# Threat Evaluation and Jamming Allocation

Nicholas R. Osner [*], Warren P. du Plessis

Department of Electrical, Electronic, and Computer Engineering, University of Pretoria, Lynnwood Road, Pretoria, South Africa
[*]nicholasosner@gmail.com

**Abstract:** A threat evaluation and jamming allocation (TEJA) system is proposed and implemented in order to optimise the jamming strategy of a platform. This TEJA system accounts for the different effects of jamming techniques on threats and radar modes, the interaction between jamming techniques and channels, the relative frequency and bandwidth used by threats, the uncertainty of the threat environment, and models the progression of threats through various radar modes from initial search to final guidance. Performance of the TEJA system is evaluated for a complex mission which considers a platform with two jammers penetrating an area with ten threats. The TEJA system is shown to be computationally efficient by using an exhaustive search to determine the optimum jamming strategy. The developed jamming strategy allows the platform to survive a mission despite its complexity.

## 1. Introduction

In the theatre of battle, the electromagnetic spectrum (EMS) has become a very complex arena due to the large number of both friendly and adversary platforms attempting to gain superiority over each other, including aircraft, ships, missiles, artillery etc.. To further complicate matters, each platform can mount an array of systems which operate in the EMS including radars, communications systems, jammers, etc. – often more than one of each. This complex realm includes numerous interactions between the various countermeasures and counter-countermeasures implemented by all parties. These interactions include the illumination of platforms, making them easier for adversaries to detect and engage, as well as both constructive and destructive interactions between jamming strategies, which can either increase or decrease jammer effectiveness. It is this complex nature of engagements within the EMS that requires the automation of the process of threat evaluation and jamming allocation (TEJA), so as to maximize the probability of survival of a platform.

Currently, there are many threat evaluation and weapon assignment (TEWA) systems that allocate weapon systems to adversary platforms according to the threat level they pose (e.g. [1], [2]). These systems represent a similar problem to that of TEJA in terms of threat evaluation and allocation of resources, but do not take into account the specific characteristics associated with actions in the EMS.

To account for these differences, a few TEJA systems have been proposed (e.g. [3] - [7]). Most of these systems use threat levels for prioritisation of threats in conjunction with either a jamming factor, or a probability of jamming success to determine the optimal allocation of jamming resources. However, these systems only allocate jamming resources to the threats without determining the optimal jamming techniques to be used. The exception to this is the system developed by Noh and Jeong, but even then, this system only chooses between either active or passive countermeasures against either radio frequency (RF) or infrared (IR) threats, rather than the specific techniques [3]. Secondly, the constructive and destructive interactions between different jamming techniques and their signals are not taken into account, despite the fact that such interactions are inherent in all actions in the EMS. This is one of the major differences to TEWA systems, in that jamming strategies will work effectively for some threats, but illuminate the platform for others depending on the frequencies and bandwidths used as well as on threat radar modes. Existing TEJA systems also do not take into account the future effects of current jamming actions which result from the progression of the radar modes of the threats from search to guidance. Finally, the inherent uncertainty involved in the threat environment is also not taken into account by these systems.

This work details a TEJA system that accounts for all of the factors listed above, including the effects of different jamming techniques on each threat, interactions between jammers, radar modes and their progression, the effects of different operating frequencies, and threat uncertainties. Also, a number of user-definable parameters allow a wide range of systems to be modelled. Despite the complexity of this problem, the models and approaches used are surprisingly simple while still capturing the most significant characteristics of the problem. The application of the proposed technique is demonstrated by considering a complex engagement with a large number of different threats engaging a platform with two jammer channels. This example engagement demonstrates that all the issues highlighted above are addressed while ensuring that the formulation remains simple and computationally efficient enough to allow an exhaustive search to be used to optimise the programming of the platform's EW systems.

The structure of this paper is as follows. Section 2 covers a description of the problem, along with all constraints and assumptions. Section 3 covers the concept of threat evaluation, Section 4 covers jamming allocation, and Section 5 covers the example scenario used to demonstrate system performance. Finally, Section 6 discusses the results of the scenario.

## 2. Problem Description

The problem considered is the automatic planning of a jamming strategy which can be used by the electronic warfare (EW) system on a platform to counter a number of interacting threats. The nature of this problem is such that a wide range of radar, jammer and EMS concepts need to be considered and modelled for such a TEJA system to be successful. The jamming techniques, weapon types, and interactions considered below are considered in a range of EW reference materials (e.g. [8] - [10]).

Due to the large number of platform types in existence, both friendly and adversary, and the large number of systems each platform contains, the TEJA system had to be developed with a large amount of variability. In this way, a user can modify system parameters according to the specific platforms and their unique systems involved in a scenario.

Note that due to the fact that this system is a high-level model, it is assumed that all the radar parameters are captured in these various user-defined system parameters, rather than accounted for specifically and individually. Further, due to the large scope of the problem and the large number of interactions at play, the system has been developed using an idealised model that excludes certain effects such as atmospheric attenuation. Also, a perfect electronic support (ES) system is assumed in order to keep the problem bounded and manageable. Note that the parameters used in this paper are heuristically obtained and chosen so as to emulate real-world systems at an idealised level and thus do not represent specific systems.

