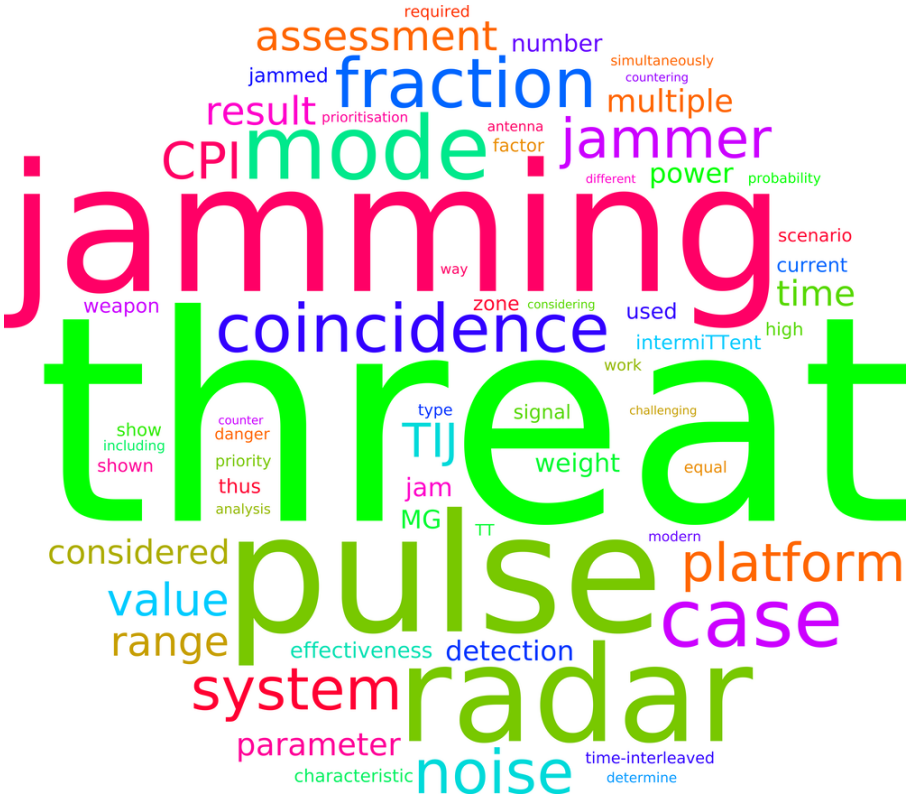
Submitted version of: Gert Claassen and Warren P. du Plessis, “Time-Interleaved Noise Jamming,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 3, pp. 3359-3367, Jun. 2023. Published version is available online at: http://ieeexplore.ieee.org/document/9969907



ABBREVIATIONS

AI	artificial intelligence
ANN	artificial neural network
AOA	angle-of-arrival
CPI	coherent processing interval
CSIR	Council for Scientific and Industrial Research
EIRP	effective isotropic radiated power
EMS	electromagnetic spectrum
ES	electronic support
EW	electronic warfare
IADS	integrated air-defence system
IEEE	Institute of Electrical and Electronics Engineers
LEDS	Land Electronic Defense System
MG	missile guidance
NF	noise figure
PRI	pulse repetition interval
RCS	radar cross section
RWR	radar warning receiver
SIGE	Defense Operational Applications Symposium
SNR	signal-to-noise ratio
TA	target acquisition
TIJ	time-interleaved jamming
TS	target search
TT	target tracking

Time-Interleaved Noise Jamming

GERT CLAASSEN
WARREN P. DU PLESSIS, Senior Member, IEEE
University of Pretoria, Pretoria, South Africa

***Abstract*—Modern jamming systems are faced with the reality that multiple threat radars will be encountered simultaneously, and potentially, all simultaneously-encountered threat radars will need to be countered to prevent detection. Modern jammer systems are capable of extremely rapid reconfiguration, allowing them to counter multiple simultaneous threats in a time-interleaved manner. However, simultaneously-encountered threats cause jamming pulses to coincide in time, leading to the problem of deciding which of the threats to jam when such coincidences occur. An approach to determining the relative priority of jammer pulses is proposed and evaluated to show that time-interleaved jamming is a viable approach to effectively countering multiple simultaneous threats.**

***Index Terms*—Time-interleaved jamming (TIJ), noise jamming, threat evaluation, electronic countermeasures, radar countermeasures, and electronic warfare (EW).**

I. Introduction

In modern war zones, multitudes of threat radars are likely to be located close enough to a platform to pose a threat. Such a high-density threat environment creates a congested electromagnetic spectrum (EMS) domain impeding the efficiency and effectiveness of a jammer. The result is an EMS environment that is difficult to safely manoeuvre in [1], [2].

Such dense environments pose difficulties for both noise and deception jamming, with the effectiveness of noise jamming being further limited by the extensive filtering used to reduce the effects of noise in modern radar systems, including pulse compression and Doppler processing [3], [4]. While the advent of modern phased-array jammers has increased the effective isotropic radiated power (EIRP) available to a jammer [3], [4], this EIRP is still limited. The power that can be allocated to each threat radar thus decreases as the number of threats that are encountered increases. Ultimately, the point is reached where the power allocated to each threat is too low to effectively counter all threats simultaneously.

Manuscript received 17 February 2022; revised 30 September 2022; accepted 23 November 2023.

Gert Claassen (e-mail: gertclaassen@outlook.com) and Warren P. du Plessis (e-mail: wduplessis@ieee.org) are with the Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria, 0002, South Africa.

Digital Object Identifier XX.XXXX/XXXX.XXXX.XXXXXXX

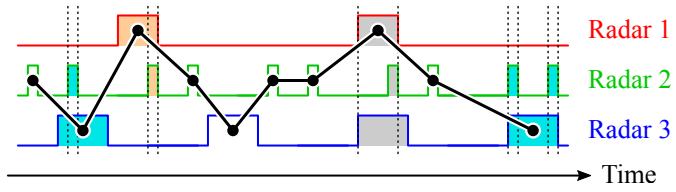


Fig. 1. Example of jamming coincidence and TIJ. The shaded pulses are in coincidence as shown by the vertical lines, and the line with dots indicates the pulses that are jammed by TIJ.

