UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

TIME-INTERLEAVED JAMMING

by

Gert Claassen

Submitted in partial fulfillment of the requirements for the degree
Master of Engineering (Electronic Engineering)

in the

Department of Electrical, Electronic and Computer Engineering
Faculty of Engineering, Built Environment and Information Technology

UNIVERSITY OF PRETORIA

January 2022

SUMMARY

TIME-INTERLEAVED JAMMING

by

Gert Claassen

Supervisor(s):	Prof. Warren du Plessis
Department:	Electrical, Electronic and Computer Engineering
University:	University of Pretoria
Degree:	Master of Engineering (Electronic Engineering)
Keywords:	coherent integration, electronic warfare, intermittent jamming, noise jamming, pulse coincidence, radar, threat evaluation, threat prioritisation, time interleaved jamming,

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. Conventional noise pulse jammers allocate the jamming resources to the highest threat radar at a given time. However, concentrating jamming resources on only the radars that pose the highest risk to the platform excludes the rest of the enemy radars. These radars can therefore detect the platform without any obstruction from any countermeasures. Countering all radars will result in the jammer having to time-multiplex countermeasures for the radars to attempt to keep the risk towards the protected platform to a minimum. This is an issue for the platform as there could potentially be radars detecting the platform without interference. Countering every pulse from every active threat radar gives the platform the benefit of countering each threat simultaneously.

Modern jammer systems are capable of 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 jamming pulses to transmit when such coincidences occur. Intermittent jamming, where a pulse noise jammer misses radar pulses, is a consequence of pulse selection in a coincidence as only a single pulse is selected whilst the rest are disregarded. Newer generation radar

systems employ integration schemes to raise the signal level above the noise. Therefore it is necessary to determine the minimum number of jamming pulses required to inhibit detection in a radar's coherent processing interval (CPI), to allow intermittent jamming to occur while still preventing detection.

An approach to determining the minimum amount of jamming pulses per CPI and the relative priority of radar pulses is proposed and evaluated to show that time-interleaved jamming utilising noise as a jamming source is a viable approach to effectively countering multiple simultaneous threats. Time-interleaved jamming provides the solution where each jamming pulse in a coincidence goes through threat evaluation and the jamming pulse with the highest priority is selected to be transmitted. Threat evaluation uses the radar mode of operation, ranges, and jamming percentage per CPI to determine the threat radar's risk factor towards the platform.

The jamming percentage calculation determines the minimum amount of jamming pulses necessary to inhibit detection in a CPI, depending on the average intermittent jamming power and the radar's maximum signal-to-noise ratio (SNR) as determined by the radar range equation, over coherent integration of a CPI. It is determined that configuring the jamming percentage as the highest weighted parameter during threat evaluation provides the best jamming performance. Over the test duration, the majority of threat radars are kept at the lowest mode of operation namely the search mode where detection, classification and verification have not occurred or is set at a minimum. Time-interleaved jamming will only let a radar transition to a higher mode when the coincidences with other higher-risk radars outnumber the number of jamming pulses required to prevent detection, or when the platform is in burnthrough.

The findings show that a jamming pulse width needs to be as small as possible whilst still taking into consideration any error in the time of arrival estimation. Large jamming pulse widths that may depend on the pulse repetition interval (PRI) results in too many jamming pulses being in coincidence. This results in over 95% of the pulses for the majority of radars being in coincidence and only the radars close to the platform being countered while the others are disregarded. Using a jamming pulse width that is dependent on the pulse width of the radar waveform will result in far fewer jamming pulses being in coincidence. The best practice is to start the jamming pulse before the radar pulse arrives to allow for errors and end the jamming pulse just after the trailing edge of the threat radar pulse. This will decrease the coincidence rate of low duty cycle pulses to be under 75%, thereby enabling more jamming pulses to be selected in a CPI before having to take into account the pulses in coincidence. A lower coincidence rate will result in a lower jamming percentage rate for a pulse in coincidence. This, in turn, results in fewer coincidence pulses in a CPI requiring to be countered and thus allowing more pulses from different radars to be selected at the coincidence.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AAA	anti aircraft artillery
AGC	active gain control
AI	artificial intelligence
ANN	artificial neural network
AOA	angle-of-arrival
CPI	coherent processing interval
CPU	central processing unit
DF	direction-finding
DRFM	digital radio-frequency memory
EA	electronic attack
ELINT	electronic intelligence
EMS	electromagnetic spectrum
EP	electronic protection
ES	electronic support
EW	electronic warfare
HOJ	home on jam
IADS	integrated air-defence system
IF	intermediate frequency
LOB	line of bearing
LOS	line of sight
LRT	likelihood ratio test
MDS	minimum detectable sensitivity
MG	missile guidance
MUSIC	multiple signal classification
PDF	probability density function
POI	probability of intercept

PRF	pulse repetition frequency
PRI	pulse repetition interval
PSD	power spectral density
RCS	radar cross section
RF	radio-frequency
RMS	root-mean-square
SNR	signal-to-noise ratio
SPAAG	self-propelled anti-aircraft gun
TA	target acquisition
TDOA	time difference of arrival
TIJ	time-interleaved jamming
TOA	time of arrival
TS	target search
TT	target tracking
UHF	ultra high-frequency
VHF	very high-frequency

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1 INTRODUCTION

1.1 PROBLEM STATEMENT

In modern war zones, multitudes of radars are likely to be located within the detection capability of the platform's electronic support (ES) system at any given time. Such a high-density threat environment creates a congested electromagnetic spectrum (EMS) domain impeding the efficiency and effectiveness of a jammer. The resultant is an arduous environment to manoeuvre in without being detected [1].

A jamming system has a high likelihood to be confronted against multiple threat radars simultaneously, and potentially, all simultaneously-encountered threat radars will need to be countered to prevent detection. Simultaneous threat jamming is a difficult situation for both noise and deception jamming. However, conventional noise jamming will find it far more difficult to suppress simultaneous radars. Jamming over a large part of the radio-frequency (RF) spectrum is especially critical for noise jammers, as a noise jammer can either transmit noise signals at a high power spectral density (PSD) in a short frequency bandwidth spanning a few megahertz or have a low PSD spread over a large frequency bandwidth. Thus as the frequency range of the bandwidth increases so does the PSD decreases allowing the threat radar to have a better chance of detecting the platform. Moreover, the noise energy is reduced further with the use of signal processing techniques from the likes of pulse-Doppler radars. Pulse-Doppler processing utilises matched filtering where the received reflected pulse is cross-correlated with a template of the transmitted pulse. Matching the known pulse with the reflected pulse will maximise the output signal energy and reduce the noise bandwidth to that of the pulse, resulting in the reduction of the noise PSD. The signal energy will increase further when sequential pulses are integrated from a coherent processing interval (CPI), thereby multiplying the signal energy and reducing the noise energy. Therefore in this dense environment with newer radar systems equipped with signal capabilities to increase the chances of detections whilst suppressing noise a jamming system must make use of as much energy as possible on each of the active threats to prevent detection [1].

Multiple types of noise jamming techniques exist that a noise jammer can use. The conventional noise jamming techniques are spot jamming, sweep jamming and barrage jamming.

Spot noise jamming has the benefit of transmitting a high PSD over a small frequency bandwidth. However, radars have the benefit to manoeuvre inside the EMS by utilising frequency agility. Moreover, a large number of simultaneously emitting radars will result in a large diversity of frequencies that the jammer will encounter. Thus spot noise jamming has the issue of deciding which frequency to target in such a vast space of the EMS.

Sweep jamming, where narrowband noise is swept across a range of frequencies, will have more success in countering multiple to all of the threats, but a threat radar will be targeted for only a certain portion of time. However, sweep jamming is not very effective against radars performing signal detection per CPI. A few CPIs may be affected when the noise is present however the target will be detected once the noise transitions to another frequency range, which will result in the sweep jammer having a low probability of intercept (POI) against these radars.

Barrage jamming, where wideband noise is transmitted ranging from hundreds of megahertz to a few gigahertz, may jam multiple threats simultaneously, however, the noise PSD would be divided over the jamming bandwidth. Utilising barrage jamming will provide the least jamming capability against integration techniques such as coherent integration on a CPI, which will result in the integrated signal echoes of the platform rising above the averaged out noise energy.

A solution for the noise jammer to work effectively and efficiently in a high pulse density environment is to apply time-interleaving in noise jamming. The capability to jam a large number of threat radars effectively requires the implementation of time-sharing of the jammer system between the threats. Time sharing is achieved by concentrating the noise jammer energy only in a time window over the threat pulse and thereafter interleaving to the next pulse in the time domain. Thus the jammer only needs to utilise spot noise jamming over the threat radar pulse, thereby providing the advantage of high noise PSD by emitting only in a narrowband. Time sharing is dependent on the jammer's ability to change jamming characteristics to counter different radars pulses when hopping between the threat radars. Using time-interleaving counteracts wasteful use of jamming resources when indiscriminately using the noise jammer which may compromise the platform and result in target detection and location.

For time-interleaved jamming to work a jammer needs to track the time of arrival (TOA) of the threat radar pulses and have prior knowledge of the waveform characteristics to be able to generate effective noise pulses. The coherent storage of the waveforms can be accomplished using a digital radio-frequency memory (DRFM) which, will provide the noise jammer with the ability to determine a time and frequency domain layout of a sequential jamming profile for an active threat radar. A jamming profile is a collection of predetermined jamming pulses against a single threat radar and is generated for every active threat [1].

Jamming profiles will need to be generated for each active threat that needs to be countered in a jamming channel. The jamming channel will attempt to transmit each pulse from each profile, however, the jamming profiles are overlayed in the time domain resulting in jamming signals overlapping. Coincidence occurs regularly within a second and increases with the introduction of more radars, higher pulse repetition frequency (PRF) and larger pulse widths. This is proven by Kaszerman's equation as the frequency of coincidences increases rapidly with every high PRF radar [2]. Figure 1.1 provides an example of pulse coincidence where the pulses highlighted in grey are in coincidence and the coincidence durations are shown by the vertical stipple lines.

Various papers and openly sourced information conceptualises jamming mechanisms from division multiplexing, multichannel jamming, distributed jamming networks, and power managed jamming to attempt at actively jamming the threat radars concurrently [3–7]. However, even with the frequencies, angles and channels divided multiple radars are still present in a jamming channel and it is expected that an overlap of jamming signals will occur.

Apart from research [2, 8, 9] found analysing the effects of pulse coincide at the receiver of ES radar systems, no research has been done regarding pulse coincidence before the transmitter of a jamming system.

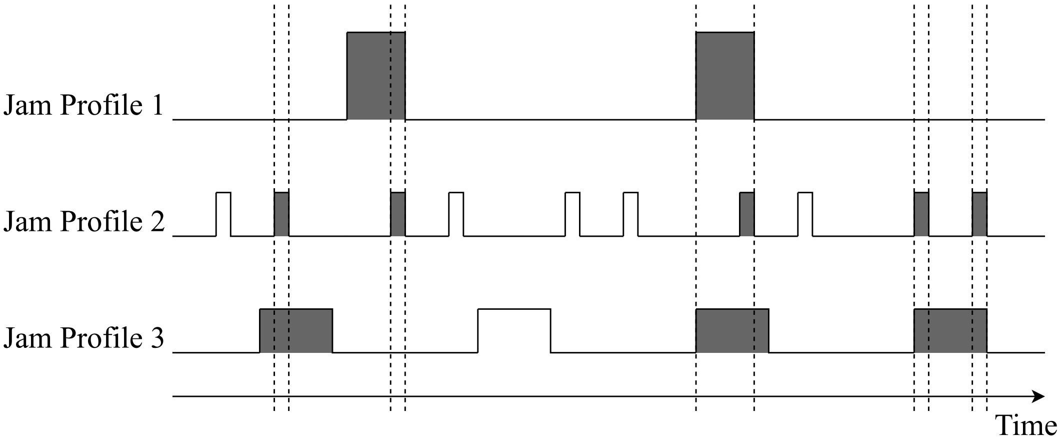


Figure 1.1. An example of jamming coincidence with the grey pulses being in coincidence and the vertical stipple lines showing the coincidence duration.

1.2 APPROACH

An approach termed time-interleaved jamming (TIJ) is proposed to jam multiple active threats simultaneously. TIJ interleaves between the active threat radar jamming profiles in the time domain and negates jamming coincidence through the use of evaluation, prioritisation and intermittent jamming.

For this dissertation, only one jamming pulse is selected in a coincidence with the rest disregarded. It will be more beneficial to only jam a single pulse with the maximum possible noise power than trying to send a jamming signal consisting of the overlapped signal frequencies. Attempting to counter multiple signals simultaneously will lead to a decrease in the PSD at the receiver of the threat radar. The more signals present the less noise power will be issued to each threat.

This is where the incorporation of jamming prioritisation is of importance and one of the key challenges of maintaining jamming effectiveness. Figure 1.2 provides an example where all solitary pulses and a single pulse from each coincidence are allocated for jamming. Each pulse will need to be evaluated to determine the risk it poses to the platform. Prioritisation is determined by monitoring the changes of a threat radar's behaviour. The pulse that poses the highest risk to the platform will be chosen above all others in a coincidence.

These behavioural changes range from a radar's inability to detect the platform to a situation where target lock-on has advanced to the point where the radar can guide a weapon system

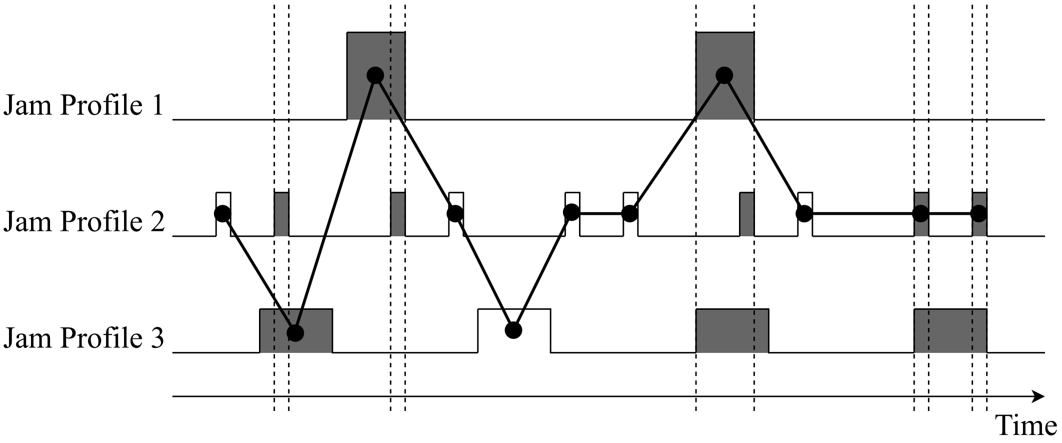


Figure 1.2. An example of Time interleaved jamming where the bold line indicates the chosen jamming pulses.

on or towards the platform. In combat situations, only the known information is available for assessment. ES provides threat observation and feedback by measuring the incident signals. Certain electronic warfare (EW) systems will interchange between jamming and ES whereas other systems can perform ES lookthrough whilst jamming is in progress. The measurements taken by the ES system will indicate any changes to the threat radar system due to jamming i.e. if the threat system radar changed mode or if lock-on is engaged or broken [1,7].

Intermittent jamming is a resultant of coincide. Impeding detection through intermittent jamming can only be achieved when jamming effectiveness is assured. Jamming effectiveness is the ability to reach a minimum probability of detection through jamming, which is far lower than the required probability of detection required by the threat radar to detect the platform. However, jamming effectiveness can only be obtained if the jamming signals can suppress the signal-to-noise ratio (SNR) below a particular range. Therefore TIJ will need to determine the size of n_j jamming pulses over a CPI of n_p pulses to reach the suppressed SNR.

To show the effectiveness of TIJ against multiple threat radars and the handling of coincidence some assumptions have been made. Firstly the amount of CPIs that needs to detect the target out of a set total necessary for target verification is unknown to the TIJ. Thus for the dissertation, the radar only needs to detect the platform in one CPI over an interval of 1 second. If the platform is detected in a CPI the threat radar will promote the mode of operation to a more lethal detection mode. Where modes range from searching for targets in a selected airspace, detecting the target and attempting to pinpoint the location, and finally tracking the target successfully where a weapon system can be used against the target. Moreover, the jammer is required to decrease the probability of detection for every CPI, of each active threat in the interval, below a required minimum probability of detection value, for the threat to lower its mode of operation.

