Threat Evaluation and Jamming Allocation

N. R. Osner and W. P. du Plessis

Email: nicholasosner@gmail.com and wduplessis@ieee.org

Introduction

Threat evaluation and jamming allocation (TEJA) is the process of analysing the adversary threats currently engaging a platform, allocating each a threat level and applying jamming techniques accordingly. A system was developed that optimises the jamming response of a platform over the course of a mission using TEJA. This is aimed at maximising the platform's probability of survival over the mission. Further, this information can be used to determine the optimal passive-countermeasure cartridge load-out of a platform prior to the commencement of a mission.

System Overview

A user sets up a mission for optimisation by entering platform waypoints, as well as the locations and characteristics of adversary threats. For flexibility the threats can be customised using a number of characteristics:

- weapon type and accuracy,
- weapon range,
- radar range and relative frequency band usage, and
- average search, acquisition and tracking times.

The locations of threats are specified by a central location (in 3D coordinates), a radius of likely encounter and a probability of occurrence. This allows for a realistic correlation to intelligence information as threats are not guaranteed and their location is not precise. This also reduces the need for artificial intelligence in each threat as all threats are assumed to be restricted to their allocated areas of likely encounter.

This user customisation ability extends to the interactions between different jamming techniques across different jamming channels, as well as interactions with the different radar stages of threats. This, along with the other variables, allows the system to be modified for use with any platform and against any adversary threats. The currently-implemented jamming techniques include range- and velocity-gate pull off, cover pulses, multiple false targets, noise jamming, a towed decoy, distraction chaff, dilution chaff and flares.

The system operates by dividing an entire mission into discrete, variable time intervals (engagements), where each is handled individually. First, danger values are calculated for each encountered threat for prioritisation purposes. Next, the effect of the jamming strategy in that time interval is calculated, on a threat-by-threat basis, as a multiplicative factor called the jamming factor. The post-jamming danger values for each threat are then summed to determine a total post-jamming danger value for the time interval. These are then totalled over the entire mission along with other important effectiveness measures such as the number of cartridges used and the number of jamming techniques used. These are then weighted and summed to create a fitness function that allows a user to vary the prioritisation between safety, cost, and stealth in the jamming strategy optimisation process. Optimisation is then performed using a genetic algorithm.

Danger Value and Jamming Factor

Danger values are used to prioritise threats according to the level of threat posed by each at a specific time interval. This value is a weighted sum of various factors, where the weights are user-defined to allow for prioritisation of different factors. The factors used in the calculation of the danger value are the

- probability of encountering the threat,
- radar stage of the threat (e.g. search, track and guidance),
- range adjusted threat accuracy,
- potential time to impact of projectile, and
- time to next radar stage.

A jamming factor is used to account for the effect of jamming on a threat's danger value. It is a multiplicative factor calculated for each threat in the encounter and is dependent on user-defined look-up tables for flexibility. It takes into account

- interference between different jamming channels,
- reduction of jamming signal power over distance,
- effectiveness of implemented technique against threat radar stage, and
- effect of frequency bands jammed and used by the threat.

Example Scenario

Operation of the system is shown with a scenario consisting of 16 RF and 5 IR threats as depicted in Figure 1 below. The scenario represents a single airborne platform entering adversary territory along 3 waypoints in order to engage a target at the 2nd waypoint, which is surrounded by a large number of threats.