The overall problem is that of a single platform, equipped with a two-channel active jamming system, entering adversary territory. The scenario is set up by entering the mission waypoints of the platform through the territory, as well as the locations of adversary platforms using a three-dimensional Cartesian coordinate system. Other aspects of the threats are also entered, including the weapon system type, accuracy, weapon range, radar range, projectile velocity, probability of encounter, radius of likely encounter, and radar stage progression rate.

This mission is divided into a number of individual encounters separated by a constant time interval. Each encounter is then individually handled and optimised, where the time interval can be chosen according to the desired compromise between speed and accuracy of the system. The flow diagram for each individual time interval appears in Fig. 1 with each stage being described in detail below.

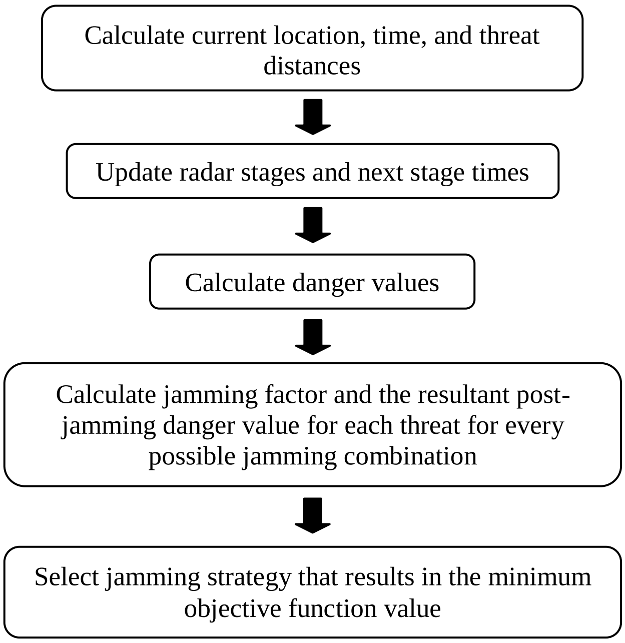
Calculate current location, time, and threat distances
Update radar stages and next stage times
Calculate danger values
Calculate jamming factor and the resultant post-jamming danger value for each threat for every possible jamming combination
Select jamming strategy that results in the minimum objective function value

***Fig. 1**. Flow diagram of the system for each individual time interval.*

It is assumed that each channel of the platform’s electronic countermeasure system (ECM) is able to implement the same five major jamming techniques: range-gate pull off (RGPO), velocity-gate pull off (VGPO), noise jamming (NJ), cover pulse (CP), and multiple false targets (MFT). It is also assumed that the radar modes of threats can be divided into a sequence of stages comprising search, acquisition, tracking and guidance (in that order), with artillery threats skipping the final stage. Search and acquisition can be grouped into the general category of search-type stages, and tracking and guidance into the category of tracking-type stages.

Threats are required to progress through the radar stages, each using a different radar mode, as well as have these broken when jammed. This is achieved by using user-defined search, acquisition, and tracking times that indicate the average time taken for a threat to progress to the next radar stage. Guidance time is calculated using the position of the threat and platform at the time of firing, along with the known projectile velocity. Break-lock is handled by a user-defined threshold. Should the performance of the threat’s radar be reduced below this threshold, lock is broken, and the radar stage reset to the search stage.

Due to the discrepancy in ranges between a threat’s weapon systems and its radar systems, there are separate ranges defined for each. A threat will be unable to progress through the search stage if the platform is outside the radar range. Once the platform enters this range, the threat is able to then progress from the search stage through to the end of the tracking stage, but will be unable to fire until the platform enters its weapon range. Once a threat has fired, it will enter the guidance stage before returning to the beginning of the tracking stage, requiring lock to be broken before it will return to the search stage.

To reduce the need for complex artificial intelligence to drive the movements and reactions of the threats, a simple distributed threat technique is used. In this approach, each threat is allocated a probability of occurrence, and a radius of likely encounter, rather than a point location. More mobile threats, and threats with less precisely known locations, are allocated a larger radius of likely encounter. On the other hand, a probability of occurrence accounts for incorrect intelligence, threats being under maintenance, etc.. An overall probability of encounter for a particular time interval is then calculated as the product of the portion of the distributed threat area within range and the probability of occurrence of the threat.

A final consideration is the accuracy of the threats. The accuracy of semi-active and active missiles is assumed to remain constant due to the fact that their receiver and guidance systems are built into the missile. However, for artillery threats, as well as command and beam-riding missiles, accuracy is assumed to be constant up to half of their maximum range, after which their accuracy decreases linearly. This accounts for the fact these weapon types are either fired or guided from the threat itself, and hence are limited by angular accuracy (where it is assumed that this angular accuracy is greater than required for the first half of the maximum range).

## 3. Threat Evaluation

Threat evaluation is the first step in the TEJA process, where the current EMS environment is scanned and processed in order to determine the status and characteristics of the current threats that are engaging the platform. This task would be performed by onboard ES systems that are able to identify threats according to a known database. Once the status and characteristics of current threats are known, the EW controller will prioritise threats using danger values.

For the present system, the danger value ($D_n$) of the $n^{\text{th}}$ threat is calculated using a number of factors: the probability of encountering the threat in the current time interval ($P_n$), as well as the radar stage ($S_n$), range adjusted accuracy ($A_n$), and projectile time (in hours) to platform ($T_n$) of the threat. The time (in seconds) to the next radar stage ($N_n$) for the threat is also included. These factors are normalised before being combined to form a weighted-sum objective function [11] giving

$$D_n = P_n[W_s S_n + W_a A_n + W_t(1 - T_n) + W_n(1 - N_n)] \tag{1}$$

where $W_s$, $W_a$, $W_t$, and $W_n$ are the weights for the above parameters. The weights are user-defined allowing a user to optimise system performance for their particular application. In this equation, $P_n$ is used as a multiplicative factor so as to scale the danger value of a threat according to the likelihood of it actually being encountered.