A number of approaches to countering multiple threats in dense environments have been proposed, including frequency-division multiplexing, multichannel jamming, distributed jamming networks, and power-managed jamming [5]–[9]. However, even separating threat radars according to frequency and angle-of-arrival (AOA), and having multiple jammers and/or jammer channels available, it is expected that threat radar signals will still occur simultaneously [10]. None of these approaches is thus able to address the fundamental problem of needing to simultaneously counter multiple threat radars.

A further benefit of modern phased-array jammers that does not appear to have been fully exploited is that modern jammers are increasingly able to rapidly reconfigure themselves [3], a trend that is likely to accelerate as adaptive and cognitive technologies are adopted in electronic warfare (EW) [2]. Additionally, most threat radars utilise pulsed waveforms [3], [4], so it is not necessary to jam these threats continuously. These observations raise the possibility of countering multiple threats in a time-interleaved manner. In this way, greater power – potentially the full jammer power – can be allocated to each of a number of threat radars in turn, thereby reducing the negative effects of having to simultaneously counter multiple threat radars.

However, the transmissions from multiple threat radars will still coincide periodically as shown in Fig. 1 [11], [12], and the major challenge to successfully implementing time-interleaved noise jamming will be addressing such coincidences. Time-interleaved jamming (TIJ) will thus require some means to determine when the threat radars will transmit, and importantly, when their transmissions will coincide. This will either require a pulse repetition interval (PRI) tracker, prior knowledge of the characteristics of the threat-radar waveforms, or more likely, a combination of the two. This information can then be used to select which of the threats to jam at each instant of time in order to effectively counter all threat radars.

Apart from research analysing the effects of pulse coincidence on electronic support (ES) systems [11], [12], the authors are not aware of research considering how to address coincidences in noise TIJ.

A technique to control a noise jammer that can only jam a single threat radar at a time is proposed. This technique selects which threat radar to jam at each time instant based on an estimate of the overall effectiveness of noise TIJ and the danger posed by the threat. This jamming effectiveness

will depend on the intermittent nature of the noise jamming as the jammer is not able to jam every pulse from all threat radars. A simulated scenario is presented to demonstrate the effectiveness of intermittent noise jamming under challenging conditions.

II. METHODS

TIJ interleaves between the active threat-radar jamming profiles in the time domain which permits time-sharing through the use of jamming prioritisation and intermittent jamming. Fig. 1 provides an example where an analysis is performed for every pulse in a coincidence, and the resulting priorities are used to select the radar pulse that will be jammed.

Each coincidence will have pulses that are of lower priority and will therefore be disregarded. The disregarded pulses are the reason jamming is intermittent over the coherent processing intervals (CPIs) of the threats. Impeding detection through intermittent jamming can only be achieved when jamming effectiveness is assured even when some pulses in a CPI are unjammed. Jamming effectiveness is the ability to reach a minimum probability of detection through jamming, which is far lower than the probability of detection, P_d, required by the threat radar to detect the platform in a CPI. However, jamming effectiveness can only be obtained if the minimum number of jamming pulses, n_j, that is capable of suppressing the signal-to-noise ratio (SNR) of a coherent radar is lower than the CPI of n_p pulses.

Determining the jamming prioritisation requires the calculation of the SNR, $D_x(n_p)$, of a coherent radar where intermittent noise jamming, T_{ij}, is present using [13]

$$D_x(n_p) = n_p \frac{(P_t\tau)G_tG_r\lambda^2\sigma F_t^2F_r^2}{(4\pi)^3R_{P_d}^4k(T_s+T_{ij})L} \tag{1}$$

where P_t is peak signal power, τ is the radar signal's pulse width, G_t is the transmitter antenna gain, G_r is the receiver antenna gain, λ is the radar pulse wavelength, σ is the platform's maximum radar cross section (RCS) (a conservative value), F_t is the pattern-propagation factor for the target-to-transmitting-antenna path, F_r is the pattern-propagation factor for the target-to-receiving-antenna path, R_{P_d} is the maximum range depending on the signal detection value of P_d, L is the product of losses along the transmitter-receiver path, k is Boltzmann's constant equal to 1.380×10^{-23} W/Hz, and T_s is the overall noise temperature [13].

The intermittent noise jamming temperature, T_{ij}, is calculated as [13]

$$T_{ij} = \frac{Q_jP_jG_jG_r\lambda^2F_{pj}^2F_j^2F_r^2}{(4\pi)^2R_c^2kB_jL_j} \tag{2}$$

where Q_j is the noise jamming quality factor (described below), P_j is the average intermittent jamming power over the CPI, G_j is the jammer antenna gain, F_{pj} is the jammer to radar polarization factor, F_j is the jammer to radar pattern propagation factor, R_c the current range measured, B_j is the noise bandwidth, and L_j is the product of losses along the jammer-radar receiver path.

The noise jamming quality factor, Q_j, depends on the effectiveness of the jamming waveform in inhibiting the signal and degrading radar detection relative to white Gaussian noise. However, it is quite difficult to replicate true white Gaussian noise (which requires the peak power rating to exceed the average jamming power, P_j, by 7 to 10 dB [13]) as the amplifier is normally operating in a saturated mode causing clipping of the high amplitude signals. Thus the noise quality factor uses typical values ranging from –5 dB to –2 dB to express its capability to transmit Gaussian noise signals [1], [13].

The emission of the jammer in the radar equation is seen as a series of pulses overlapping the return signal. Each of these noise jamming pulses has an amplitude and phase that is unrelated to each other. The noise signal power, P_j, is measured as the sum transmitted noise power of the n_s jamming pulses averaged over the CPI of size n_p [14]

$$P_j = \frac{1}{n_p}\sum_{i=1}^{n_p} P_{ji}. \tag{3}$$

where P_{ji} is the power of the single jamming pulse i. If the noise jamming is ineffective for any reason (e.g. the bandwidth does not match the radar signal bandwidth or the jamming pulse is not concentrated on the signal pulse), the average jamming power will decrease by P_{j1}/n_p. The noise average will decrease as additional pulses are missed.

The minimum required probability of detection, P_d, of the threat radar due to interference can then be calculated using the Marcum Q-function [15]

$$P_d = Q_1\left(\sqrt{2D_x(n)}, \sqrt{-2\ln(P_{fa})}\right), \tag{4}$$

where P_{fa} is the predefined probability of false alarm.