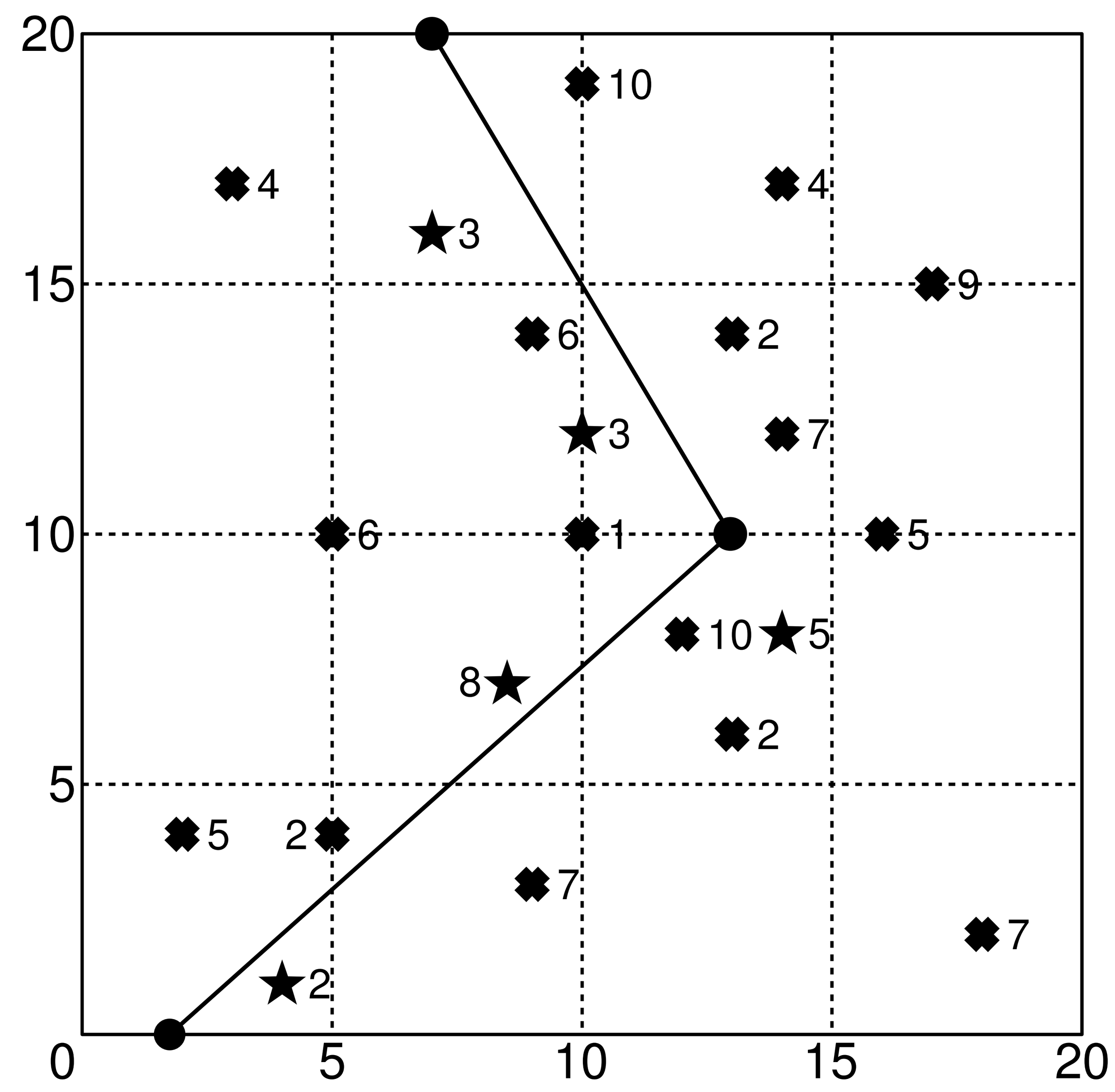

Figure 1. The example scenario. Distances are shown in km. Crosses represent RF threats, stars represent IR threats, and their associated numbers are their threat-type numbers in the threat library.

An extract of the optimum jamming strategy for the period from 30 s to 70 s from the commencement of the mission appears in Table 1 for a platform with two active jamming channels, a cartridge dispenser, and a towed decoy. This time segment covers the approach to the target and shows the format of the output: a time-based jamming strategy determined prior to the mission.

Table 1: An extract of the determined optimal jamming strategy.

Time	Active Channel 1		Active Channel 2		Passive Channel 1		Decoy Channel
	Tech	Threat	Tech	Threat	Tech	Threat	
30	NJ (M)	6	NJ (M)	4	None	N/a	None
40	CP	1	MFT	4	Flare	3	None
50	CP	6	RGPO	10	Flare	2	1
60	VGPO	10	MFT	7	Flare	8	None
70	VGPO	2	RGPO	1	Dilution	7	None

Conclusion

The performance of this system is demonstrated by the fact that safe passage cannot be found for this scenario using a human-emulating seeding method that first allocates flares, before allocating jamming to the two most imminent threats, with chaff allocated to relatively large threats thereafter. Instead, optimisation is required for the platform to just survive the mission, let alone optimise and balance mission cost, stealth and safety.