For (1), the danger value is set to zero if the threat is at a greater distance from the platform than its maximum radar range, preventing the platform from unnecessarily allocating resources to that threat. Larger probabilities of encounter and distance-adjusted accuracy values increase the danger value of a threat. On the other hand, shorter projectile-to-platform times and times to next radar stage increase the danger value, hence the use of one minus these normalised values. The normalised radar stage is represented using the numbers 0.25, 0.5, 0.75 and 1.0 for the stages in order from search through to guidance. As a result, the further along a threat is in its engagement of the platform, the greater the threat level it poses.

Normalisation of the factors in (1) is achieved as follows. Both $S_n$ and $A_n$ are by their definition already normalised. $T_n$ is normalised using $T_{max}$, the maximum expected projectile time to platform, which is defined as the time, in hours, taken by the slowest projectile to cover the largest range in the scenario. $N_n$ is normalised using the largest time to next stage value of all the threat types.

The weights can take on any positive value, where their relative magnitudes are of importance, rather than their individual values. Since the progress of the radar stages of a threat is the biggest indication of how soon it will engage the platform, the stage weight is given the largest weighting of 6.0 (chosen so that it is greater than half of the sum of the weights). Thereafter, the projectile time to platform, the time to next stage weight, and the accuracy weighting are set to 2.5, 1.0 and 0.5 respectively. This weighting approach prioritises threats that are closer to the platform in order to counteract the biasing effect of increased jamming-to-signal ratio (JSR) for further threats. Thereafter threats that are further along their engagement process are prioritised and then finally more accurate threats.

## 4. Jamming Allocation

The allocation of jamming resources forms the second part of the TEJA system, and must take into account numerous factors including the jamming techniques used, their effectiveness on each stage of radar engagement, their interaction with each other, and the cross effect of techniques on different threats due to frequency domain usage.

Each of the two jamming channels is allocated a jamming technique and threat type which the jamming is targeted at. It is assumed that the threats in the threat library are listed in order of ascending frequency band usage, meaning that threat type one operates at the lowest frequency, and threat type ten operates at the highest frequency.

### *4.1 Jamming Effect*

The post-jamming danger value is computed using

$$V_n = F_n \times D_n = \left(1 - E_{n,final}\right) \times D_n \tag{2}$$

where $V_n$ is the post-jamming danger value, $F_n$ is the jamming factor, and $E_{n,final}$ is the final jamming effect. The jamming factor is a multiplicative factor used to account for the effect of jamming on the danger value posed by a threat. It is defined such that a jamming factor value of 0.8 indicates a 20% reduction in the performance of the radar system of a threat. The jamming factor is calculated from the jamming effect as shown in (2).

A positive jamming effect indicates a positive jamming effect, and results in a jamming factor of less than one. On the other hand, a negative jamming effect indicates a negative jamming effect (illumination of the platform), and results in a jamming factor of greater than one that will enhance the danger value.

The jamming effects for the $n^{\text{th}}$ threat for each of the two jamming channels of the ECM system of the platform, are calculated using

$$E_{n,1} = \mathrm{SE}(S_n, J_1) \times I_{1,2} \times \mathrm{CE}(O_1, Y_n) \tag{3}$$

$$E_{n,2} = \mathrm{SE}(S_n, J_2) \times I_{2,1} \times \mathrm{CE}(O_2, Y_n). \tag{4}$$

The first channel's jamming technique and threat type for which it is optimised are denoted $J_1$ and $O_1$ respectively, with $J_2$ and $O_2$ having the same meaning for the second simultaneous jamming channel. The stage and threat type of the $n^{\text{th}}$ threat are denoted $S_n$ and $Y_n$ respectively. The interactions between the techniques are denoted $I_{1,2}$ and $I_{2,1}$, and are calculated using (8) and (9) below, whilst SE and CE are user-defined lookup tables which quantify the stage effectiveness and the cross effect, also discussed later.

The result of (3) and (4) is two jamming effects for each threat, with each representing the effect of one of the jamming channels. These jamming effects are then summed in order to obtain a total jamming effect ($E_{n,total}$).

This total jamming effect is then adjusted ($E_{n,adj}$) for the effect of path loss, and hence effectiveness, over distance. This is achieved using

$$E_{n,adj} = \begin{cases} E_{n,total} + \alpha d^2, & \text{if } E_{n,total} \geq 0 \\ E_{n,total} - \alpha d^2, & \text{if } E_{n,total} < 0 \end{cases} \tag{5}$$

where $d$ is the aerial distance of the platform from the threat (in km), and $\alpha$ is the jamming distance factor defined by

$$\alpha = \frac{1}{{R_{max}}^2} \tag{6}$$

where $R_{max}$ is the user-defined maximum jamming range of the platform in km, which is currently set to 40 km. The primary result of (5) is an increase in the absolute jamming effects as a function of range because the skin return power decreases with $d^4$, while the jammer power decreases with $d^2$, causing the JSR to increase with $d^2$.