The TIJ system will have no indication when a CPI starts if the radar waveform characteristics of the previous and sequential CPIs remain the same over a dwell. Exact knowledge of when the first pulse of the CPI has been transmitted is only possible if the ES detects a change of waveform characteristics of a pulse or receives the first pulses from a dwell. Otherwise, even the ES system will have no indication of when a CPI started. The TIJ system cannot assume that a particular pulse may be the start of the new CPI as this will cause an error in the calculation of the number of pulses that have been jammed over the real duration of the CPI, n_s.

In order to overcome this limitation, the TIJ system has to assume that every single threat pulse is the last pulse of a CPI. In this way, it is possible to determine if the current threat pulse should jammed or not based on calculations over the previous n_p-1 pulses. This process is known as backward CPI analysis. Backward CPI analysis indicates the necessity to jam the current threat pulse in a coincidence. The benefit of backward analysis is that it allows the repercussion of selection or rejection to affect the sequential pulses until n_p+1 pulses have passed as Fig. 2 shows.

Only the jamming pulses in the coincidence where the relevant minimum required number of jamming pulses, n_j,

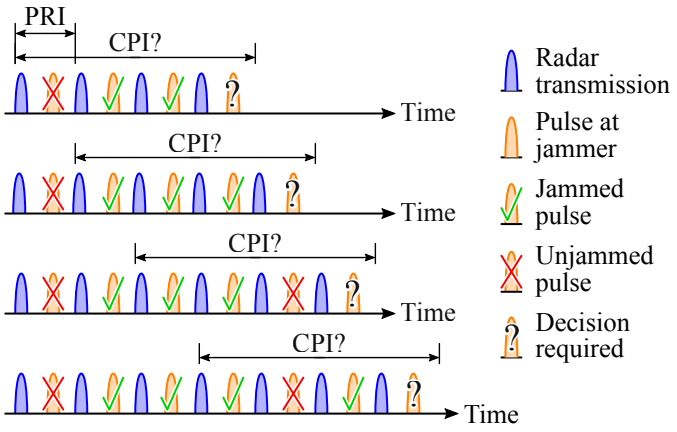


Fig. 2. An example of backward CPI analysis where a minimum of three of the four pulses in a CPI need to be jammed.

have not been transmitted will be analysed further to measure each one's priority. Prioritisation is determined by monitoring the changes of a threat radar's behaviour.

III. Threat Prioritisation and Jamming Pulse Selection

Behavioural observation is performed by analysing the change of signals transmitted by a threat radar system to determine its impact on the platform thereby creating a negative feedback loop. Without the threat assessment, the TIJ system will not be able to keep up to date with each active threat's changes in behaviour, thus blinding the TIJ system to any detrimental actions of the threats and preventing it from making proactive decisions [16].

Smart jammers on airborne platforms employ smart jamming where the threat radar's location, type, operation mode, and signal characteristics are collected and monitored. The jammer then selects the most dangerous threat at that moment. The threat radar's current mode of operation is a key indicator of the danger that the radar poses to the platform currently or can pose in the near future [1]. Multiple types of threat assessment algorithms exist, from data fusion [16]–[18], statistical and Bayesian techniques [19]–[21], to decision analysis and analytic based hierarchy approaches, and more recently, the use of advanced artificial intelligence (AI) techniques (knowledge-based systems, fuzzy logic, artificial neural network (ANN), and genetic algorithms) [21].

The result of threat assessment (the danger value) is an indicator of the risk that a threat radar system poses to the platform. Alongside the mode of operation, factors with which the platform can quantify the danger level include the platform's distance to the threat, the platform's location within the range of the threat's weapon system, and the jamming pulses still outstanding to complete the transmission of minimum required number jamming pulses in a CPI, n_j. The threat danger values need to be computed rapidly, so the approach used here is closely related to a computationally simple threat assessment algorithm where a weighted sum of the relevant parameters was used [16]. The above factors are weighted and linearly combined to produce the threat assessment equation

$$A_i = W_s S_i + W_z Z_i + W_l R_i + W_j J_i \tag{5}$$

where A_i is the threat assessment value of threat i, S_i is the radar mode, Z_i is the zone assessment value, R_i is the weapon-range indicator flag, J_i is the CPI jamming fraction, and W_s, W_z, W_l and W_j are the weights of these parameters. The threat assessment in (5) will require input from an expert to determine the values of these weights.

The threat's behaviour observed by the jammer will be primarily on the basis of changes in radar mode. The radar mode parameter S_i will be given a constant value between 0 and 1 to indicate the lethality of each mode against the platform. The conventional modes of operation that a threat radar may employ are target search (TS), target acquisition (TA), target tracking (TT), and missile guidance (MG), (fire control).

The shorter the distance between the platform and the threat, the higher the power of the radar return to the threat will be. This will result in an increased probability of detection, which in turn will mean that more jamming pulses will required required to sufficiently decrease the SNR. Therefore the zone assessment value will indicate where the platform is relative to the threat's radar detection range. The maximum detectable range and burn-through range provide a zone in which a jammer can protect the platform it is mounted on. The zone assessment value, Z_i, is thus defined as

$$Z_i = \begin{cases} 1, & \text{if } R_c < R_B, \\ Z_i = \dfrac{R_m - R_c}{R_m - R_B}, & \text{if } R_B \leq R_c \leq R_m, \\ 0, & \text{if } R_c > R_m, \end{cases} \tag{6}$$

where R_c is the current platform to threat range is denoted, R_m is the threat radar's maximum detection range when no jamming is present, and R_b is the burn-through range when all of the jammer resources are allocated to the threat. As the radar modes in a threat system change, so do the ranges due to the mode-specific SNR, the probabilities of detection and false alarm, and the waveform characteristics. Each radar mode will produce a new set of maximum and burn-through range ranges [22], and this will immediately change the zone assessment value of the threat system.

The jamming fraction, J_i, considers the previous $n_p - 1$ pulses (i.e. the current assumed CPI without the pulse for which a decision is required in Fig. 2) and is defined as

$$J_i = \begin{cases} 0, & \text{if } n_s > n_j, \\ \dfrac{n_j - n_s}{n_u + 1}, & \text{otherwise}, \end{cases} \tag{7}$$

where n_s is the number of threat pulses that have been jammed and n_u is the number of unjammed pulses. This analysis effectively assumes that the current threat radar pulse for which a decision is required will not be jammed to quantify the effect of deciding not to jam this pulse.

