\ 0 & ; \quad prf \ge 750 \\ 1.5 - \dfrac{prf}{500} & ; \quad 250 < prf < 750 \end{cases} \quad [20]$$

$$m_{prf\_m} = \begin{cases} 1 & ; \quad 750 \le prf \le 1250 \\ 0 & ; \quad 250 \ge prf \ge 1750 \\ \dfrac{prf}{500} - 0.5 & ; \quad 250 < prf < 750 \\ 3.5 - \dfrac{prf}{500} & ; \quad 1250 < prf < 1750 \end{cases} \quad [21]$$

$$m_{prf\_h} = \begin{cases} 1 & ; \quad 1750 \le prf \\ 0 & ; \quad 1250 \ge prf \\ \dfrac{prf}{500} - 2.5 & ; \quad 1250 < prf < 1750 \end{cases} \quad [22]$$

A fuzzy subset for threat level (***threat_level***) may be represented as follows

$$threat\_level = \{(threat\_level , m_{low\_threat}) , (threat\_level , m_{medium\_threat}) , (threat\_level , m_{high\_threat})\} \quad [23]$$

where

m_{low_threat} : membership function for low threat

m_{medium_threat} : membership function for medium threat

m_{high_threat} : membership function for high threat

Membership Functions for Pulse Repetition Frequency

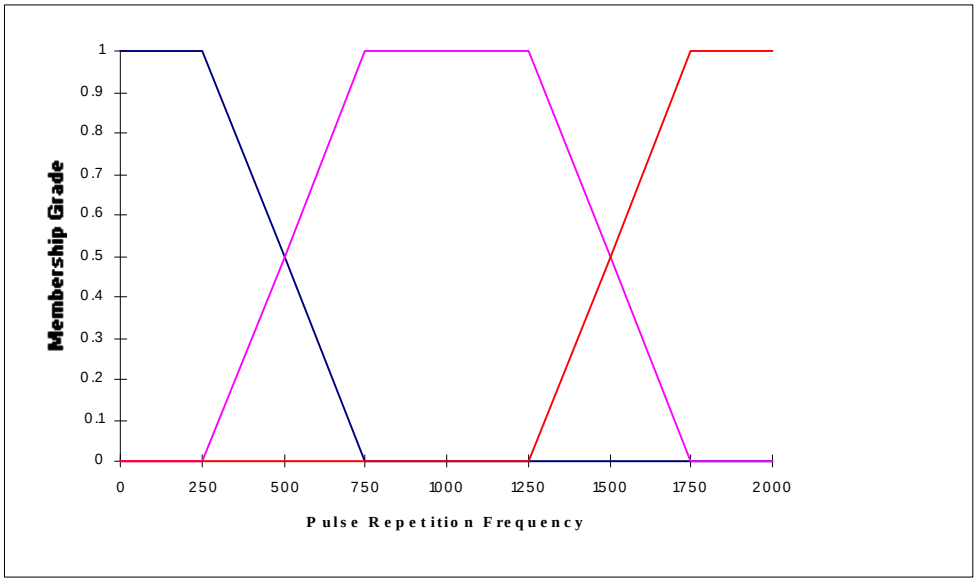

Figure 5

Membership function for ***threat_level***, as mentioned previously, may depend on a number of factors. These may be determined by the knowledge of number of emitters in the environment and assigning a threat level and threat category i.e. low, medium and high, to each type. The resulting distributions of each category of threat may represent the membership function for that category. In this paper, membership functions for threat level have been assigned as follows.

$$m_{low\_threat} = \begin{cases} 1 & ; \quad 30 \geq threat\_level \\ 0 & ; \quad threat\_level > 37 \\ \dfrac{37 - threat\_level}{7} & ; \quad 30 \leq threat\_level \leq 37 \end{cases} \quad [24]$$

$$m_{medium\_threat} = \begin{cases} 0 & ; \quad 70 \leq threat\_level \leq 30 \\ 1 & ; \quad 37 \leq threat\_level \leq 63 \\ \dfrac{threat\_level - 30}{7} & ; \quad 30 \leq threat\_level \leq 37 \\ 10 - \dfrac{threat\_level}{7} & ; \quad 63 < threat\_level < 70 \end{cases} \quad [25]$$

$$m_{high\_threat} = \begin{cases} 0 & ; \quad threat\_level \leq 63 \\ 1 & ; \quad 100 \geq threat\_level > 70 \\ \dfrac{threat\_level}{7} - 9 & ; \quad 63 < threat\_level < 70 \end{cases} \quad [26]$$