Finally, the jamming effect is set to one if it is greater than one since a jamming technique cannot be more than one hundred percent effective, before it is multiplied by a user-defined maximum jamming effect ($E_{max}$) giving

$$E_{n,final} = E_{max} \times E_{n,adj}. \tag{7}$$

The value of $E_{max}$, currently set to 0.9, prevents a jamming technique from reducing a threat to below ten percent effectiveness.

### *4.2 Stage Effectiveness*

This factor accounts for the effectiveness of an implemented jamming technique against the radar mode (or stage) of a threat. This factor is obtained from the lookup table which appears in Table 1, where a more positive number indicates greater effectiveness against the stage, whilst a more negative number indicates greater illumination of the platform.

**Table 1** Stage effectiveness factors

| Stage | RGPO | VGPO | CP | NJ | MFT |
|---|---|---|---|---|---|
| Search | -1.0 | -1.0 | 1.0 | 0.8 | 1.0 |
| Acquisition | -1.0 | -1.0 | 1.0 | 0.9 | 1.0 |
| Tracking | 1.0 | 1.0 | -1.0 | -1.0 | 0.0 |
| Guidance | 1.0 | 1.2 | -1.0 | -1.0 | 0.0 |

Noise jamming is assumed to be optimised for greater performance in jamming the acquisition phase, but the large signal strength results in the illumination of the platform for tracking-type stages.

A cover pulse is a technique aimed at fooling a search radar’s constant false alarm rate (CFAR) detector, hence its effectiveness against these types of stages. However, as a type of noise jamming, the cover pulse can illuminate the platform to tracking-type stages.

RGPO and VGPO are techniques that are, by design, effective against tracking-type radar modes, but the strong false targets generated by these techniques illuminate the platform to threats in search-type stages. VGPO has the advantage of being able to draw guided missiles towards stationary clutter, and hence has a slightly increased effectiveness against these threats [8].

Finally, MFT is effective at overloading a search-type radar, whilst having no effect on tracking-type stages.

### *4.3. Technique Interaction*

This factor is used to account for the fact that combinations of techniques can either enhance each other’s performance, or act detrimentally. This factor is calculated as the effect of channel 2 on channel 1 using

$$I_{1,2} = 1 + \mathrm{INT}(J_1, J_2) \times \mathrm{CE}(O_1, O_2) \tag{8}$$

and similarly as the effect of channel 1 on channel 2 using

$$I_{2,1} = 1 + \mathrm{INT}(J_2, J_1) \times \mathrm{CE}(O_2, O_1). \tag{9}$$

In these equations, INT is the interaction lookup table that appears in Table 2, and CE is the cross effect lookup table that is discussed later.

**Table 2** Jamming interaction factors

| Stage | RGPO | VGPO | CP | NJ | MFT |
|---|---|---|---|---|---|
| RGPO | 0.0 | 0.2 | 0.2 | -0.3 | -0.2 |
| VGPO | 0.2 | 0.0 | 0.2 | -0.3 | -0.2 |
| CP | 0.2 | 0.2 | 0.0 | 0.0 | 0.1 |
| NJ | -0.3 | -0.3 | 0.0 | 0.0 | 0.2 |
| MFT | -0.2 | -0.2 | 0.1 | 0.2 | 0.0 |

For Table 2, a value of zero indicates no effect, a positive value indicates enhancement, and a negative value indicates detrimental interaction. It is noted, that although the table is currently symmetrical, it can be modified such that each pair of techniques can have different effects depending on which technique is being examined, and which is the interfering technique. In this case, the rows represent the technique being examined, and the columns are the interfering technique.

Noise jamming and cover pulses are set to not have an effect on one another as they utilise similar principles, with both raising the detection threshold of a CFAR detector. Noise jamming and MFT are set to enhance one another, as both are aimed at jamming a search radar. Similarly, a cover pulse is set to work well with MFT as both are aimed at fooling an automated detection system, with the effect that the cover pulse will cause the system to detect the false targets instead of the real target.

RGPO and VGPO will tend to enhance one another, as the likelihood of a tracking radar following one of the two techniques is greater than that of the tracking radar being led away by just one. Noise jamming interferes with both RGPO and VGPO in a detrimental fashion, as it both makes the platform easier to track, and reduces the likelihood that the tracking radar will detect and follow the RGPO or VGPO false target. The interaction between a cover pulse, and RGPO and VGPO is set to be a positive one because if either RGPO or VGPO are successful at breaking lock, the cover pulse will then prevent rapid redetection of the platform by search radar. Finally, RGPO and VGPO interfere with the effect of MFT by singling out which target is the real one.

### *4.4. Cross Effect*

This multiplicative factor accounts for the frequency-band usage of the radar systems of the different threat types, which are assumed to be listed in ascending frequency usage order. This factor is stored in a look-up table, where the rows represent the threat type for which the jamming is optimised, and the columns represent the current threat type being examined.

In this scenario, it is assumed that all the threats types use equally spaced, similar bandwidths such that there is only a slight overlap. The bandwidth overlap has been chosen such that if an adjacent threat type is jammed, the jamming only has 40% effectiveness against the threat type being examined, and 20% effectiveness on a threat type one bandwidth step further away giving factors of 0.4 and 0.2 respectively. The effectiveness of jamming the same threat type as the type being examined is set to 100% using a factor of 1.0, and the effect on all other types further than two bandwidths away set to 0. However, the look-up table can be configured such that some threats can have a wider bandwidth by causing jamming optimised for them to have larger effect on a greater number of neighbouring threats or vice versa.