Each threat radar will use a monostatic antenna configuration with the radar beam employing that of a tracking radar to position the maxima of the antenna beam on the platform. However, a beamshape loss is added for search and acquisition modes of operation to indicate that the beam is scanning over the platform and have not yet locked on to the target but the beam will never move off the platform. This assumption results in all of the active threats to have the radar beams indefinitely on the platform disregarding the radar's mode of operation. Thus the TIJ will face all of the threats continuously thereby testing the ability of the TIJ to inhibit multiple threat radars at different modes of operation simultaneously.

Transmission losses are kept to a minimum with the assumption of clear weather and the signal frequencies to be equal to or below 10 GHz [10, 11]. This will remove any unknowns in real losses as the capability of the TIJ should be measured without any benefit in detection loss due to external losses. Moreover, the jammer can not measure the losses and propagation factors of the threat radar thus these values are set at advantageous values for the radar or disregarded as the noise jamming signal will also experience the same losses as the reflected signal at the receiver. Therefore the jammer will always measure the jamming effectiveness against the best possible return signal.

The noise jamming quality factor will be set to low with a loss of 5 dB. The low noise quality factor is used as the jammer does not know what its effect is on the radar and the only measurable factor for jamming effectiveness is the mode change.

The research only investigates the jamming capability against multiple radars. Therefore it is assumed that a theoretical pulse repetition interval (PRI) tracker is used as ES does not form part of the hypothesis. The TOA will be precisely measured for each threat thus the noise pulse will be transmitted with no error in time estimation. Through research and testing the maximum jamming effectiveness possible with the use of TIJ will be determined.

With continuous improvement in antenna design achieving direction-finding (DF) accuracy less than 2° root-mean-square (RMS) [12] where multiple DF antennas are used in unison to triangulate the radar with the added benefit of algorithms such as multiple signal classification (MUSIC) to further improve position fix [13]. Other ES support sensors such as time difference of arrival (TDOA) and radars may also be equipped to determine the distance between the threat radar and platform. The current range of the radar is assumed to be measured perfectly even though there exist limitations in range measurements. However, errors in the range measurements are out of the scope of the research.

The platform can determine what the possible radar cross section (RCS) is, however for this dissertation the TIJ will be conservative by stating that the RCS will be a constant value equal to the maximum RCS of the platform. The maximum RCS is chosen to measure the noise jamming capability against the highest detection capability of the platform. Therefore, the radar and jammer applicable equations will be determined against the maximum RCS of the platform.

Differing signal polarization between radar and jammer antennas will result in a loss to the jamming noise signal. Therefore, it will be assumed that the polarization of the jammer will be circular, which will result in the polarization factor being -3 dB against radars employing linear polarized antennas [14].

1.3 RESEARCH OBJECTIVE AND QUESTIONS

The following list provides questions regarding pulse selection in jamming coincidence.

1. How effective will the quality of jamming be if only a single pulse can be countered in every coincidence?
2. Will the quality of jamming be negatively effected by interrupting the jamming process on an active threat radar?
3. What effects will selection and rejection of the jamming signals pose on future jamming allocation?

The answers to these three questions will provide the basis for determining threat evaluation and prioritisation. By knowing how the quality of the jamming is affected by interruption will guide how priorities are allocated to pulses.

1.4 RESEARCH GOALS

The research objective is to find a solution to determine which jamming signal is of the highest priority in a jamming coincidence situation. This dissertation will show if TIJ is a viable option to counter multiple active threat radars as well as the coincidence that occurs when many radars need to be jammed simultaneously.

Prioritisation of coincidence pulses to select a single pulse will cause intermittent jamming over the CPIs of the disregarded threat radars. Thus it is necessary to determine if only a portion of the pulses in the CPI can be jammed with noise. The proposed jamming control system will fail to inhibit detection from multiple radars simultaneously if all pulses in every CPI need to be jammed.

1.5 RESEARCH CONTRIBUTION

The research contribution of this study will provide a new jamming control technique (Time-interleaved jamming) to resolve selection between simultaneous jamming signals when the noise jammer can only output a single noise jamming pulse at a time. The success of the jamming coincidence research is dependent on the jamming effectiveness achieved with the use of intermittent jamming and situational awareness of the active threats and platform.

Intermittent noise pulse jamming uses the threat radar's signal detection capability and the jamming effectiveness of a spot noise jammer to determine the minimum amount of pulses that must be jammed in a CPI. Situational awareness will indicate to the TIJ controller the lethality of the threats encountered by the platform.

1.6 RESEARCH OUTPUTS

A paper for this work is currently in preparation for submission to the IEEE Transactions on Aerospace and Electronic Systems journal. The paper titled "Time-interleaved noise jamming" will detail the concept of TIJ to resolve selection between simultaneous jamming signals through jamming percentage calculation, situational awareness, and threat assessment and prioritisation. The results of the threat assessment evaluation and jamming capability are presented to show that TIJ is a viable approach to effectively counter multiple simultaneous threats with a single jamming channel. The research presents a new method of jamming, thus the limitations of the jamming capability and threat evaluation should be analysed as well. Therefore, the cause of high coincidence rates per CPI and the high number of pulses in a coincidence that affects jamming selection, which in turn prevents jamming effectiveness over a threat or multiple threats will also be discussed.

Paper

G.Claassen and W.P. du Plessis, "Time-interleaved noise jamming," in 2021 IEEE Transactions on Aerospace and Electronic Systems (in preparation).

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 radar pulses to coincide in time, leading to the problem of deciding which of the radar pulses to jam when such coincidences occur. An approach to determining the relative priority of radar pulses is proposed and evaluated to show that time-interleaved jamming is a viable approach to effectively countering multiple simultaneous threats.

1.7 DISSERTATION OUTLINE

Chapter 2 describes the radar equation and signal detection to determine the SNR and the maximum detectable range, the addition of noise jamming as a function of temperature at the receiver to inhibit detection up until the burnthrough range, and lastly the threat assessment and prioritisation to be implemented at every coincidence.

Chapter 3 discusses the TIJ which is designed around intermittent jamming and threat evaluation to determine the highest priority pulse in a coincidence.

Chapter 4 provides detail on the simulator and tests that is used to test the TIJ algorithm. The results from the tests are provided in said chapter.

Finally, Chapter 5 provides the conclusion to the dissertation, summarising the methodology testing and results of the TIJ control system. Potential areas of further research is also discussed.

CHAPTER 2 LITERATURE STUDY

2.1 OVERVIEW

The literature study will start by describing coincidences from the jammer's point of view. The formula to determine the total coincidences per second will be provided and discussed.

An understanding of the radar range equation and its parameters are necessary before the effect of noise jamming on a radar can be determined. Thus the literature study will delve into the radar range equation and statistical detection theory before moving over to the noise jamming equation. The radar equation is important to calculate as both the maximum detection range and the burnthrough range will indicate to the jammer system when to start jamming and when jamming will be inadequate.

Finally, radar modes, threat assessment and prioritisation are discussed. Radar systems are composed of various radar modes. Each mode uses different parameters, has a different objective and poses a different threat to the platform. In a coincidence, each jamming pulse is associated with a radar operating on different modes, at different detection characteristics, at different locations, and some combined with weapon systems. Each of the jamming pulses in the coincidence needs to undergo threat assessment before being prioritised.

2.2 COINCIDENCE

A coincidence is defined as the overlap of multiple signals. From the jammer's point of view, a coincidence is caused by the integration of multiple jamming profiles. It is important to determine the number of coincidences a threat radar will have to take into account in a jamming interval as each coincidence will affect the jamming effectiveness of the affected threat radar. With a single channel that will only transmit a single jamming pulse each coincidence will result in a jamming pulse to be selected and the rest to be disregarded.

The equations from [2] provide the probability and frequency of coincidences given 2 and more radars of varying pulse widths and PRFs. The probability of coincidences from multiple radars is determined from the PRI, T_{PRI}, and pulse widths, τ of the affected coincidence radars. The probability of coincidences are measured as

$$P\left(\text{coincidences radar } i\right) = \prod_{k=1}^{i-1}\left(\frac{T_{PRIk} - (\tau_i + \tau_k)}{T_{PRIk}}\right) - \prod_{\substack{k=1\\k\neq i}}^{n}\left(\frac{T_{PRIk} - (\tau_i + \tau_k)}{T_{PRIk}}\right), \tag{2.1}$$

where i is the radar in question and n is the total radars. The probability is measured by taking the radars in sequence as the previous radars have already been taken into account [2].

The total number of coincidences per second (in line with pulses per second of the PRF) is just the sum of the coincidences multiplied by the PRF, $1/T_{PRI}$, of each radar in the iteration except for the last radar [2]

$$f = \sum_{i=1}^{n-1} P\left(\text{coincidences radar } i\right) \cdot \frac{1}{T_{PRIi}}, \tag{2.2}$$

$$= \sum_{i=1}^{n-1}\left[\prod_{k=1}^{i-1}\left(\frac{T_{PRIk} - (\tau_i + \tau_k)}{T_{PRIk}}\right) - \prod_{k=1 k\neq i}^{n}\left(\frac{T_{PRIk} - (\tau_i + \tau_k)}{T_{PRIk}}\right)\right] \cdot \frac{1}{T_{PRIi}}. \tag{2.3}$$

2.3 THE RADAR RANGE EQUATION

The radar range equation is focal to radar system design. The radar equation is discussed thoroughly in most radar handbooks and texts with each parameter's influence on the radar performance examined and detailed. The purpose of the equation is to calculate the maximum range at which a certain detection performance can be achieved from a specified set of radar, target and environmental parameters. Over the years more parameters have been added and the equation modified to accommodate different radar types [14–16].

Blake's radar range equation has been used by various texts, like the radar handbook by Merril I. Skolnik [16] and the radar equations for modern radars book by David K. Barton [14]. Furthermore, the radar equation from Blake is further built upon by Barton [14] who provides a flexible way to differentiate between coherent and non-coherent integration gains from n pulses by only requiring minor changes when implementing either one of the two integration processes.

Therefore Barton's interpretation of Blake's radar equation will be scrutinised in the dissertation. The radar range equation is

$$R_{P_d} = \left[\frac{(P_t \tau) G_t G_r \lambda^2 \sigma F_t^2 F_r^2}{(4\pi)^3 D_x(1)(kT_s) L_t L_\alpha} \right]^{1/4} \quad \text{(km)}, \tag{2.4}$$

where,

- R_{P_d} is the maximum range depending on the signal detection value of P_d measured in kilometre (km),
- P_t is the transmit power output of the transmitter measured in kilowatt (kW),
- G_t is the transmitter antenna gain,
- G_r is the receiver antenna gain,
- τ is the pulse width of the transmitted signal pulse measured in microseconds (μs),
- λ is the threat radar waveform determined as c/F_c measured in meters (m), where c is the speed of light rounded to 3×10^{-8} ms^{-1} and F_c is the carrier frequency measured in megahertz (MHz),
- σ is the platform's maximum RCS measured in meters squared (m^2),
- F_t^2 is the pattern-propagation factor for transmitting antenna to target path,
- F_r^2 is the pattern-propagation factor for target to receiving antenna path,
- k is the Boltzmann's constant equal to 1.38×10^{-23} W/Hz,
- T_s is the overall noise temperature,
- L is the product of losses along the transmitter-receiver path, and
- $D_x(1)$ is the detectability factor for a single sample detection of Swerling type x [14, 15, 17].

Antenna gain is the ratio of the maximum radiation intensity to the intensity of a lossless omnidirectional antenna at equal power levels. The narrower the antenna beamwidth the greater the gain value will be. The gain is determined by estimating the antenna dimensions and beamwidth. Thus the transmit and receive gain values can be calculated and added to the threat library. For the dissertation, it is assumed that the same antenna is used for both transmitting and receiving. This results in the gains G_t and G_r being equal as well as for the factors F_t and F_r [18, 19].

The propagation factors account for the effects of path loss where the parameters are used to consider the possibility that the target is not in the main beam maxima. The effects that the propagation factors take into account are absorption, diffraction, shadowing, refraction and multipath interference. From the perspective of an EW system like TIJ the transmit and receive antenna gain can be determined, however, the EW system will not be able to predict what the pattern-propagation effects like multipath will have on the threat radar. Therefore for the pattern propagation factors, the dissertation will state that the TIJ will assume that platform is in free space and in the maxima of the antenna patterns resulting in $F_t = F_r = 1$ [15, 16].

Losses, L, occur in every part of the radar process. Transmission line loss, L_t, is the loss experienced in the path connecting the transmitter output to the antenna terminal where the gain is measured. An EW system can only determine the output of the radar when it is transmitting from the antenna. Signal processing loss, L_x, is the product of all receiver and signal processing losses. An EW system can also not determine any internal losses experienced by the receiver and signal processing however the jamming signal will go through the same receiver and experience the same losses as the echo signal. Therefore internal radar losses are disregarded for the dissertation [14].

Beam-shape loss, L_p, accounts for the loss in search and acquisition radars where the target is not directly on the beam. The search and acquisition radars will scan in azimuth and/or elevation as it is in the process of detecting targets. The tracking radar mode does not suffer from beam-shape loss as the beam is directly pointed at the target. The beam transitions across the target resulting in the gain varying as the target is situated at different parts of the beam for successive pulses. Resulting in the amplitudes of the return echoes required for integration to vary, creating a loss of integration gain. A typical beam-shape loss of 1.6 dB can be expected for one dimension scanning (azimuth or elevation) and the loss is doubled when scanning in two dimensions (azimuth and elevation). Therefore a constant beam-shape loss value of 1.6 dB will be implemented for all of the search and acquisition modes of threat radars against the TIJ [1, 14, 16].

As the signal propagates through the air it experiences losses over the two-way path it travels. In Figure 2.1 the loss negatively affects the transmit signal and echo. The losses that are considered for the line of sight (LOS) are the free space path loss and atmospheric absorption loss. Free space path loss or spreading loss, L_s, is the attenuation of the waveform energy transmitted between two points. Spreading loss is already taken into consideration in the radar equation as L depends on the distance to the platform R_c, the RCS of the platform to take into account the path back to the receiver, and the signal wavelength λ [20].

Atmospheric absorption loss, L_α, is the loss of a signal of a certain wavelength per kilometre of transition path at certain weather conditions. [10] states that the atmospheric loss below 10 GHz is less than 0.01 dB/km and the atmospheric loss graph in [20] shows that loss is close to 0.01 dB/km below 10 GHz. This approximation is adequate in clear weather conditions where there is no perspiration or fog [11]. For this dissertation, we assume clear weather and all radars will transmit a signal equal to and below 10 GHz. Therefore the absorption loss will be calculated as $L_\alpha = 0.01 R_c$ dB.

Figure 2.1 shows the signal energy fluctuations from the transmission to reception and how this along with the noise provides the detectability factor. The detectability factor depends on all of the parameters in the range equation. The echo signal energy is calculated from the transmit energy at the target range $(P_t G_t F_t^2)/(4\pi R_c^2 L)$, the reflection and spreading return of the reflected incident signal from the target $(\sigma)/(4\pi R_c^2 L)$, and the interception area of the receiving antenna $(G_r \lambda^2 F_r^2)/(4\pi)$. The return power, P_r, is thus equated as

$$P_r = \frac{P_t G_t G_r \lambda^2 \sigma F_t^2 F_r^2}{(4\pi)^3 R_c^4 L} \quad (\mathrm{W}). \tag{2.5}$$

A fundamental limitation to the target detection capability is that interference will always be present, which at a minimum consists of receiver thermal noise. Thermal noise can not be filtered out by any circuitry and still poses a fundamental limitation to the minimum energy a signal should have to be detected. Various types of noise exist that are intercepted by the receiver and negatively influences the detectability factor. Noise is the sum of the noise within the receiver as well as noise sources in the environment surrounding the antenna. It is impossible to determine what all of the noise within the receiver will be. But there exists information regarding the noise factor values, of some radars that exist in publications of Jane's [4], which indicates what the noise can be. We can use that information to predict the noise factor, F_n, of the threat radars the jammer will come up against and determine the system noise temperature

$$T_s = T_o F_n \quad (K), \tag{2.6}$$

where T_o is the standard temperature equal to 290 K, and F_n is the noise factor [19, 20].