The jamming fraction will increase as the number of threat

TABLE I
THREAT SIMULATION PARAMETERS

Threat Type	Weapon Range (km)	Peak Power (kW)	Antenna Gain (dBi)	Frequency (GHz)	CPI (pulses)	TS PRI (μs)	TS Pulse Width (μs)	TA PRI (μs)	TA Pulse Width (μs)	TT PRI (μs)	TT Pulse Width (μs)	MG PRI (μs)	MG Pulse Width (μs)
1	25	47	15	6.4	64	32	3.2	32	4.1	30	3.6	28	2.9
2	50	25	30	9.0	128	503	0.3	533	0.3	573	0.3	593	0.3
3	75	7	28	8.8	128	65	15.0	58	12.0	50	10.0	42	7.0
4	100	100	15	8.0	128	1 073	49.0	689	49.0	345	25.0	1 074	30.0
5	125	42	25	3.0	128	1 013	12.5	1 413	12.5	20	0.9	12	0.2

radar pulses that are not jammed increases, thereby influencing the threat assessment to provide a high priority value and to increase the possibility of being selected even if the other parameters are low. This will prevent the TIJ system from ignoring lower mode threats when in coincidence with threats of higher lethality modes.

Note that the jamming fraction is dependent on the minimum number of pulses that need to be jammed, n_j, which in turn, is determined by the radar and noise jamming equations as they influence the radar or jammer performance. As a result, the jamming fraction, J_i, is dependent on all parameters of the radar-jammer engagement.

A platform being within the striking distance of the threat radar's accompanying weapon system is of high concern. Every precaution must be taken to prevent the threat radar from reaching the more dangerous modes, like MG or even TT, as lock-on is difficult to break against threats employing advanced signal processing and tracking filters. It does not matter if the weapon system is active or not, only that the platform is traversing in a very dangerous area. The weapon-range indicator flag, R_i, will result in the threat evaluation value changing as the platform moves into or out of the weapon range.

As stated, the priority of each threat radar pulse in a coincidence is calculated using (5). The radar pulse with the highest threat assessment priority value is selected to be jammed. If there are pulses that do not overlap the highest-priority pulse, these non-overlapping pulses will then be compared, with the highest-priority non-overlapping pulse being selected. All the pulses that overlap the current highest priority non-overlapping pulse are then disregarded, after which the cycle will repeat until all of the non-overlapping pulses have been compared and the highest non-overlapping pulses selected.

IV. SIMULATION

The TIJ system was tested by simulating a scenario where an airborne platform navigates through an area with a number of threat radars scattered throughout.

The simulator executes TIJ in one-second intervals to determine the jamming effectiveness after each interval. At the end of each interval, the simulator will calculate the total CPIs for each threat radar where the probability of detection was high enough for the platform to be detected. The platform

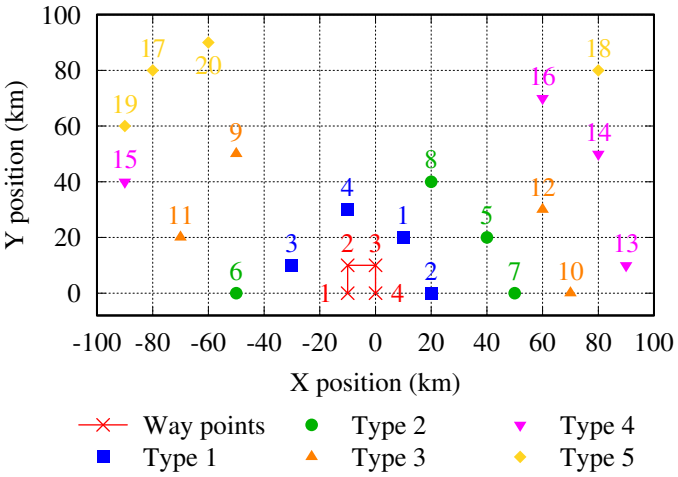


Fig. 3. The positions of the threats and the flight path of the platform. Note that all positions are integer multiples of 10 km.

needs only to be detected by a single CPI in an interval, for the threat radar to move up to the next mode, thus requiring that the jammer successfully counter all of the CPIs for each threat in each time interval to prevent mode progression.

The simulation consists of a total of 20 threats as shown in Fig. 3, and details of each radar can be found in Table I. All threats have a noise figure (NF) of 7 dB, a false-alarm rate of $P_{fa} = 10^{-6}$, a detection probability of $P_d = 0.9$, and the desired detection probabilities after jamming are 0.5, 0.3, 0.2, and 0.1 for the TS, TA, TT, and MG modes, respectively.

As outlined above, all threat radars have TS ($S_i = 0.25$), TA ($S_i = 0.50$), TT ($S_i = 0.75$) and MG ($S_i = 1.00$) modes, with each mode having different parameters. The S_i values are incremented as the radar modes become more dangerous (closer to weapon impact), to favour threats in more lethal modes when the danger values of multiple threats are similar.

The threats in Table I were selected to have a variety of weapon ranges and to operate over a wide range of frequencies. The very short pulses of threat type 2 will test whether the system artificially favours short pulses which are less likely to be in coincidence. The high duty cycle of threat type 3 and the long pulses of threat type 4 will lead to large numbers of coincidences. The dramatic variation in parameters when threat type 5 switches from TA to TT will test the TIJ