### *4.5. Noise Jamming*

The system has five different noise jamming techniques: narrow (N), medium-narrow (MN), medium (M), medium-wide (MW) and wide (W) bandwidth (BW). This accounts for the fact that most ECM systems have a maximum power output, meaning that noise jamming can be used as a powerful narrowband technique with a strong effect on one threat type, or its power can be spread over a wider bandwidth, with less of an effect across more threat types.

Noise jamming is treated the same as other techniques, except that the cross-effect values are modified using the adjustment parameters that appear in Table 3. In this table, the central C column represents the threat for which the jamming is optimised, with the H columns to the right representing the threats adjacent in the higher frequency domain, whilst the L columns represent the threats adjacent in the lower frequency domain.

**Table 3** Noise jamming adjustment parameters

| BW | L4 | L3 | L2 | L1 | C | H1 | H2 | H3 | H4 |
|---|---|---|---|---|---|---|---|---|---|
| N | 0.0 | 0.0 | -0.2 | -0.4 | 0.0 | -0.4 | -0.2 | 0.0 | 0.0 |
| MN | 0.0 | 0.0 | -0.2 | 0.4 | -0.2 | 0.4 | -0.2 | 0.0 | 0.0 |
| M | 0.0 | 0.0 | 0.4 | 0.2 | -0.4 | 0.2 | 0.4 | 0.0 | 0.0 |
| MW | 0.0 | 0.4 | 0.2 | 0.0 | -0.6 | 0.0 | 0.2 | 0.4 | 0.0 |
| W | 0.2 | 0.2 | 0.0 | -0.2 | -0.8 | -0.2 | 0.0 | 0.2 | 0.2 |

The appropriate row is essentially superimposed over and added to the appropriate column in the cross-effect lookup table. The result of this approach is that narrowband noise jamming will have an effectiveness of 100% on one threat type, medium-narrow noise will have an effectiveness of 80% spread over three adjacent threat types, medium-band noise will have an effectiveness of 60% spread over five adjacent threat types, medium-wide noise will have an effectiveness of 40% spread over seven adjacent threat types, and wideband noise will have an effectiveness of 20% spread over nine adjacent threat types. For example, a medium-narrow noise technique aimed at threat type 4 will have 80% effectiveness against threat types 3, 4 and 5. This look-up table can be modified by the user in order to implement other noise jamming techniques and other bandwidth distributions.

### *4.6. Optimisation*

The jamming techniques implemented by each jammer channel and the threat type at which those techniques are aimed need to be determined for each engagement (time interval). The necessary optimisation is achieved using an exhaustive search that calculates the objective function values for each possible combination of jamming techniques and threats for which they can be optimised, on an engagement-by-engagement basis. While an exhaustive search is inherently inefficient, it both guarantees that the best solution is found, and demonstrates the computational efficiency of the proposed TEJA system.

The parameter to be minimised is

$$V_{total} = \sum_{n=1}^{N} V_n^p \tag{10}$$

where $N$ is the number of threats. The variable $p$ is a user-defined variable that can be used to alter optimisation performance, where a larger value prioritises larger threats and vice versa. A value of 3 has been used for $p$ as a compromise between emphasising significant threats without neglecting smaller threats.

## 5. Example Scenario

The performance of the system is best illustrated with an example scenario. The scenario used in this paper is one of an airborne platform entering adversary territory in order to engage a target (at the second waypoint) guarded by multiple types of ground-based threats. The scenario is initiated and terminated close to the target, and uses a coarse time interval in order to minimise the resulting data to allow the full results to be presented. This section of the mission, where there are a large number of threats in a small area, is the most critical and shows the ability of the system to address complex scenarios.

The layout of the threats in the mission area is shown in Fig. 2, where the first number in brackets is the threat identity (ID), and the second is the threat type. The waypoints of the platform are represented by the circles and are traversed at a constant speed from bottom to top along the solid line, where the height of the platform decreases from 14 km down to 8 km in order to engage the target, before rising back to 14 km again in order to exit the mission area. The second waypoint is set to be reached 80 s from the commencement of the mission, and the third waypoint 150 s from commencement. All threats are assumed to have zero altitude and have coordinates rounded off to the nearest kilometre. Mission waypoints are also rounded off to the nearest kilometre.

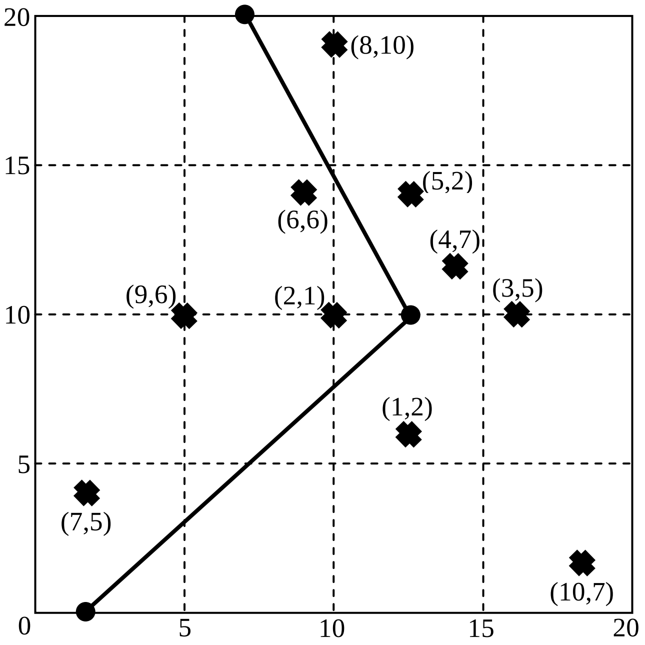

***Fig. 2.*** *Layout of threats in the mission area for the scenario (Threat ID, Threat Type), where both axes are distances in km.*