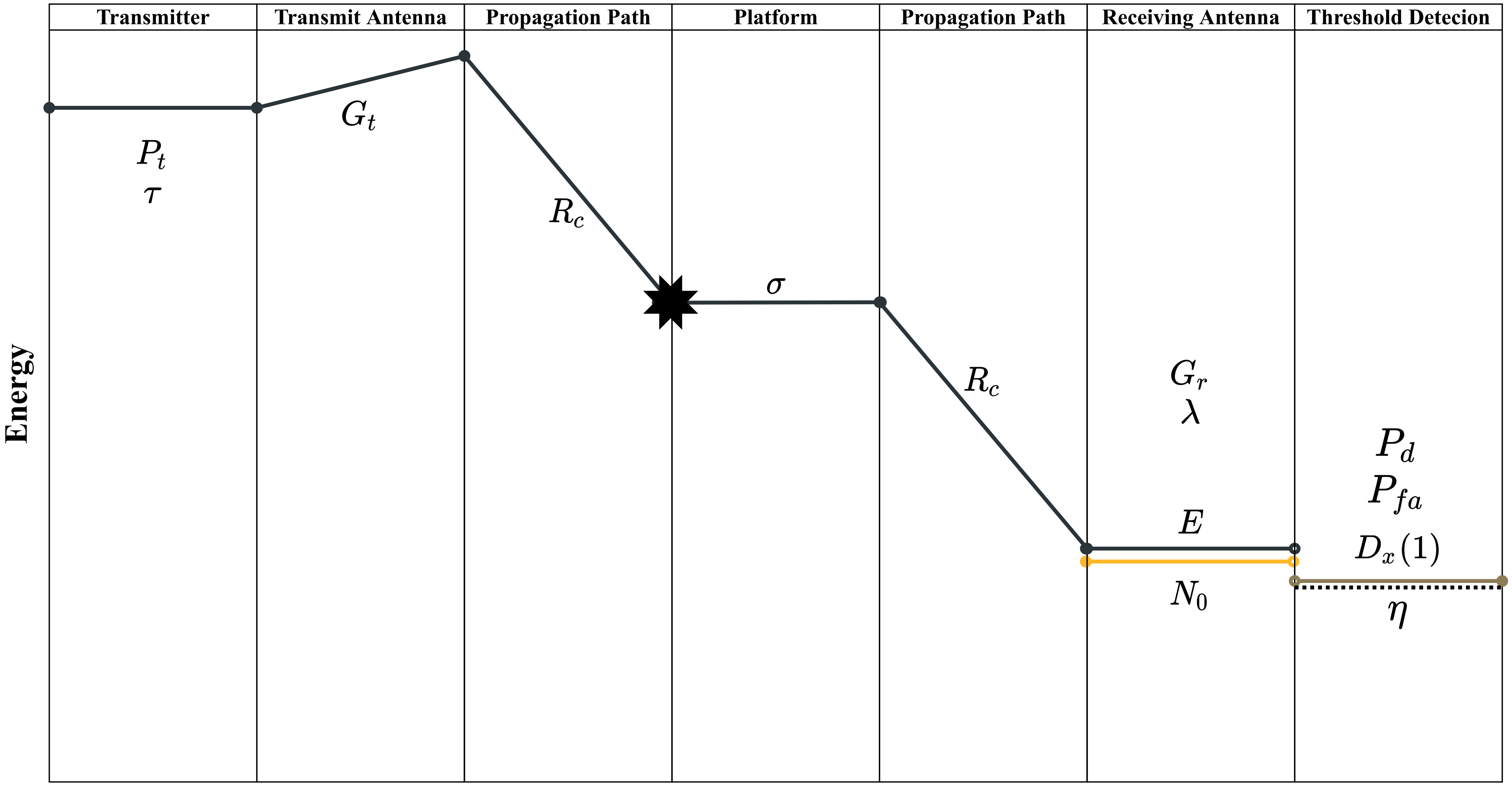


Figure 2.1. Signal and noise energy loss and gain diagram.

The noise signals within the frequencies of the detection bandwidth, B, will have a negative effect on the radar performance. Thus the thermal noise power is therefore proportional to the bandwidth of the signal. The bandwidth in this dissertation will be equal to the reciprocal of the pulse width, $\tau = 1/B$, as is used in practice. The noise power at the receiver is then calculated as

$$P_n = kT_sB \quad (W), \tag{2.7}$$

$$P_n = \frac{\tau}{kT_s}. \tag{2.8}$$

SNR or detectability factor is defined as the power ratio between the echo signal in (2.5) over the noise PSD, of (2.7), at the receiver of a single pulse and calculated as

$$D_x(1) = \frac{(P_t\tau)G_tG_r\lambda^2\sigma F_t^2F_r^2}{(4\pi)^3R_{P_d}^4kT_sL_tL_\alpha}. \tag{2.9}$$

Therefore (2.9) is just (2.4) rearranged to evaluate the achievable detectability factor of a single pulse at a range of R_c [15, 19].

2.3.1 Statistical Signal Detection

Because noise is such a random process it can only be described in terms of statistical properties. Therefore radar detection is a statistical problem [1].

The probability of detection, P_d, increases as the SNR increases for a given probability of false alarm P_{fa}. Therefore, SNR is a fundamental determinant of the quality of many radar signal processing operations. However, a single signal buried in the noise is not suitable for detection as the SNR will be far below the detection threshold, as visualised in Figure 2.2 [21].

Being able to obtain a desirable detection capability to increase the SNR multiple data samples needs to be processed together through integration (adding up the signals). As seen in Figure 2.2 it is beneficial to implement an integration scheme for the SNR to raise the signal above the noise. The two most known and discussed classes of integration are coherent and non-coherent integration techniques [21].

However, in this dissertation, only the coherent integration scheme will be used. This decision was made to test the TIJ employing noise jamming against the best performing pulse train integration scheme which is coherent integration.

Coherent integration is the measurement of complex-valued signals where the phase of each measurement is closely aligned. This allows for the integration of the signal voltages by the size n_p of the CPI. This scheme does not reduce the noise measurements as the mean noise power, μ, and variance, σ^2, as it also increases by a factor of n_p. However, the signals will increase faster than the noise as the signals are measured in voltage and converted to power, A^2, for the SNR calculation which will result in the signal integration gain being increased by a factor of n_pA^2 [15,21]. This gives a SNR of $n_p(A^2/\sigma^2)$ where the detectability factor of n_p coherent pulses can be determined as

$$D_x(n) = nD_x(1). \tag{2.10}$$

Through integration the single sample detectability factor can thus be decreased to

$$D_x(1) = \frac{D_x(n)}{n}. \tag{2.11}$$

As stated the SNR is dependent on the probability of detection and probability of false alarm. Therefore to perform capable detection the radar's detection threshold needs to be calculated.

Determining the probability of detection and probability of false alarm we consider a complex measurement z. The complex measurement consists of a complex signal s and noise w. The signal is modelled as $s = A\exp(j\theta)$ where A is the constant amplitude and θ is the constant phase. The noise is an independently and identically distributed complex Gaussian random process with the real and imaginary components having a mean equal to zero and a variance of σ^2 (also known as the mean square amplitude of the noise) and defined as the average noise power, at the output of the matched filter [21].

Two hypothesis are exist to either determine if z consists only of noise, denoted as the null hypothesis H_0, or if both are present, denoted as the alternative hypothesis H_1

$$H_0: \quad z = w, \tag{2.12}$$

$$H_1: \quad z = s + w. \tag{2.13}$$

These hypotheses are placed in probability density functions (PDFs) which describes the probability of the measurement existing in either of the hypotheses. The PDF of each hypothesis are denoted as $p(z|H_0)$ and $p(z|H_1)$ [21].

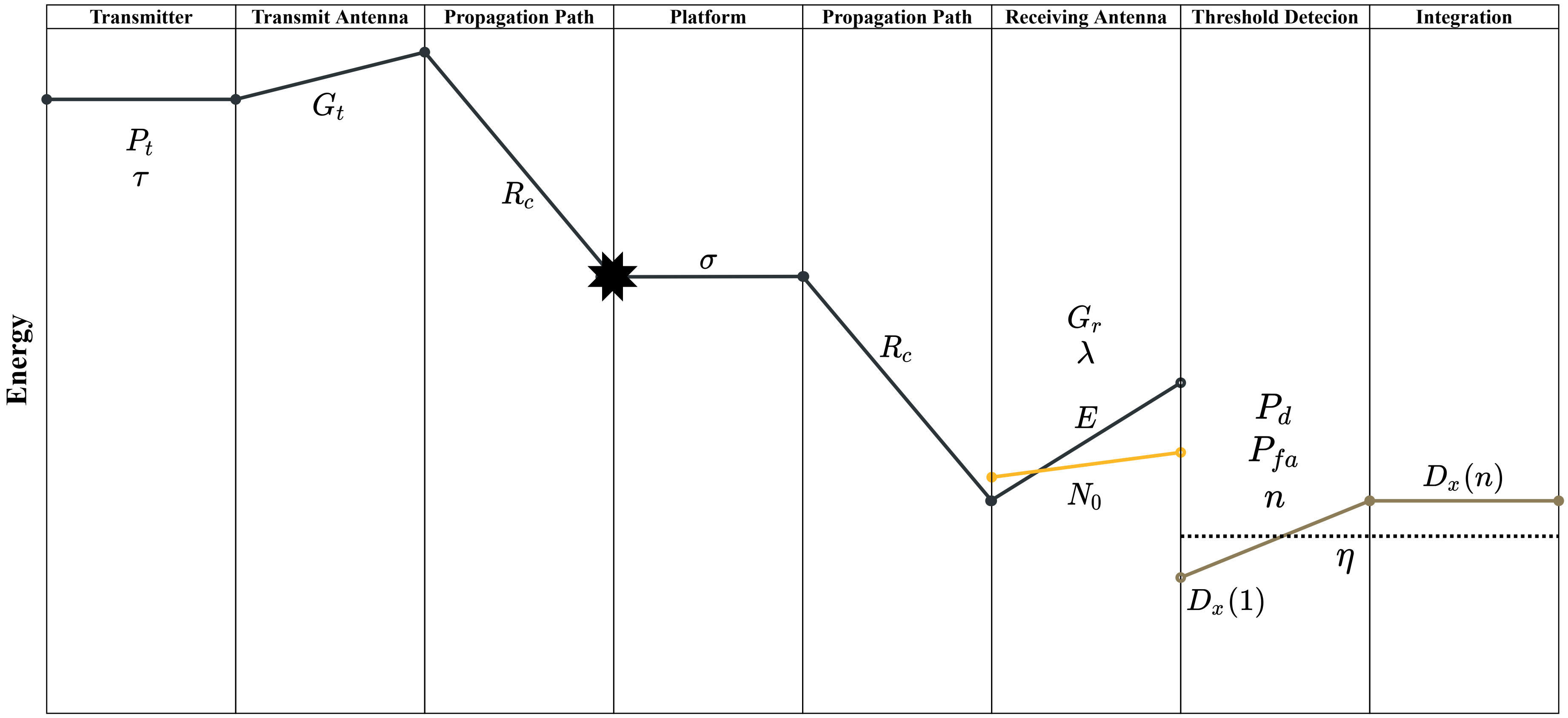


Figure 2.2. Signal and noise energy loss and gain diagram with the signals integrated to increase detection above the detection threshold.

In this dissertation, the Neyman-Pearson criterion is implemented to maximize the probability of detection by keeping the probability of false alarm at a predefined value. Implementing the detection threshold requires the likelihood ratio test

$$\Lambda(z) = \frac{p(z|H_1)}{p(z|H_0)} \overset{H_1}{\underset{H_0}{\gtrless}} \eta, \tag{2.14}$$

which can also be adapted to the log likelihood ratio test

$$\ln\left[\Lambda(z)\right] = \ln\left[\frac{p(z|H_1)}{p(z|H_0)}\right] \overset{H_1}{\underset{H_0}{\gtrless}} \ln\left(\eta\right), \tag{2.15}$$

where η is the detection thresholds [21, 22].

(2.14) states that the ratio of the two PDFs should be compared to η when observing signal samples z. Therefore the equation determines if a target is present or only noise based directly on the observed data z and η. Whereas (2.15) provides a more computationally efficient way of determining the likelihood ratio test (LRT). This is achieved by using the logarithms of two variables, as the PDFs of $\Lambda(z)$ consists of exponential functions. The LRT is a monotonic increasing operation hence taking the logarithms will not affect either the probability of detection or false alarm [22, 23].

Determining the probability of false alarm we start by determining the result of a complex noise signal using a Gaussian PDF

$$p(z|H_0) = \frac{1}{\pi\sigma^2}\exp\left[\frac{-z^*z}{\sigma^2}\right], \tag{2.16}$$

where $\cdot^*$ is the complex conjugate of the measurement. As $z = w$ for H_0 only noise is present and neither the signal amplitude nor phase are present. The Gaussian PDF is known as the Rayleigh PDF [22].

Determining the probability of detection for a none fluctuating signal plus noise H_1 must take into consideration that the phase of signal s is unknown. Signal s is remodelled as $s = \tilde{s}\exp(j\theta)$ where $\tilde{s}$ is the amplitude of the target component of the echo signal. The phase angle θ is modelled as being a random variable distributed uniformly over $(0, 2\pi)$ and independent from amplitude $\tilde{s}$. Adjusting (2.16) from (2.12) provides the capability to determine the result of a complex signal plus noise

$$p(z|H_1,\theta) = \frac{1}{\pi\sigma^2}\exp\left(-\frac{[z-\tilde{s}\exp(j\theta)]^*[z-\tilde{s}\exp(j\theta))]}{\sigma^2}\right), \tag{2.17}$$

$$= \frac{1}{\pi\sigma^2}\exp\left(-\frac{z^*z - 2|\tilde{s}^*z|\cos\theta + \tilde{s}^*\tilde{s}}{\sigma^2}\right). \tag{2.18}$$

PDF $p(z|H_1)$ can be obtained by averaging the pdf $p(z|H_1,\theta)$ over θ by using the Bayesian approach for random parameters. This will result in the PDF only relying on the magnitude of the complex signal sample but not the random phase of the target echo. This results in a Rician PDF

$$p(z|H_1) = \frac{1}{2\pi}\int_0^{2\pi} p(z|H_1,\theta)d\theta, \tag{2.19}$$

$$= \frac{1}{\pi\sigma^2}\exp\left(-\frac{z^*z+\widetilde{s}^*\widetilde{s}}{\sigma^2}\right)I_0\left(\frac{2|\widetilde{s}^*z|}{\sigma^2}\right), \tag{2.20}$$

where $I_0(\cdot)$ is the modified Bessel function of the first kind [21,22].

The log likelihood ratio test can then be written as

$$\ln\lambda = \ln I_0\left(\frac{2|\widetilde{s}^*z|}{\sigma^2}\right). \tag{2.21}$$

which indicates that it is the magnitude that is required to detect a complex signal return with an unknown phase. The amplitude $\widetilde{s}$ depends on the factors of the radar range (2.4) [21,22].

The performance of the detector can be expressed in a convenient manner through (2.22) which replaces $p(z|H_1)/p(z|H_0)$ and $\ln\eta$ from (2.15) with λ the sufficient statistic detection threshold T_d

$$\lambda \underset{H_0}{\overset{H_1}{\gtrless}} T_d. \tag{2.22}$$

The distribution of λ is therefore needed under each of the two hypotheses [22].

The optimal detection problem now changes to solving T_d through the probability of detection and false alarm PDFs expressed in terms of the sufficient statistic

$$P_d = \int_{T_d}^{\infty} P(\lambda|H_1)d\lambda, \tag{2.23}$$

and

$$P_{fa} = \int_{T_d}^{\infty} P(\lambda|H_0)d\lambda, \tag{2.24}$$

Because the probability of false alarm is set to a predefined value as defined by the Neyman-Pearson criterion meaning that T_d can be solved with the use of (2.24). The probability of detection can then be calculated from (2.23) as a function of the known values from the probability of false alarm with T_d as an intermediate between the probabilities [21].

Under H_0 which only exist of complex random Gaussian processes the PDF is denoted as $\mathcal{N}\{0,\sigma^2/2\}$ where the noise mean is zero and variance is $\mathcal{N}\{\mu,\sigma^2\}$. As it is noise λ will be

Rayleigh distributed

$$p(\lambda|H_0) = \begin{cases} \frac{2\lambda}{\sigma^2}\exp\left(-\frac{\lambda^2}{\sigma^2}\right), & \lambda \geq 0 \\ 0, & \lambda < 0 \end{cases}. \tag{2.25}$$

Therefore the probability of false alarm is then

$$P_{fa} = \int_{T_d}^{\infty} p(\lambda|H_0)d\lambda, \tag{2.26}$$

$$= exp(-\frac{T_d^2}{\sigma^2}). \tag{2.27}$$

Inverting (2.26) provides the threshold detection

$$T_d = \sigma\sqrt{-lnP_{fa}}, \tag{2.28}$$

which provides the way to set the threshold at the input of the linear detector to achieve a set P_{fa}, assuming the noise power at the detector is known [22].