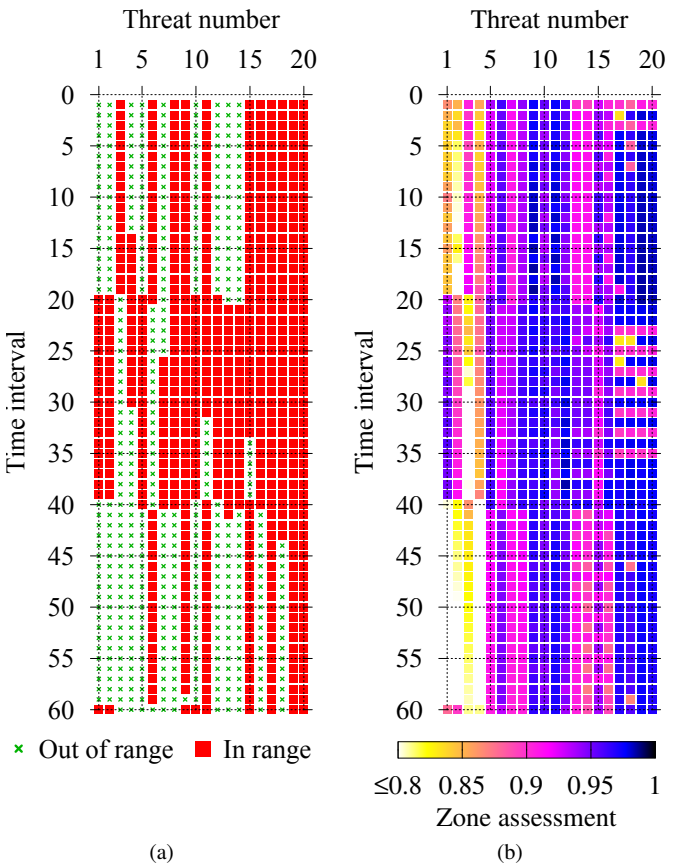


Fig. 4. Diagrams indicating (a) whether the platform is within weapon range and (b) the zone assessment value as an indication of the platform's position relative to the threat's radar range. Note that the colour axis in (b) starts at 0.8, while the full range is stretches from 0 to 1.

system's response to changes. Finally, threat type 1 has a duty cycle of around 10%, making it representative of a short-range threat.

An indication of the characteristics of this scenario is provided in Fig. 4 by considering the range of the platform from each threat at each time instant. Fig. 4(a) shows when the platform is within the weapon range of each threat, and it can be seen that different threats are relevant at different times during the engagement, with 18 of the 20 threats being within weapon range for time intervals 26 to 30. Fig. 4(b) shows that zone assessment values for all threats are high, indicating that simultaneously jamming all threats will be challenging. This combination of characteristics makes this a challenging scenario for any jammer system.

Each threat will start in the TT mode. This will make the scenario more challenging as all threats must be simultaneously jammed at the start of the scenario to avoid threats reaching the MG mode and launching weapons.

The platform travels along the flight path shown in Fig. 3, passing through the four indicated way points. The platform altitude is constant at 1 000 m, and it travels a constant 500 m/s, so it takes 60 s to travel from way point 1 to way point 4.

The platform is provided with a single noise jammer that has a maximum output power of 200 W (53 dBm) and a phased array antenna with a gain of 10 dBi. The main beam of the jammer phased array can be steered to point directly towards any of the threats, and cover noise jamming will be used [1].

It is assumed that ideal ES system is used so that the parameters of the threat signals are perfectly known. This was done to exclude ES inaccuracies from this study to emphasise the characteristics of the TIJ system. The jammer is also ideal in the sense that it will transmit the precise jamming signal at the intended time with the intended duration with the phased array main beam pointing exactly towards the peak of the main beam of the threat radar.

TABLE II
SUMMARY OF THREAT MODES

Case	TS	TT	TA	MG
1	640 (52%)	217 (18%)	185 (15%)	168 (14%)
2	828 (68%)	191 (15%)	130 (11%)	71 (6%)
3	970 (79%)	185 (15%)	57 (5%)	8 (<1%)
4	997 (82%)	191 (16%)	32 (3%)	0 (0%)

V. RESULTS

The results of the simulations described in Section IV are considered below to illustrate the potential effectiveness of TIJ.

The following four cases will be considered to explore how prioritising threats in different ways affects the outcome.

Case 1: Threat evaluation with the radar mode, zone assessment and weapon-range flag have equal weights, and the jamming fraction is ignored ($W_s = W_z = W_l = 1$ and $W_j = 0$) to serve as a baseline.

Case 2: All weights are equal ($W_s = W_z = W_l = W_j = 1$) to show the effect of the jamming fraction.

Case 3: Only the jamming fraction is considered ($W_s = W_z = W_l = 0$ and $W_j = 1$) to investigate how effective this metric alone is.

Case 4: An optimised case with $W_s = 2$, $W_z = 3$, $W_l = 0$, and $W_j = 4$.

A. Threat Modes

The way the modes of the threats vary with time is shown in Fig. 5 and is summarised in Table II.

The effect of ignoring the jamming fraction in threat prioritisation (Case 1) is shown to be surprisingly effective at countering the majority of the threats, but still allows threats to progress to the MG mode 14% of the time. Giving all the threat-evaluation parameters and the jamming fraction equal weights (Case 2) results in significant improvements with threats only reaching the MG mode 6% of the time. The importance of considering the jamming fraction is thus clearly demonstrated by the improvement from Case 1 to Case 2.

When only the jamming fraction is considered (Case 3), the results are significantly improved from Case 2, with threats only reaching MG mode only 0.66% of the time. The jamming fraction is the only one of the parameters used to determine the threat assessment in (5) that considers the characteristics of