In this example, the time resolution is set to 10 s. $T_{max}$ is calculated as 0.03 hours using the rounded maximum diagonal range of 30 km and a minimum expected projectile velocity of 1000 km/h. The threats and their parameters appear in Table 4, where the search, acquisition, and tracking times have been set to 30 s, 10 s and 20 s respectively for every threat. These values have been set equal to make the results easier to follow, but could differ for each threat. Also, the projectile velocities have all been set to 2000 km/h, since any variations would result in no changes in the results at the coarse time interval used. Finally, for the weapon (W) column, guided missiles have been abbreviated M, and artillery A.

**Table 4** Scenario threats

| ID | $Y_n$ | W | Weapon Type | Acc | Range | Radar Range | Prob | Rad |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | M | Active | 0.95 | 12 km | 15 km | 0.85 | 1 |
| 2 | 1 | A | Explosive | 0.75 | 9 km | 11 km | 0.90 | 3 |
| 3 | 5 | M | Command | 0.80 | 7 km | 10 km | 0.85 | 5 |
| 4 | 7 | M | Semi | 0.90 | 8 km | 12 km | 0.95 | 2 |
| 5 | 2 | M | Active | 0.95 | 12 km | 15 km | 0.70 | 3 |
| 6 | 6 | A | Explosive | 0.70 | 8 km | 10 km | 0.80 | 1 |
| 7 | 5 | M | Command | 0.80 | 7 km | 10 km | 0.75 | 2 |
| 8 | 10 | M | Beam | 0.85 | 9 km | 12 km | 0.85 | 2 |
| 9 | 6 | A | Explosive | 0.70 | 8 km | 10 km | 0.90 | 4 |
| 10 | 7 | M | Semi | 0.90 | 8 km | 12 km | 0.70 | 1 |

Note that not all threat types (3, 4, 8 and 9) from the range 1 to 10 are included in the scenario. However, the inclusion of these threat types in the total number of 10 threat types serves two purposes. Firstly, the system works with a threat database, with not all threats being encountered in each mission, and as a result, a user would not edit this library for each scenario. Secondly, this shows the functionality of adding in extra threats to the library to create gaps in the frequency spectrum as required by the user.

Also, note that the ranges of the threat types have been chosen to create a good example in the context of the size of the mission area, rather than attempting to accurately represent real systems. Probabilities and distributions have been chosen at random, and accuracies and relative ranges have been chosen to create a combination of more dangerous threat types and less threatening ones at each time interval.

## 6. Results

The developed jamming strategy is shown in Table 5, with its effect on the radar stages of the threats over the course of the mission shown in Table 6. Importantly, the platform escapes the mission unharmed.

**Table 5** Jamming strategy

| Time | Coordinates (km) | | | Channel 1 | | Channel 2 | |
|---|---|---|---|---|---|---|---|
| (s) | x | y | z | Tech | $O_1$ | Tech | $O_2$ |
| 0 | 2.0 | 0.00 | 14.0 | MFT | 4 | NJ (M) | 4 |
| 10 | 3.4 | 1.3 | 13.3 | NJ (M) | 4 | NJ (MW) | 3 |
| 20 | 4.8 | 2.5 | 12.5 | NJ (MN) | 2 | NJ (MN) | 6 |
| 30 | 6.1 | 3.8 | 11.8 | NJ (MN) | 1 | NJ (MN) | 6 |
| 40 | 7.5 | 5.0 | 11.0 | NJ (MN) | 1 | NJ (MN) | 6 |
| 50 | 8.9 | 6.3 | 10.3 | NJ (MN) | 1 | NJ (MN) | *6* |
| 60 | 10.3 | 7.5 | 9.5 | NJ (MN) | 1 | NJ (MN) | 6 |
| 70 | 11.6 | 8.8 | 8.8 | NJ (MW) | 4 | NJ (MW) | 8 |
| 80 | 13.0 | 10.0 | 8.0 | NJ (M) | 3 | NJ (M) | 8 |
| 90 | 12.1 | 11.4 | 8.9 | RGPO | 9 | MFT | 6 |
| 100 | 11.3 | 12.9 | 9.7 | RGPO | 10 | MFT | 1 |
| 110 | 10.4 | 14.3 | 10.6 | RGPO | 2 | NJ (MN) | 6 |
| 120 | 9.6 | 15.7 | 11.4 | NJ (MN) | 1 | NJ (M) | 8 |
| 130 | 8.7 | 17.1 | 12.3 | NJ (MN) | 1 | NJ (M) | 8 |
| *140* | *7.9* | *18.6* | *13.1* | *RGPO* | *6* | *NJ (M)* | *9* |
| 150 | 7.0 | 20.0 | 14.0 | RGPO | 10 | NJ (MW) | 5 |