Determining the probability of detection of a signal in noise we determine the distribution under H_1 which is denotes as $\mathcal{N}\{\widetilde{s}\cos\theta, \sigma^2/2\}$ for the real components and $\mathcal{N}\{\widetilde{s}\sin\theta, \sigma^2/2\}$ for the imaginary components. The PDF of λ for a signal plus noise is thus

$$p(\lambda|H_1) = \begin{cases} \frac{2\lambda}{\sigma^2}\exp\left(-\frac{\lambda^2+\widetilde{s}^2}{\sigma^2}\right) I_0\left(\frac{2\widetilde{s}^2\lambda}{\sigma^2}\right), & \lambda \geq 0 \\ 0, & \lambda < 0 \end{cases}, \tag{2.29}$$

from which the probability of detection can then be determined from. For convenience the integration of (2.29) can be substituted with $t = \lambda/\sqrt{\sigma^2/2}$ and $\alpha = \sqrt{2\widetilde{s}^2/\sigma^2}$. This ensures a more standard integral

$$Q_m(\alpha,t) = \int_{T_d}^{\infty} t\exp\left(-\frac{t^2+\alpha^2}{2}\right) I_0(\alpha t)dt. \tag{2.30}$$

which is known as Marcum's Q-function. In terms of Marcum's Q-funtion the probability of detection is

$$P_d = Q_m(\alpha,t) = Q_m\left(\sqrt{\frac{2\widetilde{s}^2}{\sigma^2}}, \sqrt{\frac{2T_d^2}{\sigma^2}}\right). \tag{2.31}$$

The arguments from (2.31) can be replaced with the detectability factor and probability of false alarm to give

$$P_d = Q_m\left(\sqrt{2D_x(1)}, \sqrt{-2\ln(P_{fa})}\right). \tag{2.32}$$

which provides the probability of detection of a single sample non fluctuating target in Gaussian complex noise [22].

However we need to determine the detection capability for coherent integration over a CPI of n_p pulses. The measurements are then taken over the entire CPI

$$z_{n_p} = s_{n_p} + w_{n_p}, \tag{2.33}$$

with the n_p measurements placed in a vector giving

$$\underline{z} = \left[z_0, \cdots, z_{n_p-1}\right]^T, \tag{2.34}$$

$$\underline{s} = \left[s_0, \cdots, s_{n_p-1}\right]^T, \tag{2.35}$$

$$\underline{w} = \left[w_0, \cdots, w_{n_p-1}\right]^T. \tag{2.36}$$

The joint PDF for the complex measurements of size n_p will be

$$p(\underline{z}) = \frac{1}{\pi^{n_p}\sigma^{2n_p}} \exp\left(-\frac{(\underline{z}-\underline{s})^H(\underline{z}-\underline{s})}{\sigma^2}\right), \tag{2.37}$$

where H is the Hermatian operator (the conjugate transpose). However as the signal phase is not known we replace the known signal $\underline{s}$ with the signal with unknown phase $\underline{\tilde{s}}\exp(j\theta)$. Equations (2.16) to (2.21) are repeated again. All of the equations will still be the same except that the vectors of (2.34) and $\underline{\tilde{s}}\exp(j\theta)$ will be used instead of the single sample measurements and the complex conjugate $\cdot^*$ is replaced with the conjugate transpose $\cdot^H$ [21].

As seen here the coherent integration is identical as the single sample detection but the SNR will be increased by the size of the CPI. (2.37) under H_0 will result in $\underline{s} = 0$ and under H_1 where $s \neq 0$ resulting in the log likelihood ratio to be

$$\ln\Lambda(\underline{z}) = \frac{2\Re(\underline{s}^H\underline{z}) - \underline{s}^H\underline{s}}{\sigma^2}. \tag{2.38}$$

The detection statistic can thus be determined as the matched filter over multiple measurements (also known as the coherent detector) $\lambda = \Re(\underline{s}^H\underline{z})$ [21].

Under H_1 with $s_{n_p} = A_{n_p}\exp(j\phi_{n_p})$ (2.38) can be further calculated as:

$$\lambda(z) = \Re(\underline{s}^H\underline{s} + \underline{s}^H\underline{w}), \tag{2.39}$$

$$= \Re\left(\sum_{i=0}^{n_p-1}|A_i|^2 + \sum_{i=0}^{n_p-1} w_i A_i \exp(-j\phi_i)\right), \tag{2.40}$$

$$= E + \Re\left(\sum_{i=0}^{n_p-1} w_i A_i \exp(-j\phi_i)\right). \tag{2.41}$$

$E = \sum_{i=0}^{n_p-1}|A_i|^2$ is the total energy in $\underline{s}$ and $E = n_pA^2$ in the equal mean case with $A_i = A$. From (2.39) the signal power after the dot product will be $A^2n_p^2$ and for the signal, the noise variance is $n_p\sigma^2$. The SNR is thus equal to (2.10) [21].

Under H_0 the coherent comparator is denoteds as $\underline{s}^H\underline{z} \sim \mathcal{N}\{0, 2\sigma^2 E\}$. From hereon the detection statistic for the Rayleigh distribution is calculated as

$$p(\lambda|H_0) = \begin{cases} \frac{2\lambda}{E\sigma^2}\exp\left(-\frac{\lambda^2}{E\sigma^2}\right), & \lambda \geq 0 \\ 0, & \lambda < 0 \end{cases}. \tag{2.42}$$

The probability of false alarm is therefore

$$P_{fa} = \int_{T_d}^{\infty} p(\lambda|H_0)d\lambda, \tag{2.43}$$

$$= \exp\left(-\frac{T_d^2}{E\sigma^2}\right). \tag{2.44}$$

[22] states that inverting (2.43) provides the threshold detection

$$T_d = \sqrt{-E\sigma^2 \ln(P_{fa})}. \tag{2.45}$$

Determining the probability of detection of a signal in noise we determine the distribution under H_1 which is denotes as $\underline{s}^H\underline{z} \sim \mathcal{N}\{E, \sigma^2 E\}$. The PDF of λ for a signal plus noise is thus

$$p(\lambda|H_1) = \begin{cases} \frac{2\lambda}{E\sigma^2}\exp\left(-\frac{\lambda^2+E^2}{E\sigma^2}\right) I_0\left(\frac{2\lambda}{\sigma^2}\right), & \lambda \geq 0 \\ 0, & \lambda < 0 \end{cases}. \tag{2.46}$$

The probability of detection can then be determined from (2.46) by using the Rician PDF from T_d to ∞ and again expressing it in terms of the Marcum Q-function

$$P_d = Q_m(\alpha, t) = Q_m\left(\sqrt{\frac{2E}{\sigma^2}}, \sqrt{\frac{2T_d^2}{E\sigma^2}}\right). \tag{2.47}$$

Note that $E/\sigma^2 = n_p A^2/\sigma^2$ which is the detectability factor for n_p measurements and expressing the threshold in terms terms of hte probability of false alarm will give

$$P_d = Q_m\left(\sqrt{2D_x(n)}, \sqrt{-2\ln(P_{fa})}\right), \tag{2.48}$$

which is similar to (2.32) but with the single sample SNR replaced with the integrated SNR of measurements [22].

2.3.2 Maximum Range

The maximum detectable range for the threat radar corresponds to the lowest signal return power measured at the receiver's minimum detectable sensitivity (MDS) that will produce detection of a platform. When the maximum range of the radar is specified it should be stated in a statistically, by referring that the radar has a detection range of R_{P_d} km on a σ m^2 Swerling x target with a probability of detection P_d and a probability of false alarm of P_{fa} integrated with integration scheme c over n_p pulses. As indicated in Section 2.3.1 the probability of detection is dependent on SNR therefore the detection range R_{P_d} is also dependent on SNR [1, 15, 20].

Substituting (2.9) with the single sample detectability factor $D_x(1)$ into (2.10) gives

$$D_x(n) = n_p \cdot \frac{(P_t\tau)G_tG_r\lambda^2\sigma F_t^2F_r^2}{(4\pi)^3R_{P_d}^4kT_sL_tL\alpha}. \tag{2.49}$$

However, for a radar implementing coherent integration of size n_p, it is suffice to use the CPI time and average power transmitted over the CPI. The CPI, T_f, is determined as

$$T_f = nPRI \quad (\mu\text{s}), \tag{2.50}$$

and the average power is the peak power transmitted over the PRI

$$P_{av} = P_t\frac{\tau}{PRI} \quad (\text{kW}). \tag{2.51}$$

By substituting T_f and P_{av} with the P_t and τ gives in (2.49)

$$D_x(n) = \frac{(P_{av}t_f)G_tG_r\lambda^2\sigma F_t^2F_r^2}{(4\pi)^3R_{P_d}^4kT_sL_tL\alpha}. \tag{2.52}$$

This equation will provide the detectability factor value, $D_x(n)$, for n_p coherently integrated pulses at a distance of R_c. Equations (2.9) and (2.52) provide the detectability factors for both a single pulse and n_p coherently integrated pulses. The results of (2.9) and (2.52) can then be inserted in the (2.32) and (2.48) to determine the probability of detection P_d at range R_c.

(2.52) provides the maximum detection range R_{P_d} after coherent integration

$$R_{P_d} = \left[\frac{(P_{av}t_f)G_tG_r\lambda^2\sigma F_t^2F_r^2}{(4\pi)^3D_x(n)kT_sL_tL\alpha}\right]^{1/4} \quad (km). \tag{2.53}$$

Therefore to attain the detection range of R_{P_d} either (2.4) for a single pulse detectability factor or (2.53) for a detectability factor value from n_p coherently integrated pulses should be met [15].

As shown in Figure 2.1 a single pulse detectability factor has to be higher than the threshold detection, η, to detect a target at a detection range of R_{P_d}. Figure 2.1 also show that the detectability factor of from n_p coherently integrated pulses increases the detectability factor to be far above the threshold level η. Thus coherent integration provides two advantages for the radar (2.53). Firstly the range can be extended, the single pulse detectability factor will be well below the noise power but the detectability factor from n_p coherently integrated pulses will equal the required P_d. The second advantage is to keep the distance of the current detection range of R_{P_d} for a single pulse detectability factor, but the probability of detection will be decreased when using the detectability factor from n_p coherently integrated pulses. This will allow the radar to detect targets at a lower probability of detection.

2.4 NOISE JAMMING

Noise jamming is an electronic attack (EA) technique used to raise the noise threshold to compromise the sensitivity of the threat system receiver and interfere with the signal detection process of a threat system. Thus when noise jamming enters the receiving antenna within the range bin of the detection signal, the noise jamming level will increase the receiver noise level above the received signal amplitude. The effectiveness of noise jamming is evaluated by including the jamming spectral density, J_0, to the radar equation as a component of interference [14]. The jamming spectral density is equated as

$$J_0 = \frac{Q_j P_j G_j G_r \lambda^2 F_p j^2 F_j^2 F_r^2}{(4\pi)^2 R_c^2 B_j L_{tj} L_{\alpha j}}, \tag{2.54}$$

where,

- Q_j is the jamming noise quality factor,
- P_j is the jammer transmitter power measured in kilowatt (kW),
- 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 in kilometer (km),
- B_j is the noise bandwidth in megahertz (MHz),
- L_{tj} is the jammer transmission line loss, and
- $L_{\alpha j}$ is the jammer to radar atmospheric attenuation for one way propagation [14].

Figure 2.3 shows the change in power of the threat radar waveform through the air from the threat to the platform. The jammer output power is far higher than that of the reflected signal energy. This is because the jamming signal is attenuated in proportion to the second power of the range as the noise signal only travels one way. This is in contrast to the signal which is attenuated to the fourth power as detailed in Section 2.3. The signal power is also influenced by the back-scattering characteristics of the target platform. But as indicated in Section 2.3.1

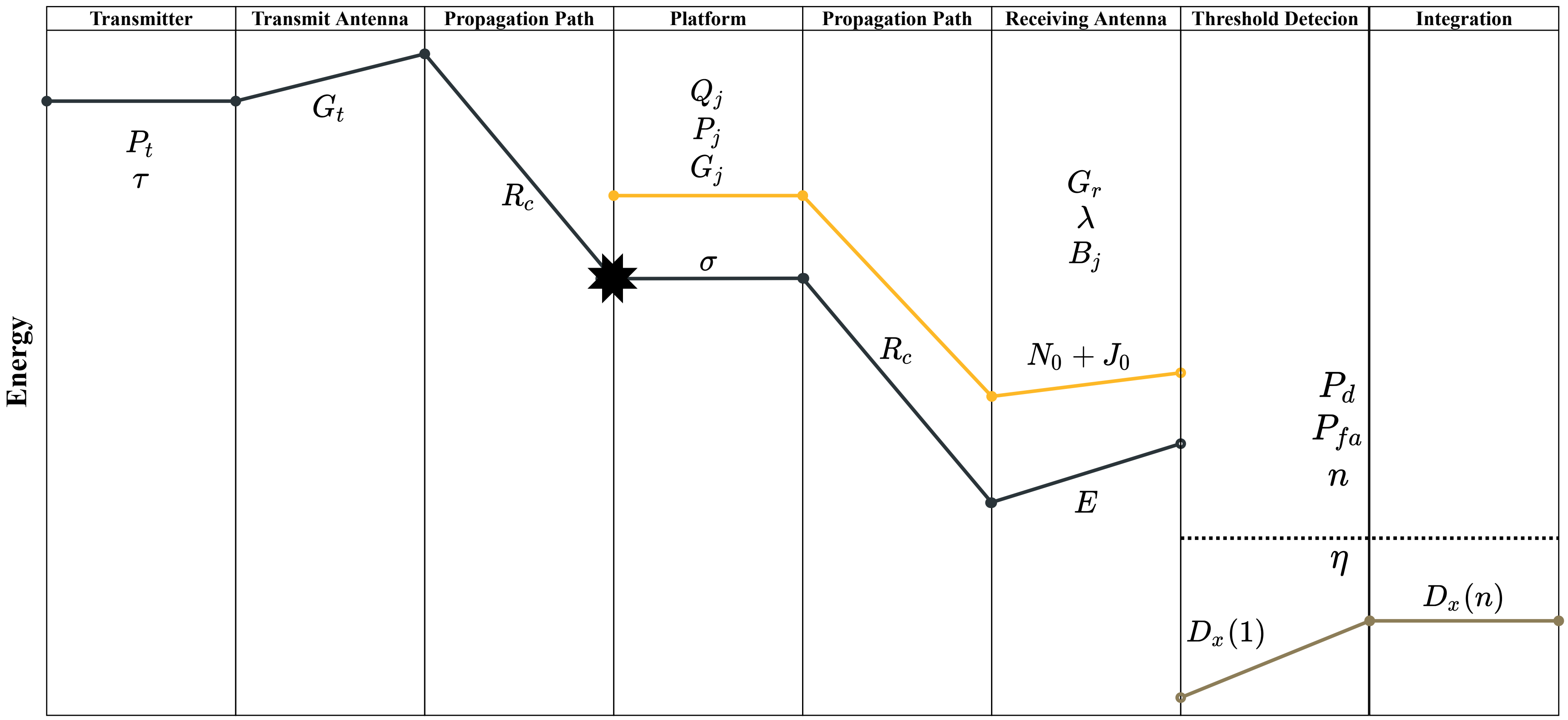


Figure 2.3. Signal and jamming plus noise energy loss and gain diagram.

the signal energy in the SNR is squared as opposed to the average noise signal power and also increases by the factor of the CPI size [1].

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. [24] states that the noise signal power, P_j, is the average noise power over signal size of n_p is

$$P_j = \frac{1}{n_p} \sum_{i=1}^{n_p} P_{ji}. \tag{2.55}$$

For self-screening noise jammers using cover pulse jamming the output P_{ji} is measured after the jammer has reached full output. The typical jamming duty cycle will be 10% of the threat radar PRI. Smart noise jammers will adjust the output power based on the incident signal amplitudes measured. If they are integrated with a DRFM the jamming bandwidth can be that of a spot jammer resulting in the jammer lowering the output power even more [1, 14].

If for any reason the noise signal is not concentrated on a pulse then the average jamming power will decrease by a factor of P_{j1}/n_p. The noise average will decrease the more signals are missed.

The noise jammer will concentrate on the carrier frequency of the transmit signal with its PSD spread over a larger frequency bandwidth, B_j, than what the pass-band of the receiver will allow. If white noise, where the PSD is uniform across the spectrum, is used for jamming then only a fraction will pass through the receiver. The bandwidth in spot jamming is slightly larger than the known intermediate frequency (IF) pass-band, $B_j > B$, to incorporate for errors in the measurements and jammer and radar tuning uncertainties. However, the bandwidth is much smaller than barrage jamming resulting in more energy to be passed in the threat radar receiver [11, 14].

The noise quality factor 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 P_j by $+7$ dB) 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 to -2 dB to express its capability to transmit Gaussian noise signals [1, 14].