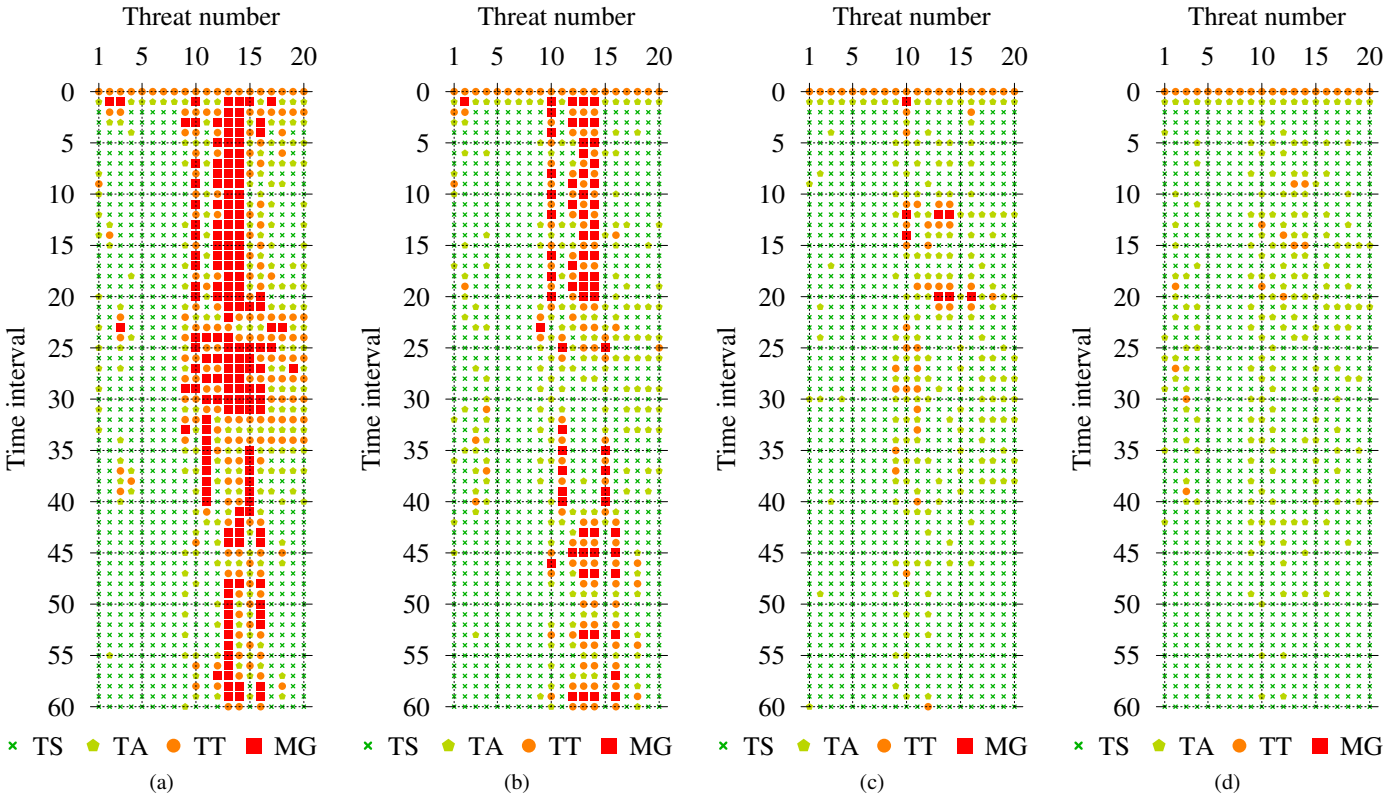


Fig. 5. The threat modes for (a) Case 1 (jamming fraction not considered), (b) Case 2 (all parameters), (c) Case 3 (only jamming fraction), and (d) Case 4 (optimised).

intermittent jamming, so this result is reasonable, if somewhat surprising. This suggests that an effective TIJ system can be constructed using only the jamming fraction as a prioritisation metric, despite the use of even the relatively simple threat-evaluation approach considered here. Additionally, the computational requirements can potentially be reduced by only considering jamming fraction for pulse prioritisation – an important issue as extremely low latencies are required for jammers to be effective [3].

The optimised result in Case 4 was obtained by exhaustively testing all possible combinations of integer values from 0 to 3 for W_s, W_z and W_l, and integer values from 3 to 9 for W_j for a total of 448 possible combinations of weights. This combination of weights allows all weights to be equal or the first three parameters to be ignored, while emphasising the jamming fraction more strongly in light of its demonstrated significance. Remarkably, there are nine combinations of weights where no threat reaches the MG mode, demonstrating that this outcome is possible. Furthermore, there 146 combinations of weights which ensure that the MG is reached fewer times than when only the jamming fraction is considered (Case 3). Considering a combination of multiple threat-prioritisation parameters is thus shown to give better results than any one parameter alone.

Despite the apparent utility of all the threat-evaluation parameters combined in (5), eight of the nine optimised cases that avoid any threat entering MG mode allocate a weight of zero to the weapon-range flag, R_i, ($W_l = 0$), and the remaining case allocates the lowest non-zero weight ($W_l = 1$). This surprising outcome is believed to be a reflection of the fact that the none of the threats reach MG mode, so whether a threat is within weapon range or not is irrelevant to these cases.

B. Coincidences

The four cases are explored further in Fig. 6, which shows the coincidence fractions for each threat over time. The coincidence fraction is the proportion of the pulses over a CPI that are in coincidence, which quantifies the challenge associated with selecting which pulse to jam. Only Cases 1 and 2 are presented as the results for Cases 3 and 4 do not display significant differences to those of Case 2.

The primary conclusion from Fig. 6 is that the vast majority of pulses are subject to collisions with the median coincidence fraction being over 99.3% in all cases. The performance of the TIJ system considered above is remarkable in light of this extremely high coincidence rate.

An interesting observation is that the coincidence fraction significantly reduces for Threats 17 to 20 over time intervals 23 to 35 in Case 1, but not in the other cases. This is a result of the significant reduction of the pulse repetition interval (PRI) and pulse width for threat type 5 on changing from TA mode to TT mode, which was noted above. Case 1 allows these threats to progress to the TT mode, while the remaining cases ensure that these threats do not progress beyond TA mode. This result shows that the TIJ system correctly priorises prevention of

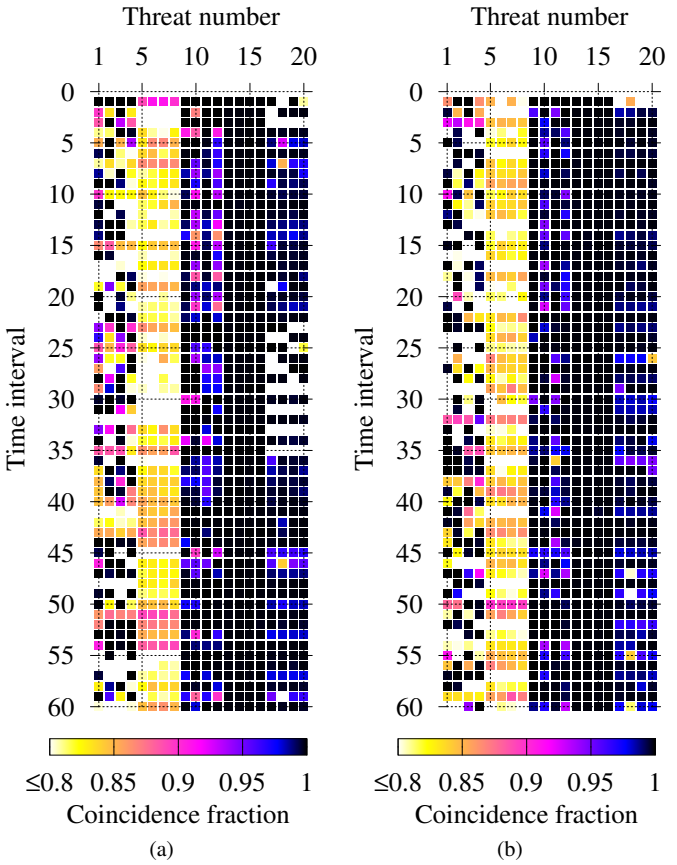


Fig. 6. The coincidence fraction for (a) Case 1 (jamming fraction not considered) and (b) Case 2 (all parameters). Note that the colour axis starts at 0.8, while values as low as 0 are possible.