Membership Functions for Threat Level

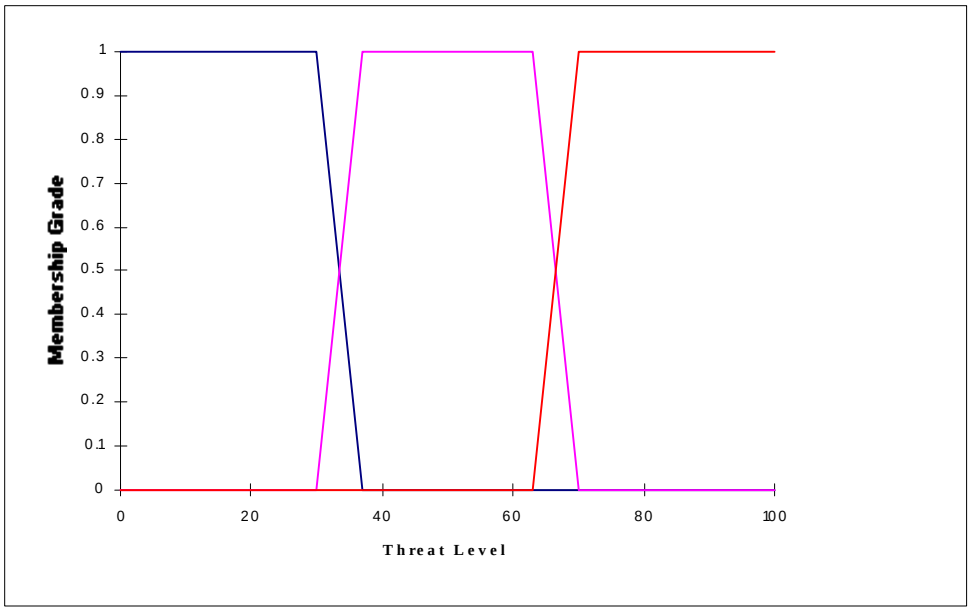

Figure 6

The rules are listed as follows

IF asr is high THEN threat is high

IF asr is low THEN threat is low

IF asr is medium AND prf is low THEN threat is low

IF asr is medium AND prf is medium THEN threat is medium

IF asr is medium AND prf is high THEN threat is high

An example in the next section will explain the operation of the entire threat analysis sub-system in detail.

5.0 Example

This section discusses an example that clarifies the operation of the classifier and the prioritiser discussed in the previous sections. Consider an emission that has been intercepted and its characteristics measured by the RWR. Its parameters are listed as follows

Frequency	:	1300 Megahertz , ***l*** band
Emission Type	:	***pul***
PRF	:	480 Hertz
Antenna Scan Type	:	***cir***
Antenna Scan Rate	:	6 revolutions per minute

The classifier first uses the emission type and applies it to the production rules. Classifier is unable to classify the emission solely on the basis of the emission type. Then the antenna scan type is applied to the production rules. The classifier classifies the emission as being from a ***SCAN*** radar. Output of the classifier is concatenated with the frequency band of the emission i.e. ***l*** and the concatenated string ***SCAN.l*** is applied to the production rules. The classifier is able to classify the emission as being from a ***LF_SCAN*** radar.