The current range, R_c, is defined as the linear distance between the platform and the threat radar system. The platform relies on its ES DF antennas and their placement and the signals transmitted by the threat radar system to determine the position fix. The measured incident signal parameters that are most frequently used for determining the position fix are the azimuth angle-of-arrival (AOA), line of bearing (LOB), phase, and TDOA. Other range measure sensors can also be equipped like a radar on the platform determining the range of other platforms in the space. As stated the dissertation assumes that the current range measurements will be precise.

The jammer to radar pattern propagation factor, F_j, accounts for the effects of path loss where the jammer antenna beam is not in the main beam maxima of the receiver. F_j will equal 1 in the dissertation as the platform performs self-screening noise jamming on the axis of the radar mainlobe [14]. The polarization factor, F_{pj}, is the ratio of the amount of jamming signal voltage received by the threat antenna. As stated the jamming antennas are assumed to be circular with the threat radar antennas vertical or horizontal, resulting in a polarization factor to be -3 dB. The jammer one-way transmission line loss and atmospheric attenuation is half the decibel value of the radar transmission line loss and atmospheric attenuation [14].

If only the thermal noise and jamming noise are present in the range interval at the receiver input then the jamming spectral density of (2.54) can be expressed in the form of temperature (T_j) [14, 25, 26]. The noise jamming temperature equation will thus be

$$T_j = \frac{J_0}{k} = \frac{Q_j P_j G_j G_r \lambda^2 F_p j^2 F_j^2 F_r^2}{(4\pi)^2 R_c^2 k B_j L_{tj} L_{\alpha j}} \quad (\mathrm{K}), \tag{2.56}$$

and the total noise power at the receiver is then

$$P_{n+j} = kT_s + kT_j, \tag{2.57}$$

$$= k(T_s + T_j). \tag{2.58}$$

2.4.1 Burnthrough Range

The burnthrough range is the range where the platform can be detected with the jammer fully active against a threat radar [14]. It can be seen in Figure 2.4 that the burnthrough range can be increased by either increasing the CPI size to increase the SNR further, using a high probability of detection value resulting in the detection range being shorter, but the detection process requires a higher SNR, or just by sending more energy to the target with an increase in the duty cycle.

The burnthrough range is obtained by replacing T_s in (2.53) with the noise jammer present system noise of (2.57)

$$R_{P_d} = \left[\frac{(P_{av}t_f)G_tG_r\lambda^2\sigma F_t^2F_r^2}{(4\pi)^3D_x(n)k(T_s+T_j)L_tL\alpha} \right]^{1/4} \quad (\mathrm{km}). \tag{2.59}$$

(2.59) provides the maximum distance that the threat radar will be able to detect the platform when the maximum amount of noise jamming PSD in the IF is added as thermal noise over the entire CPI.

2.5 THREAT ASSESSMENT AND RANKING

Radars do not normally consist of a single set of radar waveform characteristics to detect platforms but are compromised with a variety of waveform fundamentals. This results in a radar that consists of multiple instances of the same radar mode with varying waveform characteristics, where a mode can interchange between the instances to prevent EA jamming attacks interfering with its detection capabilities. The threat systems will with a high likelihood consist of multiple radar modes transitioning from one radar mode to the next, with the intent to secure lock-on on the platform. Therefore a threat system can consist of multiple radar modes with each mode consisting of multiple waveform instances [19].

The types of modes of operation that can be employed are search, acquisition, target tracking and missile guidance/fire control. Table 2.1 discusses these modes in more detail.

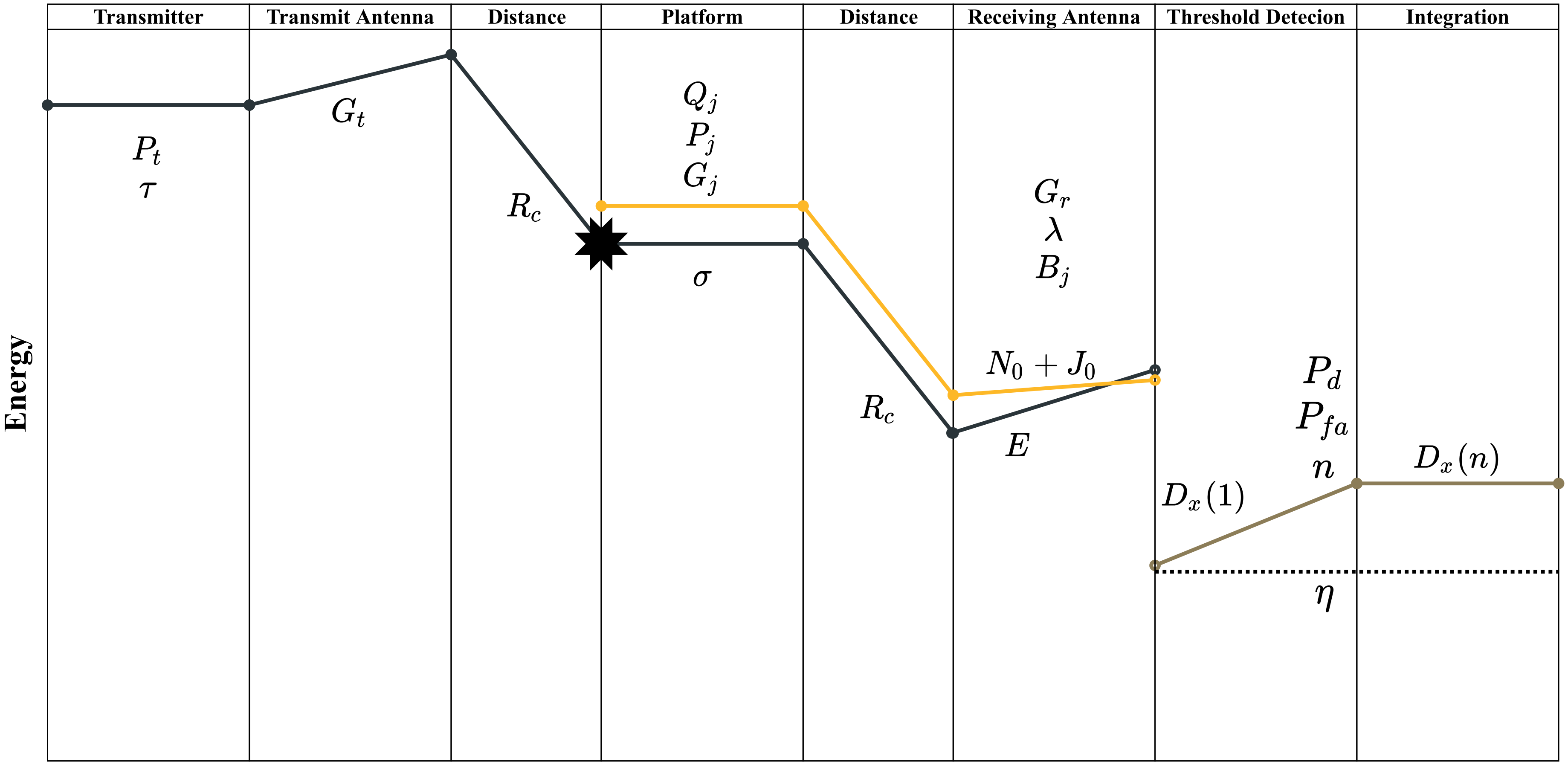


Figure 2.4. Signal and jamming plus noise energy loss and gain diagram when burnthrough occur.

Table 2.1. Table of radar modes

Mode	**Short Code**	**Definition**	**Characteristics**
Target Search	TS	The search radar looks for targets where there exists no prior knowledge of the target profile and location. The search radar determines the approximate location of the target [23].	• High powered for a larger maximum range, • low and medium PRF, • antenna rotates 360° in azimuth in search of targets, • use of fan beams to cover large volumes of space quickly, and • frequency bands from very high-frequency (VHF) - ultra high-frequency (UHF) and L-band for long range surveillance, ranging from low to medium resolution and accuracy with no effects from the weather to S-, C-, and X-bands for short range surveillance with high accuracy but subject to moderate weather effects [27].

Mode	**Short Code**	**Definition**	**Characteristics**
Target Acquisition	TA	The target acquisition mode with less range resolution of the search mode but with higher accuracy to obtain a stable track on a target with more precise 3D measurements (range, velocity, angle). The acquisition involves the target detection based on the pulse integration and SNR to achieve a probability of detection with a given probability of false alarm. When the desired probability of detection is achieved lock-on is achieved that results in the transition to the tracking mode [27].	• Search in a given limited coordinate area where the target is located, • acquire smaller targets at greater ranges in contrast to search radars, • multi function radar capable of acquiring the target, measure the 3D coordinates, tracking and identification, • high sensitivity and complex waveforms to distinguish between targets and allow for better identification, and • normally operating frequency ranges in the S-, C-, and X- bands [27].

Mode	Short Code	Definition	Characteristics
Target Tracking	TT	The target tracking mode is switched from the acquisition mode when the 3D coordinates and trajectory parameters of the target are observed at a sufficient level to allow for the tracking mode to keep an automatic lock-on on the target [27].	• narrow pencil beam of a few degrees, • frequency bands from S-, C-, and X- bands for long range tracking subject to moderate weather effects to $\mathrm{K_u}$- and $\mathrm{K_a}$ bands for short range tracking in clear conditions, • this mode also indicates that the weapon system is being aimed at the platform, • medium and high PRF, • uses pulsed Doppler techniques to obtain four coordinates, which are the 3D coordinates with radial velocity to allow for better clutter rejection, reduced vulnerability to EA and maintain track even with low SNR, and • use of filters such as the Kalman filter to predict platform trajectory [27].

Mode	Short Code	Definition	Characteristics
Missile Guidance	MG	Missile guidance mode is the target tracking mode when the weapon system is active or firing. This mode indicates when the radar is either firing or steering the missile or anti aircraft artillery (AAA) guns towards the platform [27].	• This mode encompasses the fire control and missile guidance radars, and • the tracking mode is active to track the platform and missile where guidance commands are then computed and transmitted to the missile [27].

Assessing these modes and determining their lethality to the platform requires threat assessment analysis. Threat assessment is defined as an "expression of intention to inflict evil, injury, or damage. The focus of threat analysis is to assess the likelihood of truly hostile actions and if they were to occur, project possible outcomes" [28].

There exist multiple types of threat assessment algorithms. These threat assessment algorithms differ from data fusion [28–31], statistical and Bayesian techniques [32–34], to decision analysis and analytic based hierarchy, and more recently the use of advanced artificial intelligence (AI) techniques (knowledge-based systems, fuzzy logic, artificial neural network (ANN), and genetic algorithms) [34].

The jamming profiles of all the active threats in the channel are merged to form an intermediary time-interval jamming profile. The jamming pulses from the intermediary jamming profile are either unobstructed or overlap with each other. The standalone jamming pulses are automatically added to the overall time-interval jamming profile. However, measures need to be taken to determine which jamming signal to consider in a jamming coincidence. This requires threat assessment to be incorporated with ranking and only during coincidence.

Jamming selection for a coincidence can be viewed as a scheduling with conflicts problem, where multiple jobs in a time-frame are in conflict with each other but they cannot be scheduled concurrently [35]. The scheduling with conflicts problem is in the majority of occasions the consequence of resource constraints. The resource constraint for the TIJ controller is the single output channel per jamming band. This can create a cumulative demand on the jammer to transmit multiple jamming pulses simultaneously. However, only a single pulse can be chosen in a jamming coincidence [35].

Even with the constraint of possessing only a single jamming channel per frequency band, the TIJ has to keep the jamming effectiveness high enough to inhibit detection over all the active threats. Thus it is required to select the best possible pulse in a coincidence situation with the input information available. Various methods exist to solve scheduling conflicts. Scheduling methods such as conflict graphs, mutual exclusion scheduling [35, 36], the greedy algorithm [35], central processing unit (CPU) priority scheduling, gang scheduling exist to prioritise tasks.

However, these methods either require parallel processes or are able to shift jobs around. Each pulse in the coincidence needs to be observed in conjunction with the other affected pulses, to select the most vital jamming pulse. Thus the pulses in the coincidences should be prioritised and ranked.

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 selects the appropriate jamming technique to cope against the most lethal 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].

The threat evaluation technique closely related to determine the danger of a mode in close proximity of time with the use of multiple factors and parameters is that of [31]. A countermeasure strategy was developed for the implementation of different types of jamming techniques that can be used against multiple threats. These threats are prioritised on a time interval to time interval basis according to the danger they pose to the platform. Different countermeasures in different channels are allocated to each threat to minimise the lethality they pose. The optimised equation that [31] proposed is

$$D_n = P_n \left[W_s S_n + W_a A_n + W_t \left(1 - T_n\right) + W_n \left(1 - N_n\right) \right], \tag{2.60}$$

where

- D_n is the danger value of threat n,
- P_n is the probability of encountering the threat in the current time interval,
- S_n is the radar mode,
- A_n is the range adjusted accuracy,
- T_n is the projectile time, in hours, from the threat to the platform,
- N_n is the next change of radar mode measured in seconds, and
- $W_{s,a,t,n}$ is the weights of the parameters.

These parameters relate in a relative sense to the requirements of threats and their respective pulses in a coincidence. Each pulse in the coincidence originates at a threat that is located at a certain distance from the platform and emits at a certain mode with a set of signal detection criteria optimised to detect the platform. The platform is also within a certain distance outside or inside the lethal range of the threat radar's weapon system. Taking this into account (2.60) should be more closely reconfigurable to propose the next step in smart noise jamming to fit the need of the TIJ in coincidence.

2.6 SUMMARY

As stated coincidence in noise pulse jamming causes intermittent jamming. No matter how many jammer channels an EA system consists of coincidence will exist meaning intermittent jamming will occur. Therefore to determine a new jamming controller that can counter multiple radars a theoretical understanding of the coincidence rate and threat radar's range and signal detection calculations are required to calculate the noise energy required to inhibit detection from a coherently integrated CPI.

However, there is a likelihood that the waveform characteristics change between modes of a radar. Therefore the jammer should be able to adapt to the changing modes as higher modes pose more risk to the platform. Various threat assessment techniques exist that are used to determine the lethality of threats. Thus a jammer should measure the threat's risk towards the platform as well as determine the jamming effectiveness, thereby making sure the correct jamming pulse in a coincidence is selected for transmission.

CHAPTER 3 METHODOLOGY

3.1 OVERVIEW

This chapter will provide a comprehensive solution to both intermittent jamming and threat evaluation and prioritisation. The methods discussed here will rely on the interleaving technique to move from jamming pulse to jamming pulse in the time domain. Threat evaluation will only be determined in a coincidence situation as standalone jamming pulses will always be selected. Historic information of the previously transmitted jamming pulses and missed pulses is used to provide information for the evaluation technique for the following jamming pulses. The methodology will show that intermittent jamming provides a solution to coincidence rather than being an obstacle.

Furthermore, the threat evaluation and prioritisation technique will be discussed. This evaluation and prioritisation technique is defined as the mode assessment calculation due to the possibility of each radar mode of operation of each threat consisting of different waveforms. Different radar characteristics will result in a change in range measurements and the jamming percentage calculation. Higher modes have the risk of initiating weapon systems integrated into the threat radar.

3.2 M-OF-N JAMMING

For successful jamming where the detection of the target is inhibited a specified amount of jamming pulses have to be transmitted against a radar using a CPI of size n_p to decrease the SNR below the radar's probability of detection. Therefore the jamming pulses should also be grouped into pulse trains of the same size as the opposing radar's CPI. Thus the jamming CPI is the same size n_p as that of the radar's CPI, consisting of n_s standalone pulses and n_c coincidence pulses

$$n_p = n_s + n_c. \tag{3.1}$$

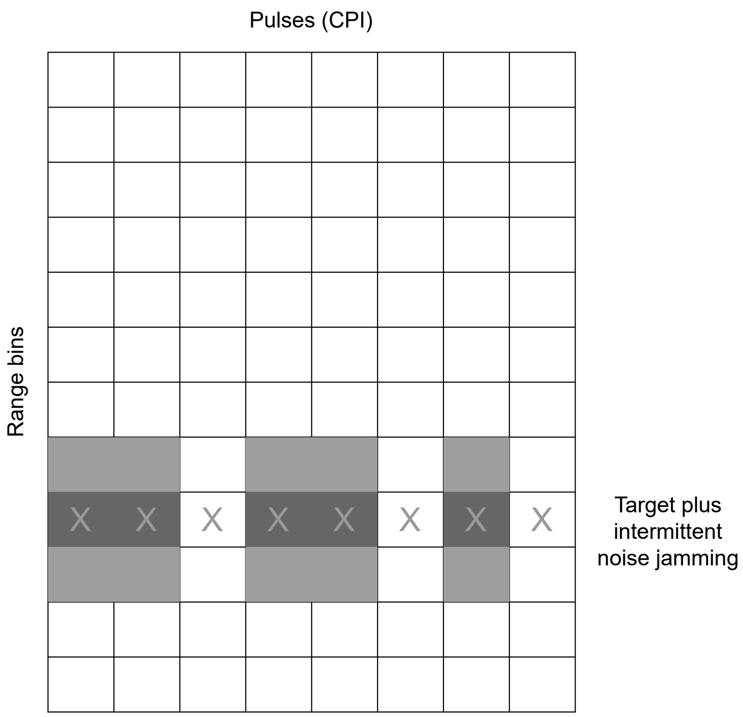


Figure 3.1. Implementing intermittent noise jamming in a CPI.