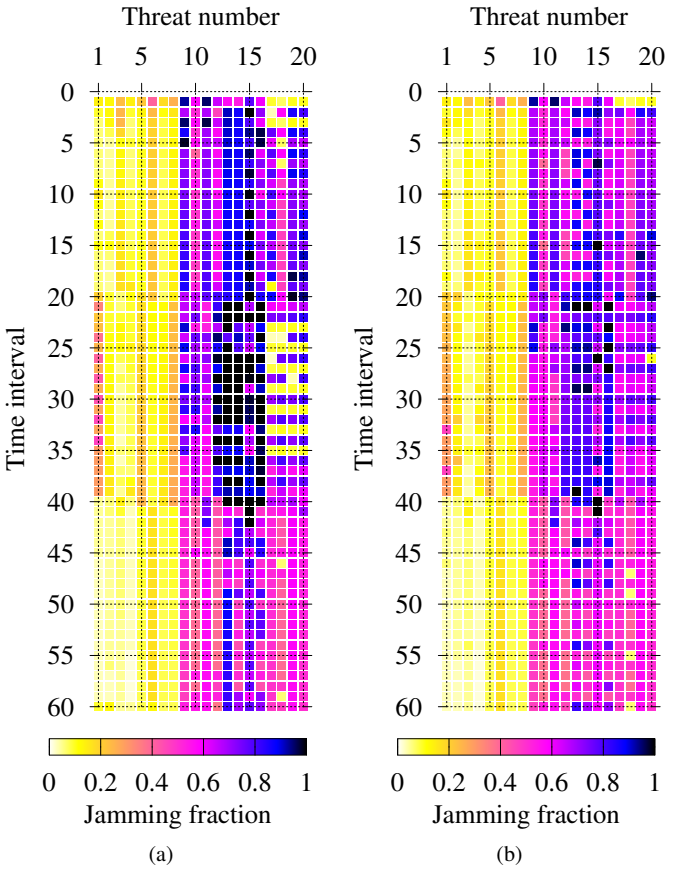


Fig. 7. The jamming fractions for (a) Case 1 (jamming fraction not considered) and (b) Case 2 (all parameters).

mode progression over allowing mode progressions that would reduce the number of coincidences.

Threats 5 to 9 show far lower coincidence fractions than the other threats in all tests as a result of the extremely low pulse width of threat type 2.

C. Jamming Fraction

The final performance metric considered is the jamming fraction, which quantifies how important it is to jam each threat radar pulse in a coincidence. This interpretation arises from the fact that all pulses that are not in coincidence are jammed as noted in Section II, so only pulses in coincidence are considered in the computation of this factor. Again, only Cases 1 and 2 are considered due to Cases 3 and 4 being similar to Case 2.

The effect of the shorter pulses of threat types 1 and 2 are clearly seen in the low jamming fractions of Threats 1 to 8 (< 0.165 in all cases) in Fig. 7. These lower jamming fractions mean that it is less important to jam pulses from these threats that are in coincidence because so many of their pulses are not in coincidence, as expected.

By comparison, the jamming fractions for the remaining threats are far higher with jamming fractions of > 0.432 in all cases. The long pulses and/or high duty cycles of these threats thus mean that larger proportions of the pulses of these threats are in coincidence, making it more important to jam such pulses. The effect of this is particularly clear in Case 1 (Fig. 7(a)), where the high jamming fractions of Threats 12 to 16 in intervals 21 to 40 can be seen to correspond to these threats regularly reaching more dangerous modes, including MG, mode over this time in Fig. 7(a).

D. Implications of Assumptions

This work assumes that the TIJ system can instantaneously switch between threats and has perfect knowledge of all threats, and that only noise jamming is used and that there is no communication between threats (i.e. this is not an integrated air-defence system (IADS)). These effects were ignored on the basis that they would add significant additional complexity to this work without comparable contributions to the conclusions. The implications of each of these assumptions are briefly considered below.

The primary effect of the jammer requiring time to switch between threats will be that the number of threats that can be countered would be reduced. This switching time can depend on a number of factors, including the frequency difference and angular separation between threats, so no attempt was made to model this complicated effect here.

Uncertainty about the precise values of threat parameters would manifest primarily as uncertainty around the time when

a given threat must be jammed. There are various ways to address this, such as jamming the entire period over which a threat-radar pulse is expected to arrive, but the development and implementation of a suitable approach are considered to be beyond the scope of this work. However, the primary effect of threat uncertainties will again be to reduce the number of threats that can be countered.

The primary motivation for only considering noise jamming is that rigorous mathematical analyses of the effect of noise jamming exist, and noise jamming remains relevant and useful. Considering other jamming techniques would have added significant additional complexity to model them, potentially obscuring the effect of TIJ. The primary effect of other jamming techniques, such as pull-off techniques, would be to change the time at which the jamming signal should be transmitted. This timing variation is likely to have a positive effect as patterns that cause threat-radar pulses to routinely coincide (e.g. PRIs that differ by an integer factor) would be reduced.

Finally, communication between threats would greatly increase the complexity of TIJ as the effect that jamming one threat would have on the others would need to be considered. The dramatic additional complexity of an IADS model and the huge implications on TIJ are considered beyond the scope of this work. The primary effect of considering an IADS would be that the danger posed by each threat would increase because failing to successfully counter any threat may lead to all threats entering more lethal modes. The importance of countering all threats would thus increase for an IADS.

Future work will investigate these effects of these assumptions, with some initial results already being available [23].

VI. Conclusion

The concept of TIJ, where a jammer rapidly switches between multiple threats, has been considered. A TIJ system is capable of countering multiple simultaneous threats, allowing it to function in dense environments where a more traditional jammer that only considers one threat at a time would be overwhelmed.