As the emitter has been classified as being an ***LF_SCAN*** radar, its threat priority has to be derived from the antenna scan rate and PRF by the prioritiser. Following membership values for the PRF are generated inside the prioritiser

m_{prf_h} = 0

m_{prf_m} = 0.46

m_{prf_l} = 0.54

Similarly following membership values are generated for the antenna scan rate inside the prioritiser

m_{asr_h} = 0

m_{asr_m} = 0.1

m_{asr_l} = 0.9

These membership functions generate the following truth values for each of the rules in the fuzzy expert system

IF asr is high THEN threat is high	**0**
IF asr is low THEN threat is low	**0.9**
IF asr is medium AND prf is low THEN threat is low	**0.1**
IF asr is medium AND prf is medium THEN threat is medium	**0.1**
IF asr is medium AND prf is high THEN threat is high	**0**

MIN inferencing is then applied i.e. the output membership function is clipped off at a height corresponding to the rule premise's computed degree of truth. All the membership functions generated for each output variable are then combined together to form a single fuzzy subset for each output variable. This accomplished by ***MAX composition*** where the combined output fuzzy subset is constructed by taking the pointwise maximum over all of the fuzzy subsets assigned to the output variable by the inference rule. This generates the following fuzzy subset ***threat_level*** (figure 7).

$$fuzzy_{threat\_level} = \begin{cases} 0.9 & ; \quad 0 \le threat\_level \le 30.7 \\ \dfrac{37 - threat\_level}{7} & ; \quad 30.7 < threat\_level < 36.3 \\ 0.1 & ; \quad 36.3 \le threat\_level \le 69.3 \\ 10 - \dfrac{threat\_level}{7} & ; \quad 69.3 < threat\_level < 70 \\ 0 & ; \quad 70 \le threat\_level \le 100 \end{cases} \qquad [27]$$

Finally defuzzification is carried out to provide a figure for the threat level. A number of defuzzification methods ranging from calculation of the ***centroid*** to ***average of maxima*** can be applied. Here a simple value is calculated by calculating the weighted sum of the mean position of the shaded areas in figure 7. This provides a threat level of 19.1.

Fuzzy Subset for Output Variables

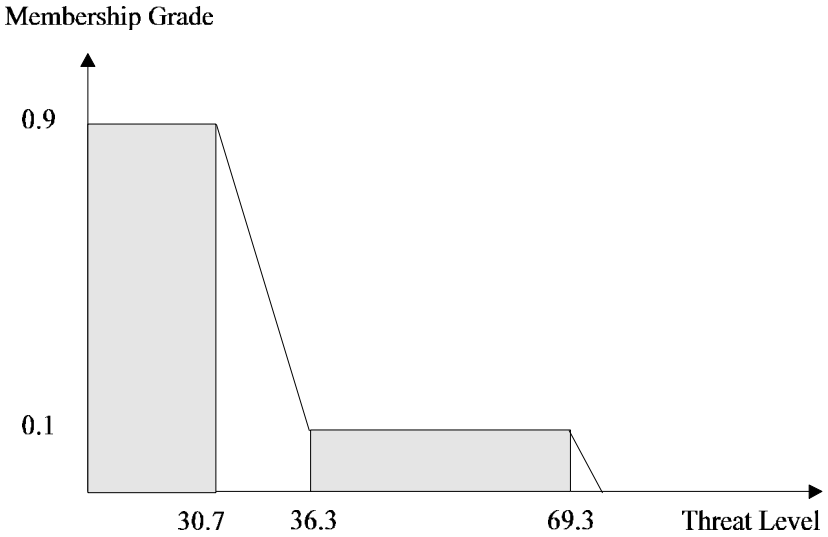

Figure 7

The same radar can operate at a different mode where its emission parameters change to the following

Frequency	:	1300 Megahertz , ***l*** band
Emission Type	:	***pul***
PRF	:	691 Hertz
Antenna Scan Type	:	***cir***
Antenna Scan Rate	:	12 revolutions per minute

Although the radar is still classified as an ***LF_SCAN*** but its threat priority is increased to 39.82. This is due to the increase in the antenna scan rate as well as the PRF.

6.0 Conclusions

This paper presents a threat analysis sub-system for radar warning receivers and electronic support measure receivers. Syntactic measures for emitter classification employed here can be implemented by a simple rule base and a bottom up parser. A fuzzy expert system is used to prioritise threats within each threat category. The fuzzy rule base used in this system allows effective description of parameters that are generally evaluated subjectively. Moreover each threat is assigned a specific priority level corresponding to the threat that it poses thereby attempting to provide an accurate representation of the threat scenario.