Intermittent jamming only occurs where jamming coincidence exists. As there exists a possibility that a higher priority threat radar signal will be present. This will result in not every pulse being jammed in the CPI as shown in Figure 3.1

However, the noise jammer does not need to target every single pulse in the CPI. The jammer only needs to transmit n_j pulses to suppress detection to a minimum probability of detection far below what the radar requires it to be. The TIJ will allocate more jamming pulses than necessary which provides a buffer when any error in the transmission or jamming waveform occurs. The minimum probability of detection values as shown in Table 3.1 assures that enough intermittent jamming pulses transmitted will keep the probability far below the threat's required probability of detection and inhibit detection, without knowledge of the CPI's starting pulse [37]. The minimum probability of detection ensures that even if fewer than the required jamming pulses have been transmitted that the threat's probability of detection will still be lower than the required rate. Minimum probability of detection provides assurance to maintain a low probability of detection even against threats utilising cumulative probability of detection, which tries to detect the threat a minimum amount of times over multiple scans.

The minimum probability of detection values in Table 3.1 has been chosen to keep the threat's

Table 3.1. Radar probability of detection versus the minimum required probability of detection to be achieved by the jammer.

Radar P_d	**Minimum P_d**
0.9	0.3
0.8	0.2
0.5	0.1

probability of detection very low. These values have not been chosen from any known tests or data but have been selected to measure the performance of the TIJ when more than the required jamming pulses are required to be transmitted per CPI. If the TIJ only attempts to lower the probability of detection just below the required rate, a high rate of detections will most definitely occur over a high coincidence rate.

Attempting to decrease the probability of detection to a far lower value than what the threat radar requires provides the jammer with a larger error rate of misses. It is accepted if the jammer misses some of the required pulses with such a low probability of detection as detection will still be lower than required. All of the pulses from the CPI and intermittent jamming pulses will be integrated as shown in Figure 3.2 to determine the detectability factor.

The total intermittent jamming pulses are dependent on the average jammer transmit power over the CPI

$$P_{ij} = \frac{1}{n_p}\sum_{n=1}^{n_j} P_n. \tag{3.2}$$

Substituting P_j with P_{ij} in (2.56) will provide intermittent jammer power over the CPI. As opposed to smart jamming changing the power level from pulse to pulse, intermittent jamming requires the maximum jamming power output for the required pulses. This will decrease the number of pulses needed to counter as opposed to smart jamming where most to all pulses are countered but at varying power levels.

The detectability factor of the CPI with intermittent jamming present can be calculated from rearranging (2.59) to

$$D_x(n) = \frac{(P_{av}t_f)G_tG_r\lambda^2\sigma F_t^2F_r^2}{(4\pi)^3R_{P_d}^4(kT_s+kT_j)L_tL_\alpha}. \tag{3.3}$$

The minimum required probability of detection of the threat radar due to interference can then be calculated using (2.48). The n_j pulses in (3.2) shall be increased until the detectability factor in (3.3) is equal to or below the required probability of detection for jamming necessary for efficient jamming.

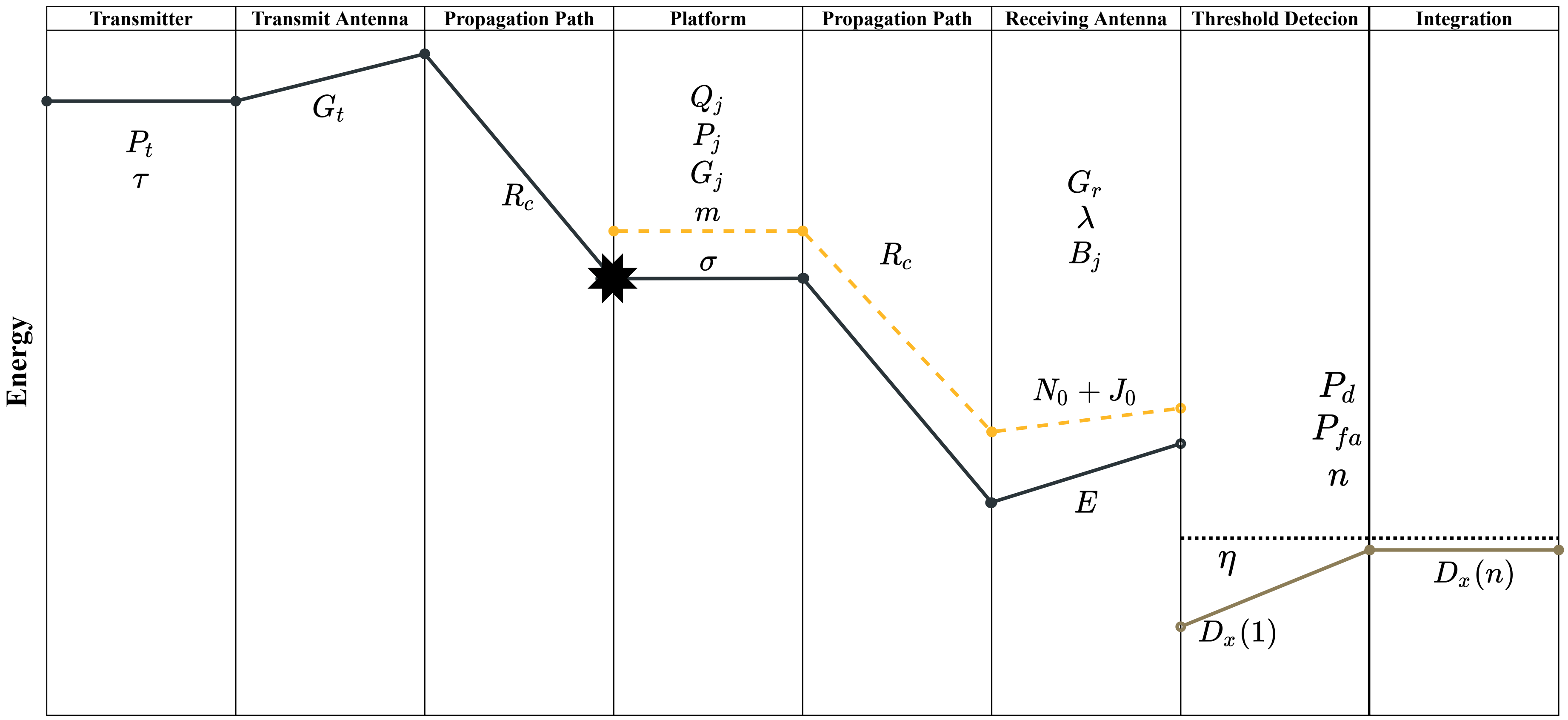


Figure 3.2. Signal and Intermittent jamming plus noise energy loss and gain diagram.

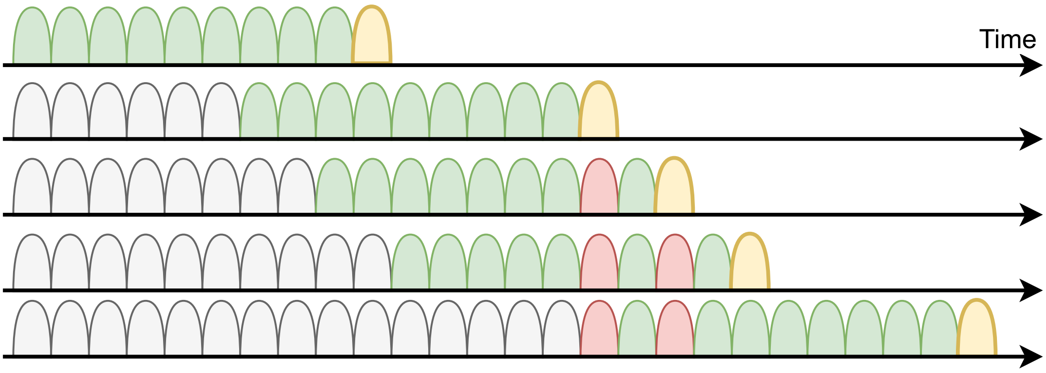


Figure 3.3. Implementation of backward CPI analysis.

The TIJ controller has no indication of when a CPI starts. Moreover, the TIJ cannot decide which pulse may be the start of the new CPI. This will cause an imbalance as the jamming pulses over the real CPIs will differ. Therefore the TIJ has to accept that every single pulse may be the start or end of the CPI.

Two analysis techniques can be used for the jamming effectiveness against a CPI. These are the forward analysis technique and backward analysis technique. The forward analysis looks at each pulse as the start of a CPI. It determines how many pulses are standalone and how many are in coincidence. From this, it knows if the jamming pulse should be selected or not. However, with this technique, the assessed pulse is disregarded when the sequential pulse gets assessed.

The other technique is backward analysis. The analysis of the CPI for the TIJ will rule that each pulse is the last pulse of the CPI. Figure 3.3 provides an example of backward CPI analysis. The yellow pulses are the current jamming pulses in coincidence, the green pulses are transmitted jamming pulses, and the red pulses are the disregarded jamming pulses. As in forward analysis, backward analysis also determines how many jamming pulses were transmitted and how many were disregarded. This will indicate the necessity to transmit the current jamming pulse. The benefit of backward analysis is that it allows for the repercussion of selection or rejection to affect the sequential pulses until $n_p + 1$ pulses have passed. Therefore backward analysis will be accepted as the CPI analysis technique.

After calculating the required n_j pulses it is necessary to determine how many of the jamming pulses of the total CPI will be standalone jamming pulses and how many in coincidence. This is stated as a jamming percentage. Determining the jamming percentage of the ith radar, J_i, is calculated by first checking the resultant n_{j-s}

$$n_{j-s} = \begin{cases} 0, & \text{if } n_j \leqslant n_s \\ n_j - n_s, & \text{if } n_j > n_s \end{cases}. \tag{3.4}$$

This resultant determines if the standalone pulses n_s are equal to and more than n_j then n_{j-s} will be set to 0, or if n_s is less than the n_j, where the results will be the difference between the two values.

The jamming percentage can then be determined as the difference between n_j and n_s over the total pulses in coincidence in the CPI n_c

$$J_i = \frac{n_{j-s}}{n_c}, \tag{3.5}$$

which calculates the percentage pulses required from the coincidences to inhibit detection.

The jamming percentage is dependent on the radar and noise jamming equations, as these factors influence the power of either the radar signal or noise pulse. Changing the value of a parameter will affect the number of noise jamming pulses required in a CPI. This is also true for the signal processing variables if either the probabilities or the CPI size changes.

3.3 ZONE ASSESSMENT

Zone assessment represents the distance between the platform and threat radar. The zone assessment is comprised of the current platform to jammer range (R_c discussed in Section 2.4), maximum detectability range of (2.53) and the burnthrough range of (2.59).

The zone assessment is dependent on the mode type of the radar. As the radar modes change in a threat system so does the ranges due to the mode-specific SNR, probability of detection and false alarm, and the waveform characteristics. Each radar mode will produce a new set of maximum and burnthrough range values [19]. This will immediately change the zone assessment value of the threat system.

The maximum detectable range and burnthrough range provide a zone where a platform can traverse and provide adequate jamming capability. Figure 3.4 provides a graphical view of what should be expected when a platform enters a threat radar zone. Figure 3.4 illustrates the change in jamming capability of the platform, where the green area allows for effective

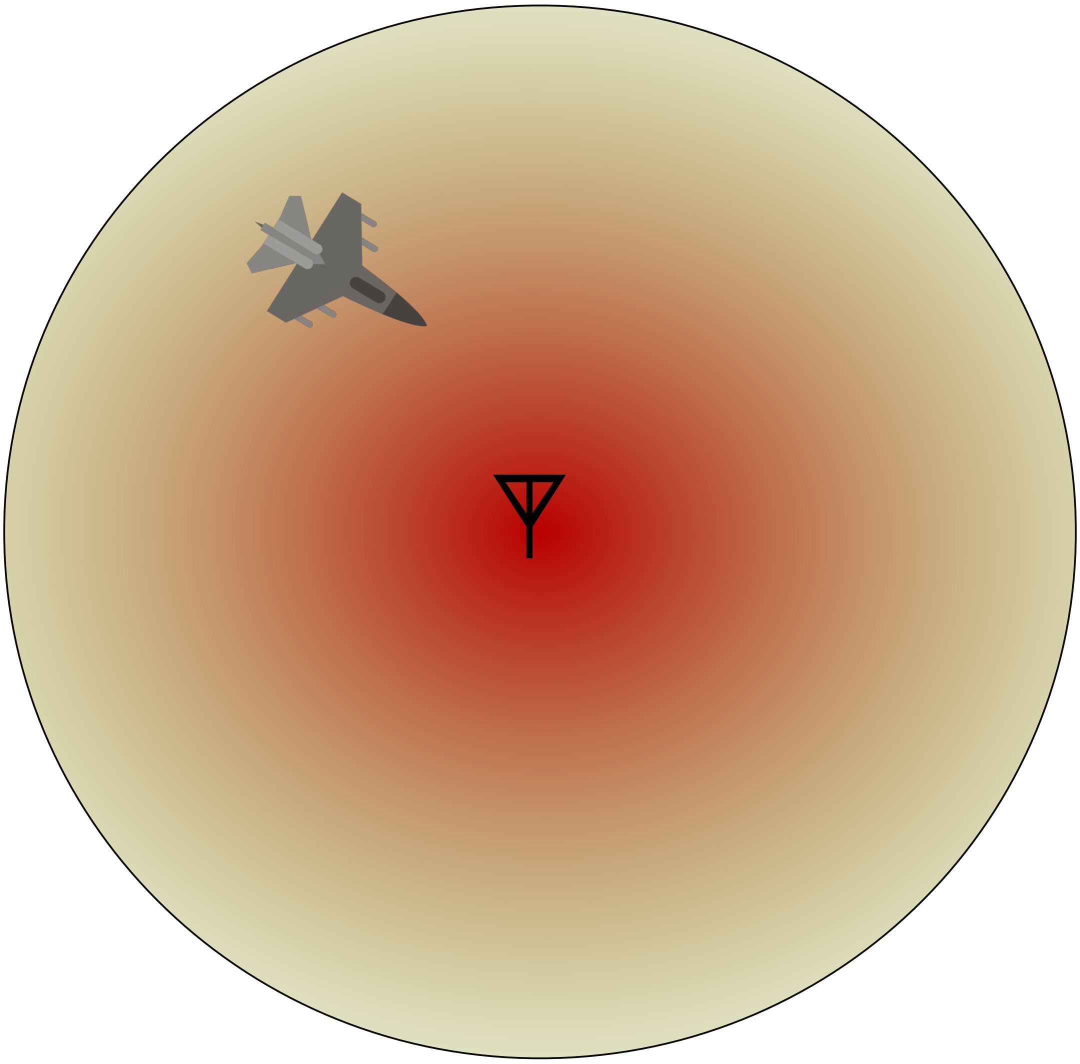


Figure 3.4. Representation of the change in emitting threat radar signal strength.

jamming and the red area shows burnthrough range where the threat radar SNR is high enough that no jamming signal can hinder detection. Possessing knowledge of the location of the emitting threat, the incident power at the platform, the maximum probability of detection, and the parameter values used in the radar range equation allows the TIJ to identify the range radii zones.