**Table 6** Threat radar stages

| Time (s) | Threat 1 | Threat 2 | Threat 3 | Threat 4 | Threat 5 | Threat 6 | Threat 7 | Threat 8 | Threat 9 | Threat 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | Search | Search | Search | Search | Search | Search | Search | Search | Search | Search |
| 10 | Search | Search | Search | Search | Search | Search | Search | Search | Search | Search |
| 20 | Search | Search | Search | Search | Search | Search | Search | Search | Search | Search |
| 30 | Search | Search | Search | Search | Search | Search | Search | Search | Search | Search |
| 40 | Search | Search | Search | Search | Search | Search | Search | Search | Search | Search |
| 50 | Search | Search | Search | Search | Search | Search | Acquisition | Search | Acquisition | Search |
| 60 | Acquisition | Acquisition | Search | Search | Search | Search | Search | Search | Search | Search |
| 70 | Search | Search | Acquisition | Acquisition | Search | Acquisition | Search | Search | Search | Search |
| 80 | Search | Search | Search | Search | Acquisition | Search | Search | Acquisition | Search | Acquisition |
| 90 | Search | Search | Search | Search | Tracking | Search | Search | Tracking | Acquisition | Tracking |
| 100 | Acquisition | Acquisition | Search | Search | Tracking | Search | Search | Tracking | Search | Search |
| 110 | Tracking | Search | Acquisition | Acquisition | Guidance | Search | Search | Search | Search | Search |
| 120 | Search | Search | Search | Search | Search | Search | Search | Search | Search | Search |
| 130 | Search | Search | Search | Search | Search | Acquisition | Search | Search | Acquisition | Search |
| *140* | *Search* | *Acquisition* | *Search* | *Search* | *Search* | *Tracking* | *Search* | *Acquisition* | *Tracking* | *Search* |
| 150 | Search | Tracking | Search | Acquisition | Acquisition | Search | Search | Tracking | Search | Search |

It is seen that the system initially attempts to keep all the threats in a search stage by using a combination of multiple frequencies and bandwidths of noise jamming, and multiple false targets. However, once threats start entering acquisition and tracking stages, the system moves towards a combination approach that utilises range-gate pull off to tackle the tracking-stage threats, whilst using noise jamming and multiple false targets in a different part of the frequency spectrum to ward off search-stage threats.

A good example of the interaction between the two jamming channels appears in the fifteenth time interval that occurs between 140 and 150 s after the commencement of the mission. The danger values during this time interval appear in Table 7. It is seen from these values that most of the threats, which are in search-type stages, have relatively similar danger values, where threat 6 of type 6 is clearly the largest danger to the platform and hence should be prioritised.

**Table 7** Values for the fifteenth time interval

| Threat ID | Danger Value | Jamming Factor | Post-Jamming Danger Value |
|---|---|---|---|
| 1 | 3.4177 | 1.0000 | 3.4177 |
| 2 | 4.9085 | 1.0000 | 4.9085 |
| 3 | 0.7762 | 1.5358 | 1.1922 |
| 4 | 4.5471 | 0.7853 | 3.5709 |
| 5 | 3.3998 | 1.0000 | 3.3998 |
| 6 | 5.9056 | 0.1000 | 0.5906 |
| 7 | 0.0000 | 1.5959 | 0.0000 |
| 8 | 5.4144 | 0.4142 | 2.2424 |
| 9 | 3.9295 | 0.1000 | 0.3930 |
| 10 | 0.0000 | 0.6185 | 0.0000 |
| Total | 32.2989 | n/a | 19.7150 |

A combination of range-gate pull off optimised for a threat of type 6 and medium-bandwidth noise jamming optimised for a threat of type 9 is used.  This combination of techniques is seen to dramatically reduce the danger value of threats 6, 8 and 9, whilst having an illuminating effect on threats 3 and 7. However, the effect of this illumination is acceptable due the fact that the platform is out of range for threat 7, and threat 3 poses minimal danger in the time interval being examined. As a result, the total post-jamming danger value has been substantially reduced.  This ability to assess such interactions between threats and jamming is one of the key benefits of the proposed TEJA system.

For threat 6 in this time interval, the stage value is 0.75, due it being in the tracking stage, and its accuracy danger value of 0.5920 is calculated from

$$R_6 = \frac{T_{6,Ground\ Distance}}{T_{6,Range}} = \frac{\sqrt{1.1^2+4.6^2}}{8} = 0.5912 \qquad (11)$$

$$A_6 = \frac{T_{6,Accuracy}}{2\times R_6} = \frac{0.7}{2\times 0.5912} = 0.5920 \qquad (12)$$

as the target range is more than half the threat's maximum range. The projectile time to platform value is 0.2321, as calculated from

$$T_6 = \frac{1}{T_{max}} \times \frac{T_{6,Air\ Distance}}{T_{6,Velocity}} = \frac{\sqrt{1.1^2+4.6^2+13.1^2}}{0.03\times 2000} = 0.2321. \qquad (13)$$

The probability of threat encounter is 0.8, due to the platform being within range of the entire area of likely encounter of the threat. Finally, the time-to-next-stage danger value is 0.333 due to fact that the platform will have 10 s remaining in the tracking stage by the end of the time interval out of an allocated maximum of 30 s.