Threat classification is carried out separately from emitter identification as it is expected that emission parameters will vary in different scanerios. Thus the threat posed by all unidentified emitters can be evaluated using these measures. It is expected that such measures will provide reasonably realistic evaluation of the threat in the electromagnetic environment. This will in turn reduce the work load of the operators of such systems, enabling them to make judgements and take actions which would correspond to actual threat environment. Moreover system resources such as display, jammers etc., may also be programmed to handle more threatening emitters with a higher priority.

The approach described here provides results which are more accurate as compared to techniques based on simple data matching and rule based systems. When compared with techniques based on Bayesian analysis and neural networks, this technique is simple and effective.

Threat analysis can be viewed as an instance of task scheduling. Thus the approach discussed here can be applied to task scheduling in other domains. Tasks assigned to a system can be broadly categorised into distinct classes. Each task within a class can be assigned a priority level depending upon the different attributes of the task. A task processor can then process each task on the basis of the priority assigned to it.

References

1. FULLER, K.L. *To see and not be seen,* IEE Proceedings. 137F(1), February 1990, 1-9.
2. HEWISH, M. *Neural computing, bringing brain power to defence.* Defence Electronics & Computing Supplement to International Defence Review, February 1990, 17-19.
3. VACCARO, D.D. *Electronic warfare receiving systems.* Artech House Inc., 1993.

4. ROE, J., CUSSONS, S. & FELTHAM. A. *Knowledge based signal processing for radar ESM systems.* IEE Proceedings, 137F(5), October 1990, 293-301.

5. GOLDEN, A. Jr. *Radar electronic warfare.* American Institute of Aeronautics and Astronautics Inc., 1987.

6. TSUI, J.B.Y. *Microwave receivers with electronic warfare applications*. John Wiley & Sons, 1986.

7. ROGERS, J.A.V. *ESM processor system for high pulse density radar environment.* IEE Proceedings, 132F(7), December 1985, 621-625.

8. WHITTAL, N.J. *Signal sorting in ESM systems*. IEE Proceedings, 132F(4), July 1985, 226-228.

9. DODD, R.W. *EW receivers use multiple technologies*. Defence Electronics, September 1990, 59-65.

10. YAGHAR, R.A. *Eight laws of electronic combat*. Journal of Electronic Defense, January 1991, 62-65 .

11. TOU, J.T. & GONZALEZ, R.C. *Pattern recognition principles.* Addison Wesley Publishing Company Inc., 1974.

12. FIREBAUGH, M .W. *Artificial Intelligence, a knowledge based approach.* Boyd & Fraser Publishing Co. ,1988.

13. WILEY, R.G. *Electronic Intelligence : the analysis of radar signals.* Artech House,1993.

14. SKOLNIK, M.I. *Introduction to radar systems.* McGraw Hill Inc., 1980.

15. KINGSLEY, S. & QUEGAN, S. *Understanding radar systems.* McGraw Hill Book Company, 1992.

16. SKOLNIK, M.I. *Radar handbook.* McGraw Hill Inc., 1970

17. PARKER, D. & MAURER, H.A. *The era of active RF missiles.* Microwave Journal, February 1984, 24-34.

18. KANAL, L. *Patterns in pattern recognition 1968-1974.* IEEE Transactions on Information Theory, IT-20(6), November 1974, 697-722.

19. CHEN, C.H. *On statistical and structural feature extraction.* Pattern Recognition and Artificial Intelligence, C.H. Chen, Academic Press, 1976.

20. JOHNSTON, S.L. *CESM - A new category of radar ECCM.* IEEE AES Magazine, 10(2), February 1995, 36-38.

21. KANDAL, A. *Fuzzy techniques in pattern recognition.* John Wiley & Sons, 1982.

22. BEZDECK, J.C. *Partition structures : A tutorial.* Analysis of Fuzzy Information, Vol III, J.C. Bezdeck, CRC Press Inc., 1987.

23. GRAHAM, I. & JONES, P.L. *Expert Systems : Knowledge, uncertainty and decision*. Chapman & Hall, 1988.