The zone assessment is a fairly simple algorithm. Figure 3.5 shows the zones and ranges that are used to determine the zone assessment system. The maximum detectable range, R_m, and the burnthrough range, R_B, is used as the outer and inner zone of the zone assessment calculation respectively. The zone assessment value of the ith radar, Z_i, ranges from $0 \leq Z_i \leq 1$, where $Z_i = 0$ is at the maximum detectable range and $Z_i = 1$ is at the burnthrough range of the threat radar. If the platform is moving outside the maximum detectable range the zone

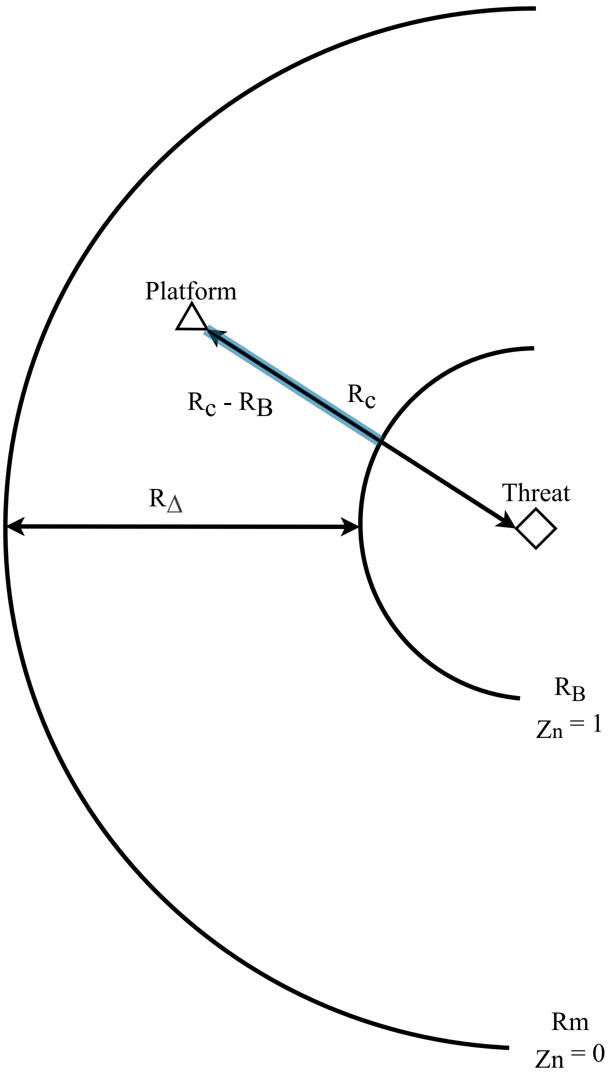


Figure 3.5. Description of zone assessment zones and ranges.

assessment value will always equal 0. When the platform is moving between the burnthrough range and threat radar location the zone assessment value will always equal 1.

The ranges required to calculate the zone assessment value are the range between the platform and threat indicated as the current range, R_c, the delta range, R_Δ, which is the difference between the maximum detectable range and the burnthrough range, $R_\Delta = R_m - R_B$, and the difference of the current range and the burnthrough range.

The zone assessment value, Z_i, is determined as

$$Z_i = \frac{R_\Delta - (R_c - R_B)}{R_\Delta} \text{ where } Z_i = \begin{cases} 1, & \text{if } R_c < R_B \\ 0, & \text{if } R_c > R_m \end{cases}. \tag{3.6}$$

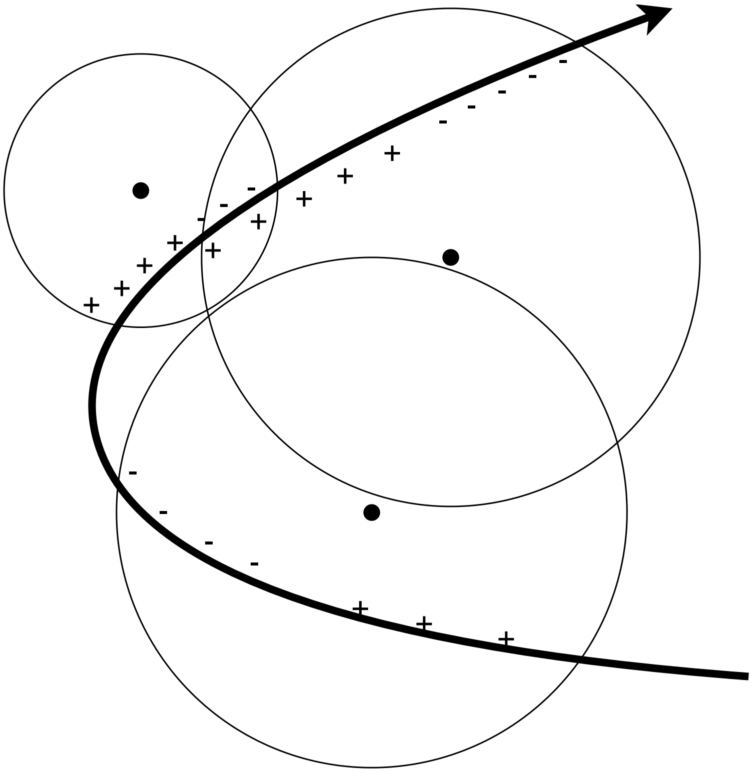


Figure 3.6. Zone assessment value change of multiple threat radars over a flight path.

As seen in Figure 3.6 the zone assessment value will change for each threat as the platform flies closer to and further away from the threat radar systems. The zone values will change as the platform analyses the collected incident waveforms transmitted from the threat system during look through. The ranges will change and the zones shift depending on the triangulation measurements.

3.4 MODE ASSESSMENT

The focus of analysing the modes of operation is to monitor the change of lethality the threat poses to the platform. Mode assessment is derived as a threat assessment monitoring the change of the radar mode and its impact on the platform. Without the mode assessment system, the TIJ and platform will not be able to keep up to date with each active threat's behaviour. This will blind the platform of any detrimental actions of the threats and prevent the TIJ system from making proactive decisions.

The TIJ controller only takes into consideration known threat radars that are defined in a threat library. This entails that the library expert has a certain amount of knowledge of each defined threat radar. The mode assessment requires input from the expert on each of the radar modes available to the threat radar. The TIJ controller is mostly a predictive and statistical system.

Using inputs from an electronic intelligence (ELINT) (expert) adds restrictions to the TIJ controller. This acts as a prevention mechanism for the TIJ to not diverge to an error state, thus the mode assessment should be modular and interchangeable to allow for different types of threat assessment algorithm to be used depending on the expert's set of requirements.

The mode assessment system parameters rely on what the expert deems necessary. Some of the parameters that may be required are:

- the radar modes,
- the zone assessment values,
- the presence of weapon system with a known range, and
- the percentage jamming of intermittent jamming.

The mode assessment uses this information to determine the threat assessment algorithm. The mode assessment value must be normalised as it is used in the threat ranking to be compared against other threat radars comprising of other system parameters and TIJ values. This will ensure that when an algorithm changes that the interface to the threat ranking is not compromised.

With some alterations and tweaking any of the threat assessment techniques in Section 2.5 can be used in the TIJ. However, the peer-reviewed evaluation technique from [31] is chosen for the detail in the information available, simplicity of the equation, and the parameters used in the equation that is similar to the information discussed in this dissertation.

The parameter P_n in (2.60) will always be set to 1.0 as the threat radar will always be present in the duration of the flight. Therefore the parameter can be removed from the equation.

The threat's actions or behaviour observed by the platform will be primarily on the change in radar mode. The radar mode parameter S_i will stay close to the same as was used initially. Each mode will be given a constant value between 0 and 1 to indicate the lethality of the mode against the platform. The radar modes classified in the dissertation are target search, target acquisition, target tracking and missile guidance. The following values for each mode of operation are given to indicate the danger it poses to the platform. These values are configurable by the user.

The search mode is given the lowest value of 0.25 to show that the radar is searching for targets. Search mode translates to the beam scanning over the platform, however, due to the constraints in the dissertation, the beam will be fixed on the platform. Thus, it is highly likely that the radar has detected the platform and is busy identifying/verifying before transitioning to the next mode stage.

The acquisition mode is given a value of 0.5. The mode has detected the target and is now attempting to narrow the location of the platform. The quality of the location measurements depends on the quality of the signal at the range gate. The more precise the location measurements become the close the radar is to lock on to the platform.

The next two stages are highly lethal to the platform. The target tracking mode is given a value of 0.75. A narrow tracking beam is locked onto the platform and the radar knows precisely the location, angle and range of the platform. Here the EW system must do as much as possible to break the lock and attempt to get the radar to revert to acquisition.

The last stage is the most lethal radar mode. The missile guidance mode is given a value of 1.0. Here lock-on and tracking have proceeded long enough that the weapon system can be used to eliminate the target. The path to the target is calculated and weapons like missiles or self-propelled anti-aircraft gun (SPAAG) are guided towards the target by the radar.

W_aA_n will be replaced with the zone assessment value Z_i determined in (3.6). TIJ does not care for the range adjusted accuracy of the weapon system in this dissertation, as the threat lethality range is currently the only parameter of the threat's weapon system taken into consideration. All the other factors and parameters are about the threat radar signal and detection characteristics. Thus the zone assessment value is important to the TIJ as it will indicate where the platform is relative to the threat's radar detection range. The Z_i will result in the threat evaluation value changing in the duration of the flight as the platform manoeuvres in the environment.

The value $W_t\left(1-T_n\right)$ will be changed to L_i which is a binary weapon system lethal range indicator value. L_i will indicate if the platform is outside (0.0) or inside the lethal range (1.0). Such a high value is used when the platform is inside lethal range to increase the priority level. An increased priority level inside the burnthrough range indicates to the TIJ that it is necessary to keep the threat mode as low as possible and prevent radar to change to a more lethal mode such as target tracking or missile guidance, which will activate the weapon system and target the platform. It does not matter if the weapon system is active or not, only that the platform is traversing in a very dangerous area. L_i will result in the threat evaluation value changing as the platform moves in or out of the lethal range.

$W_n(1-N_n)$ implemented is used to determine the jamming effectiveness against the threat and if the threat is close to changing mode. Jamming effectiveness is measured on the CPI level due to the fact that TIJ measures each CPIs independently. Therefore, resulting in J_n to be replaced with the jamming percentage value, J_i determined in (3.5).

These changes results in the mode assessment equation

$$M_i = \begin{cases} 0, & \text{if } L_i = 0 \text{ and } J_i = 0 \\ W_s S_i + W_r Z_i + W_l L_i + W_j J_i, & \text{otherwise} \end{cases}, \tag{3.7}$$

where, M_i is the mode assessment value of threat i, S_i is the radar mode, Z_i is the zone assessment value, L_i is the weapon system lethal range indicator flag, J_i is the CPI jamming percentage, and $W_{s,r,l,j}$ is the weights of the parameters.

All four of the variables, S_i, Z_i, L_i, and J_i, are normalized. The sum of the weights should equal 1 to provide a mode assessment value between 0 and 1 for all threat radars.

3.5 THREAT RANKING

Ranking is only necessary when multiple jamming pulses are in coincidence. The mode assessment equation of (3.7) is used to calculate the priority of each jamming pulse in a coincidence. The jamming pulse with the highest mode assessment priority value is selected to be transmitted. The pulses that do not overlap with the highest priority pulse will then be compared (only if any non-overlapping pulses exist), where the highest priority non-overlapping pulse is selected. All the pulses that overlap the current highest priority non-overlapping pulse are disregarded and the cycle will repeat, until all of the non-overlapping pulses have been compared and the highest non-overlapping pulses selected. Thus the jamming pulses selected to be transmitted in a coincidence are the highest priority pulse and the highest priority non-overlapping pulses.

An example of how jamming pulse selection works in a coincidence is shown in Figure 3.7.

Table 3.2. The mode assessment values calculated for each pulse in the example coincidence of Figure 3.7.

Jamming Profile	Pulse	Mode Assessment Value
1	1	0.32
2	2	0.83
	3	0.86
	4	0.89
3	5	0.63
	6	0.64
	7	0.65
	8	0.66
	9	0.67
4	10	0.87

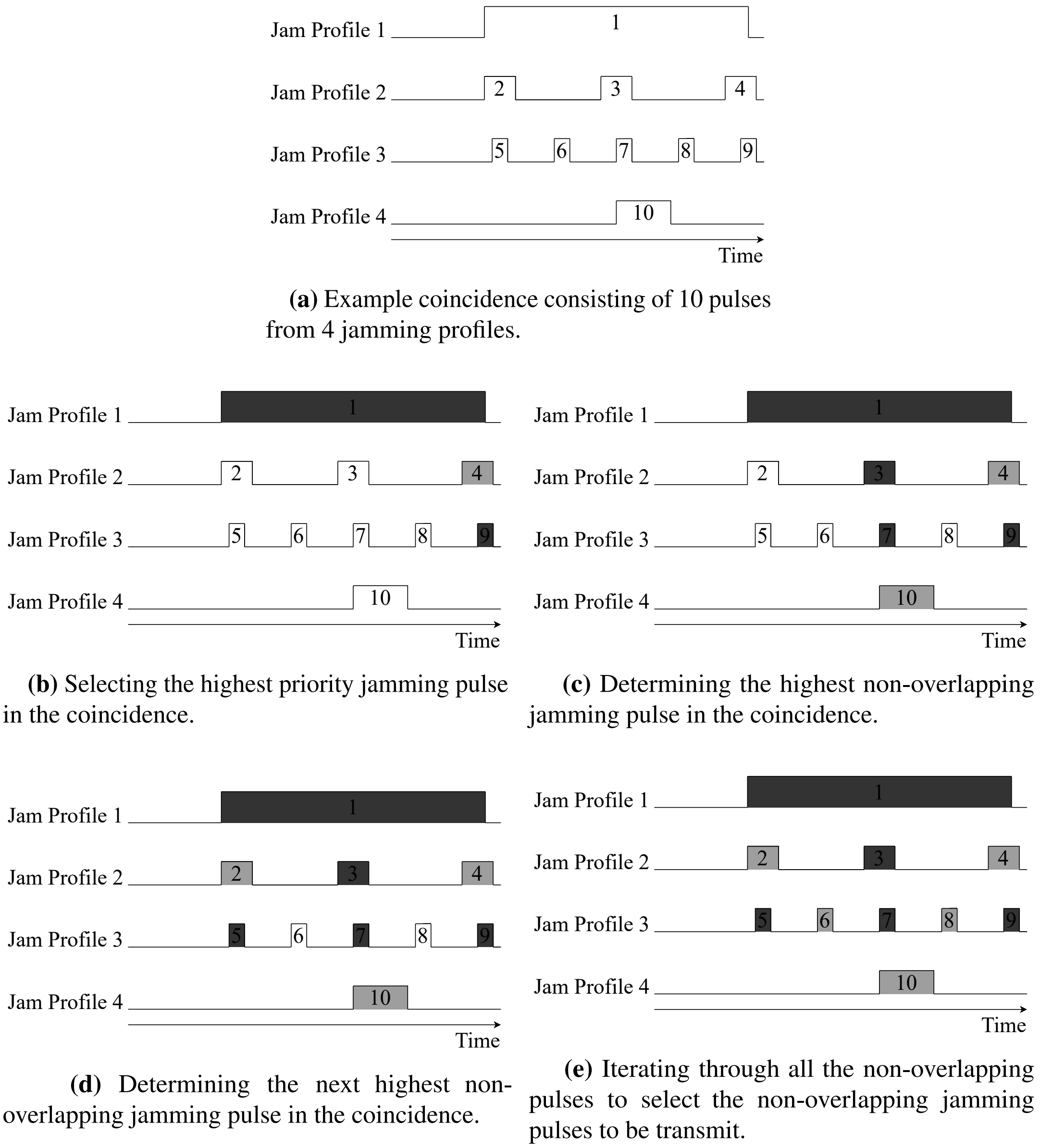
The coincidence as seen in Figure 3.7(a) consist of 10 jamming pulses from 4 jamming profiles with the mode assessment value of each jamming pulse shown in Table 3.2.

As seen in Table 3.2 the overall highest priority pulse with the highest mode assessment value is pulse 4 from jamming profile 2. Selecting pulse 4 will result in pulse 1 from jamming profile 1 and pulse 9 from jamming profile 3 to be disregarded as shown in Figure 3.7(b). The non-overlapping pulses are then pulse 2 and 3 from jamming profile 2, pulse 5, 6, 7, 8 from jamming profile 3 and pulse 10 from jamming profile 4.

Selecting all of the non-overlapping pulses to be transmitted is an iterative process. As shown in Figure 3.7(c) and Table 3.2 the non-overlapping pulse with the highest mode assessment value is jamming pulse 10. Jamming pulse 10 will be selected which result in pulse 3 from jamming profile 2 and pulse 7 from jamming profile 3 to be disregarded which leaves pulses 2, 5, 6, and 8 to be ranked.

Pulse 2 from jamming profile 2 is the next highest priority pulse as seen in Figure 3.7(d) and Table 3.2. Pulse 5 will be disregarded which will leave only pulses 6 and 8 to be ranked.