Next, the jamming factor for this sixth threat is calculated as the total effect of both channels using (2) to (9). Examining channel 1, the interaction due to the use of noise jamming in channel 2 is calculated using (8) and Table 2 as a factor of 1.0, due to the fact that the second channel is operating far enough away in the frequency spectrum. The jamming effect of channel 1 is then calculated using (3) and Table 1, along with the appropriate cross effect value, as 1.0. Similarly, the jamming effect of channel 2 is calculated as zero. Again, this is due to the fact that the second channel is operating sufficiently far away in the frequency spectrum. The final jamming factor for this threat is then calculated as 0.1000 after the jamming value has been adjusted for distance, and the maximum jamming effect. Since this jamming factor is below the break-lock threshold of 0.3, the tracking lock of threat 6 is broken, and it returns to the beginning of the search stage in the next time interval.

The jamming factor for threat 4 of type 7 shows the effect of interaction to an even greater extent than for threat 6. The interaction factor remains as 1.0, but the jamming effect due to channel 1 (RGPO) is calculated as -0.4 due to the stage effect of -1, and the cross effect of 0.4 due to the technique being aimed at an adjacent threat in the frequency domain. The jamming effect due to channel 2 (NJ) is calculated as 0.48 when the CE value in (4) has been appropriately modified using Table 3, with the sum of the effect of the two channels being equal to 0.08. After adjusting for distance and the maximum jamming effect in (5) and (7) respectively, the jamming factor for threat 4 is calculated as 0.7853.

## 7. Conclusion

A threat evaluation and jamming allocation (TEJA) system was proposed and implemented. This system overcomes the limitations of previously-proposed TEJA systems by considering a number of issues which are inherent in jamming systems.

The first improvement is that the varying effects of different jamming techniques on different threats and radar modes were considered. Arguably the most significant improvement is the ability to model the interaction between the jamming techniques used by multiple jammer channels as such interactions are inherent in systems operating in the EMS. The effects of frequency and bandwidth were also considered, thereby allowing a variety of noise-jamming techniques to be considered, for example. The uncertainty of the threat environment was yet another factor accounted for in order to more accurately represent real-world systems. Finally, the progression of a threat through various radar modes was modelled, thereby allowing the future effects of the current jamming strategy to be considered.

A test problem with a large number of complex interacting threats was considered. The ability of the proposed TEJA system to successfully consider the issues highlighted above was demonstrated. Additionally, use of an exhaustive search was possible despite the complexity of the problem, thereby demonstrating the computational efficiency of the proposed system. Importantly, the final jamming strategy was able to ensure that the platform survived the mission.

## 8. Acknowledgements

The authors would like gratefully acknowledge the contribution of J.C. Mocke of the Radar and EW Competency Area at the Council for Scientific and Industrial Research (CSIR) in Pretoria to an earlier TEJA system which highlighted the need for many of the capabilities described above.

This work is based on the research supported in part by the National Research Foundation of South Africa (NRF) (Grant specific unique reference number (UID) 85845). The NRF Grantholder acknowledges that opinions, findings and conclusions or recommendations exressed in any publication generated by the NRF supported research are that of the author(s), and that the NRF accepts no liability whatsoever in this regard.

## 9. References

[1] Johansson, F., G Falkman, G.: 'Performance Evaluation of TEWA Systems for Improved Decision Support', in Torra, V., Narukawa, Y., Inuiguchi, M. (Ed.): 'Modeling Decisions for Artificial

Intelligence' (Springer-Verlag, Berlin, 2009), pp. 205-216

[2] Karasakal, O.: 'Air Defense Missile-Target Allocation Models for a Naval Task Group', Computers and Operations Research, 2008, 35, (6), pp. 1759-1770

[3] Noh, S., Jeong, U.: 'Intelligent Command and Control Agent in Electronic Warfare Settings', International Journal of Intelligent Systems, 2010, 25, (6), pp. 514-528

[4] Zhai X., Zhuang, Y.: 'IIGA Based Algorithm for Cooperative Jamming Resource Allocation'. Asia Pacific Conf. Postgraduate Research in Microelectronics and Electronics, Shanghai, China, 2009, pp. 368-371

[5] Lv, M., Liu, D., Jiang, N., Chen, Q.: 'Radar Jamming Resources Assignment Algorithm for EW Real-time Decision Support System of Multi-Platforms'. Int. Conf. Intelligent Control and Information Processing, Dalian, China, 2010, pp. 83-96

[6] Wei, P., Ziming, S., Lin, M.: 'Research on Force Assignment for Ground-to-Air Radar Jamming System based on Chaos Genetic Algorithms'. 27th Chinese Control and Decision Conf., Qingdao, China, 2015, pp. 1215-1220

[7] Kang, S., Park, H., Noh, S., *et al.:* 'Autonomously Deciding Countermeasures Against Threats in Electronic Warfare Settings'. Int. Conf. Complex, Intelligent and Software Intensive Systems, Fukuoka, Japan, 2009, pp. 177-184

[8] Neri, F.: 'Introduction to Electronic Defense Systems' (SciTech Publishing, Raleigh, 2006, 2nd edn.)

[9] De Martino, A.: 'Introduction to Modern EW Systems' (Artech House, Boston, 2012, 1st edn.)

[10] Lothes, R., Szymanski, M., Wiley, R.: 'Radar Vulnerability to Jamming' (Artech House, Boston, 1990)

[11] Arora, J.: 'Introduction to Optimum Design' (Academic Press, Waltham, 2012, 3rd edn.)