The selection of which threat radar pulse to jam in a coincidence was considered in light of the intermittent nature of the jammer with the jamming fraction being defined as a suitable metric. A challenging scenario where a median of over 99.3% of threat radar pulses are in coincidence was described, and a TIJ system was evaluated with varying threat prioritisations. While a number of assumptions were made, these assumptions mainly serve to make the results slightly optimistic and do not otherwise significantly affect the results.

The results show that even a TIJ system is capable remarkably good performance, especially in light of the challenging nature of the scenario and the simple threat-evaluation algorithm used. Usefully, the jamming fraction alone was found to produce excellent results, suggesting that this metric can be used alone without the need to resort to complicated threat-prioritisation systems. However, including multiple threat-prioritisation metrics was shown to give better results than even the jamming fraction alone.

Acknowledgement

Warren du Plessis would like to acknowledge Dr Vitorio Rossi whose presentation at Defense Operational Applications Symposium (SIGE) in 2013 first introduced him to the concept of TIJ.

References

[1] D. C. Schleher, *Introduction to electronic warfare*. Norwood, MA: Artech House, 1986.

[2] K. Haigh and J. Andrusenko, *Introduction to Electronic Defense Systems*. Norwood, MA: Artech House, 2021.

[3] F. Neri, *Introduction to Electronic Defense Systems*, 3rd ed. Norwood, MA: Artech House, 2018.

[4] A. de Martino, *Introduction to modern EW systems*, 2nd ed. Norwood, MA: Artech House Publishers, 2018.

[5] N. Ahmed and Hong Huang, "Distributed jammer network: Impact and characterization," in *IEEE Mil. Commun. Conf. (MILCOM)*, Boston, MA, 18-21 Oct. 2009, pp. 1–6.

[6] *Jane's Radar and Electronic Warfare Systems*. IHS Jane's, 2002.

[7] J. Haystead, "Cognitive/adaptive learning requirements drive continuous advancement of DRFM technology," *J. Eletron. Def. (JED)*, vol. 42, no. 11, pp. 46–56, Nov. 2019.

[8] B. Zhang and W. Zhu, "Research on decision-making system of cognitive jamming against multifunctional radar," in *IEEE Int. Conf. Signal Process Commun. Comput. (ICSPCC)*, Dalian, China, 20-22 Sep. 2019, pp. 1–6.

[9] C. Kopp. (2014, 27 Jan.) The anatomy of the Tacjammer. [Online]. Available: http://www.ausairpower.net/TE-Tacjammer.html

[10] P. Kaszerman, "Frequency of pulse coincidence given n radars of different pulsewidths and PRFs," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 7, no. 5, pp. 1013–1014, Sep. 1971.

[11] G. T. Demos and M. S. Weprin, "Probability of pulse coincidence in a multiple radar environment," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 19, no. 4, pp. 635–640, Jul. 1983.

[12] S. Stein and D. Johansen, "A statistical description of coincidences among random pulse trains," *Proc. IEEE*, vol. 46, no. 5, pp. 827–830, May 1958.

[13] D. K. Barton, Ed., *Radar Equations for Modern Radar*. Boston, MA: Artech House Inc., 2013.

[14] A. Golden, *Radar electronic warfare*. Washington, DC, USA: American Institute of Aeronautics and Astronautics, 1987.

[15] M. Richards, *Fundamental of Radar Signal Processing*, 1st ed. New York, USA: McGraw-Hill, 2005.

[16] N. R. Osner and W. P. du Plessis, "Threat evaluation and jamming allocation," *IET Radar, Sonar Navig.*, vol. 11, no. 3, pp. 459–465, Mar. 2017.

[17] E. P. Blasch, J. J. Salerno, and G. P. Tadda, "Measuring the worthiness of situation assessment," in *IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Dayton, OH, 20-22 Jul. 2011, pp. 87–94.

[18] Q. Changwen and H. You, "A method of threat assessment using multiple attribute decision making," in *Int. Conf. Signal Process.*, vol. 2, Beijing, China, 26-30 Aug. 2002, pp. 1091–1095.

[19] N. Okello and G. Thorns, "Threat assessment using Bayesian networks," in *Int. Conf. Inf. Fusion (FUSION)*, Cairns, Australia, 8-11 Jul. 2003, pp. 1102–1109.

[20] X. T. Nguyen, "Threat assessment in tactical airborne environments," in *Int. Conf. Inf. Fusion (FUSION)*, vol. 2, Annapolis, MD, 8-11 Jul. 2002, pp. 1300–1307.

[21] M. L. Hinman, "Some computational approaches for situation assessment and impact assessment," in *Int. Conf. Inf. Fusion (FUSION)*, Annapolis, MD, 8-11 Jul. 2002, pp. 687–693.

[22] G. W. Stimson, *Introduction to airborne radar*, 2nd ed. New Jersey, USA: SciTech Publishing Inc., 1998.

[23] G. Claassen, "Time-interleaved jamming," Master's thesis, University of Pretoria, Pretoria, RSA, Jan. 2022.

Gert Claassen received the B.Eng.(Computer and Electronic) degree from the North-West University in 2012, and the B.Eng.Hons.(Electronic) and M.Eng.(Electronic) degrees from the University of Pretoria in 2019 and 2022, respectively.

He worked for Denel Dynamics in 2013 where he was part of the Seeker 400 UAV communication protocol team as a software engineer. He then joined SAAB Grintek Defense as a software engineer from 2013 to 2020 as part of the Land Electronic Defense System (LEDS) and then the radar warning receiver (RWR) teams. He moved to the Council for Scientific and Industrial Research (CSIR) in 2021 where he has since worked on the development of the radar control of the Illovane radar system. His research interests include radar and EW control systems and strategic theory.

Warren P. du Plessis (M'00, SM'10) received the B.Eng. (Electronic), M.Eng. (Electronic), and Ph.D. (Engineering) degrees from the University of Pretoria in 1998, 2003, and 2010, respectively, winning numerous academic awards including the prestigious Vice-Chancellor and Principal's Medal. He is an Associate Editor of the IEEE Transactions on Aerospace and Electronic Systems.

He spent two years as a lecturer at the University of Pretoria, and then joined Grintek Antennas as a design engineer for almost four years, followed by six years at the Council for Scientific and Industrial Research (CSIR). He is currently a Professor at the University of Pretoria, and his primary research interests are cross-eye jamming and thinned antenna arrays.