From Figure 3.7(e) and Table 3.2 it is seen that jamming pulse 8 and then jamming pulse 6 will be selected with no other pulses overlapping either of them. Thus in the example coincidence pulses 2 and 4 from jamming profile 2, pulses 6 and 8 from jamming profile 3 and pulse 10 from jamming profile 4 will be selected to be transmitted.



(a) Example coincidence consisting of 10 pulses from 4 jamming profiles.

(b) Selecting the highest priority jamming pulse in the coincidence.

(c) Determining the highest non-overlapping jamming pulse in the coincidence.

(d) Determining the next highest non-overlapping jamming pulse in the coincidence.

(e) Iterating through all the non-overlapping pulses to select the non-overlapping jamming pulses to be transmit.

Figure 3.7. An example of ranking and selection of jamming pulses in a coincidence to be transmitted.

The parameters in the mode assessment equation are chosen to prevent constant selection of the most lethal threats or the jamming pulse with the highest jamming effectiveness at every coincidence but to spread the jamming allocation over all of the active threats in the channel.

Note that if the platform is outside of the lethal range and the minimum amount of jamming pulses required to lower the probability of detection to an acceptable level for jamming then the mode assessment value will be set to 0 and the pulse can be disregarded in the coincidence.

While the platform is in the lethal range it is safer to keep on determining the mode assessment if $J_i = 0$. The TIJ has to keep the mode of operation as low as possible to prevent the threat from reaching missile guidance.

3.6 SUMMARY

Threat situational awareness, m-of-n jamming analysis, jamming pulse prioritisation and allocation are discussed in this chapter to form the mode assessment calculation. The mode assessment equation (3.7) is dependent on the current mode of operation, the zone assessment value, the knowledge of the platform is inside or outside the lethal range, and the jamming percentage value of the current pulse in coincidence. Unobstructed jamming pulses are transmitted without hindrance, but in a coincidence situation, the mode assessment calculation will have to determine the highest priority jamming pulse. Each coincidence jamming pulse will be provided with a priority value used to prioritise and select the highest priority pulse.

The zone assessment equation determines and normalises the location between the threat radar and the platform. The zone assessment value for each threat radar is determined from (3.6). The range value is used to evaluate the platforms range in regards to the threat radar's maximum detectable range and burnthrough range.

For successful jamming where the detection of the target has to be inhibited, a specified amount of jamming pulses have to be transmitted against a radar using a CPI of size n_p to decrease the SNR below the radar's probability of detection. The total jamming pulses n_j is determined from (3.2) and (3.3) to determine the number of jamming pulses required to lower the probability of detection to a minimum value. The jamming percentage equation (3.5) indicates how many of these required jamming pulses are in coincidence.

CHAPTER 4 RESULTS

4.1 OVERVIEW

This chapter will show how the change in the mode assessment parameter selection and weights, jamming window size, and error estimations influence the TIJ effectiveness at countering multiple active radars, the rate of coincidences, and the number of pulses in a coincidence. A scenario has been crafted to incorporate various radars with varied waveform and signal detection characteristics and placed at different distances, to the platform flight path, to measure the performance of the TIJ. This provides an effective mechanism to test how the TIJ will respond against radars close to the calculated maximum range, the burnthrough range, high and low duty cycles, large and short pulse widths, and varied signal detection probabilities and CPI sizes.

4.2 TESTING CONDITIONS AND CONSTRAINTS

The simulated jamming system is a heuristic to display the functionality of the TIJ controller on a self-protection jamming platform. As indicated it is assumed that a theoretical PRI tracker is used as ES does not form part of the hypothesis, therefore the parameters of the collected signals received will be ideal as there will be no inaccurate timing predictions. The jammer will transmit the precise jamming signal characteristics at the intended time with the intended duration in the main beam of the threat radar. However, it will be fruitful in future research to investigate the effectiveness of the TIJ system when less than ideal information is presented, as what can be expected in the real world.

The TIJ will be tested through the use of a simulation that consists of a main interval loop function and three processing functions within the main loop. The three processing functions consist of the interval coincidence calculator, the interval coincidence sweeper, and the interval threat radar evaluator.

The main function loops through each time interval, where the total time intervals are determined from the flight path and velocity of the platform. Each jamming interval time will be one second long, where only known pulse radar signals are encountered. The interval coincidence calculator determines and stores the coincidences with the pulses associated. The list of coincidences is processed by the interval coincidence sweeper that determines the high priority pulses at each coincidence depending on the threat evaluation and prioritisation technique employed.

Lastly, after processing the interval the total pulses in each CPI jammed and the total pulses required to be jammed in each CPI is calculated for each threat. This will indicate if the mode of operation for the threat has to either move up or down. The post-processing time is independent of the jamming intervals in the simulation. The platform only needs to be detected by a single CPI in an interval for the radar to move up to the next mode. Thus the jammer is required to successfully counter every CPIs in the interval. Moreover, the jammer has to counter each CPI without the knowledge of when a CPI starts.

The simulation consists of platform, jammer, and threat parameters and characteristics. The platform flightpath is dependent on the 3D Cartesian coordinates and velocity all of which are user-configurable. The RCS of the platform is set at 3 m^2.

The jamming features are in line with jammer systems currently in production bar the antenna and channel capabilities [4, 38]. A single noise jammer is in operation, where the noise jammer consists of a single channel connected to directional antennas, with a gain of 10 dB, all pointing directly in the main beam of the threat radars. Cover noise jamming will be used as stated in [1] for smart noise jamming. The jammer will transmit at a maximum output power of 200 W (53 dBm) with a jamming bandwidth of 50 MHz larger than the bandwidth of the signal pulse. As specified in Section 2.3 the frequency range will be from 1 to 10 GHz (Bands D to I).

The simulation will consist of a total of 20 threats, details of each radar can be found in Table A.1 in Addendum A. Each radar consists of target search (TS), target acquisition (TA), target tracking (TT) and missile guidance (MG) modes, where each mode will differ in radar waveform and detection parameters. However, the antenna type of every mode will represent that of a tracking antenna, thus no search radar calculations will be used. Basic PRF patterns will be used as the dissertation does not take into consideration PRF techniques such as jitter and stagger patterns. As discussed in Section 2.3.1 the radars will implement coherent integration. Another advantage for the threat radar is that the jammer does not know when a CPI starts for a threat radar.

The missed pulses in Table A.1 refer to the pulses missed by the jammer before the start of the interval. The missed pulses may be due to the radar still attempting to identify the threat mode during lookthrough or that the mode changed before lookthrough occurred. The missed pulses will equal zero if the mode stays the same for the next interval. This is only used to provide added strain to TIJ to provide the capability of jamming effectiveness.

4.3 TEST SCENARIOS AND RESULTS ANALYSIS

This section consists of the test scenarios, results and discussion. These three sections are normally separated but for this dissertation are merged into one as each test depends on the results of the previous test. The discussion of each result is presented at each test as each test interlinks with the next test. The TIJ is tested on the mode assessment parameter variability, the preferred jamming window size, effectiveness against multiple threats, and the effect of error in the estimations of the signal detection characteristics i.e. CPI size, probability of detection and probability of false alarm.

All of the tests below are executed using the same scenario of Figure 4.1. All of the threats, represented by a red ’X’ symbol, will start at TT and it is up to the TIJ to try and revert the modes to TS. The threats are spaced around the flight path, shown in blue, with the platform in close proximity to the radars. Only the parameters of the TIJ will differ to provide detailed results of its jamming effectiveness.

This scenario was chosen to provide an overall indication of the performance of the TIJ. The TIJ will face several variations of the threat radars characteristics and location placement. It is also important to measure how a threat radar will influence the performance of the TIJ against the other radars.

The platform will be out of lethal range for the entire flight duration for radars 1, 2, 3, 12, 15 and 20. This will measure if the TIJ will ignore these radars when the platform is facing radars inside of the lethal range and if their mode of operation will also be kept as low as possible.

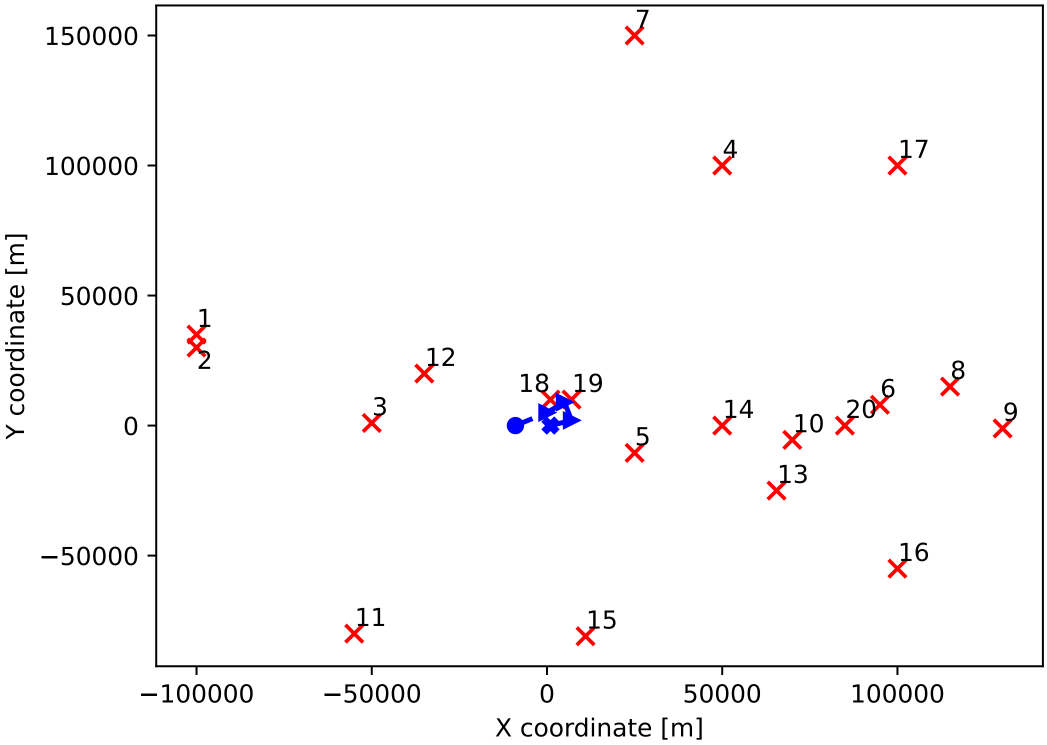


Figure 4.1. Top view of the flightpath and the threat radar locations.

Radars 1, 2, 3, 12, and 15 provides the conditions of measuring the jamming effectiveness and coincidence rate of threat radars, outside the lethal range, with low duty cycles and short pulse widths. However, radar 20's overall duty cycle will be high which will most likely result in a high coincidence rate. Thus allowing the measurement of the jamming effectiveness of a threat with high duty cycles outside the lethal range.

Radars 1, 2, 3, 15 and 20 will have large CPI sizes and detection probabilities to make sure that the TIJ will have to counter a number of pulses in a CPI. Radar 12's CPI is very low with a high detection probability value which will result in fewer pulses to be countered than that of the other radars outside the lethal range.

The platform will be inside the lethal range for the entire flight duration for radars 5, 7, 8, 9, 10, and 17. These radars are spread throughout with some radars like radar 5 being close to the flight path and radar 7 and 17 being further away than the rest.

Radars 5 and 10 provides the conditions of measuring the jamming effectiveness of threat radars, inside the lethal range, with very low duty cycles and short pulse widths. Radars 5 and

10 have high CPI size and probability of detection values, thus these radars will have a high likelihood of detecting the platform even if the average signal power is low. However, short pulse widths will most likely result in low coincidence rates. Thus the TIJ will be tested against threats with low duty cycles inside the lethal range to measure jamming effectiveness.

Radar 9 has a high duty cycle with long pulse widths. This will result in a high coincidence rate as the pulses will be transmitted in short succession from one another which will most likely envelope other jamming pulses. The CPI size and probability of detection is low compared to the other radars which may lessen the number of jamming pulses needed to inhibit detection in a CPI.

Radar 7 has a high duty cycle for TS and TA and a low duty cycle for TT and MG. Thus radar 7 will have more coincidences in the lower two modes and a low coincidence rate in the upper two modes, which may result in the TIJ transitioning between TA to TT. However, the CPI size is very high at TT and MG requiring a large number of jamming pulses to be transmitted. It will still be easier for the TIJ to go from TT to TA, due to the low coincidence rate, but it will be difficult for the TIJ to keep radar 7 at TS and TA, which is necessary when inside the lethal range.

Radars 8 and 17 have low duty cycles but long pulse widths. Almost all of the jamming pulses intended for these two threats will be in coincidence. Both these threats have relatively low CPI sizes however all jamming pulse selections will occur in coincidences. The jamming percentage of these two radars will always be high and result in the other jamming pulses being disregarded. Thus the jamming effectiveness of the TIJ will be tested against threats, where the platform is inside the lethal range, and where all of the pulses will be in coincidence.

The platform will be in and out of lethal range for the entire flight duration for radars 4, 6, 11, 13, 14, 16, 18, and 19. Moving in or out of lethal range will show how well the TIJ responds to these conditions. The TIJ will need to lower a high mode as quickly as possible over the minimum number of intervals when entering the lethal range. It will also show how the TIJ will change the priority of the threat once it left the lethal range and shift priority to threats where the platform is still inside the lethal range.

Radar 16 will consist of a low duty cycle, closely resembling radar 15. The platform will be in the lethal range for radar 16 up until interval 54. Therefore, the TIJ will need to keep radar 16 in the lowest modes for the majority of the intervals.

Radars 6, and 11 have low duty cycles and short pulse widths. Resulting in the likelihood for a relatively high coincidence rate as the jamming pulses will be close to one another The platform will move inside the lethal range of radar 6 at around interval 20 where the platform will stay over the entire scenario duration. The platform will be inside the lethal range for only the first third of the flight duration.

Radar 13 and 14 has a low duty cycle but short to long pulse widths. The coincidence rate for both will be relatively high as there is a chance for most of the jamming pulse to be in coincidence. The platform will be in the lethal range of radar 13 for the majority of the flight duration. The TIJ will need to keep the modes as low as possible resulting in the jamming pulse for radar 13 to be selected in most of the coincidences. The platform will only move in and out of lethal range in the middle part of the flight duration for radar 14. Radar 14 provides the test to determine if the TIJ will keep the modes low when a platform moves quickly in and out of lethal range and what the TIJ will do outside of lethal range.

Radar 4 has a very long pulse width (with regards to the pulse widths of the other radars) resulting in all of the jamming pulses being in coincidence just like radar 8. The platform moves into the lethal range of radar 4 around interval 20 where it will then stay inside of the lethal range. This results in the platform being inside of the lethal range of two radars and almost all of the jamming pulses for both being in coincidence. The TIJ will have to successfully inhibit detection for both these radars as well as the other radars, especially in lethal range.

The platform will be inside burnthrough and lethal range for radar 18 and 19 for several intervals. Radars in burnthrough and lethal range will result in high mode assessment values. These two radars will provide a measure of how the coincidence selection will be negatively affected as radars even in burnthrough are also currently set to be jammed. This will indicate how radars in burnthrough will affect the jamming effectiveness of the other radars and how long it will take to normalise the jamming effectiveness over all of the radars once the platform moves out of burnthrough.

All of the figures of the test results are located in Addendum B. The intervals will start at 0 for the mode heat maps to indicate the starting modes of the threat radars. Interval 1 will show what the modes currently are after the first interval. All of the other heat maps will start the intervals at 1.

4.3.1 Mode assessment evaluation test

The first test determines the effectiveness of the mode assessment technique of (3.7). The weights add variability to the equation. Thus testing is required to determine the effectiveness of the parameters. It is important to know if some of the parameters require a larger weight than the others.

The first two test cases of Test Cases 4.3.1.1 and 4.3.1.2 follow the smart jamming worst threat selection technique discussed in [1]. The type of radar, its mode of operation and location are used to determine the highest priority threat. Therefore the jamming percentage weight W_j is set at 0 to simulate a smart jammer only looking at the parameters from [1]. Test Cases 4.3.1.3 to 4.3.1.5 will detail the changes to the jamming evaluation and prioritisation when the jamming percentage is added.

The jamming signal will be the size of the pulse width of the signal to measure the effectiveness of the mode assessment from the perspective of a perfect noise jammer.

4.3.1.1 Mode and range assessment

The first test case only looks at the mode, S_i, and range, Z_i, of the radar. Two parameters are required as multiple radars in a coincidence may match when utilising only the mode parameter. Therefore, range is utilised as the tie-breaker parameter which will select the threat closest to the platform. The results are visualised in heat maps in Figure B.1.

Radars 4, 6, 8, 14, 18, 19 and 20 have intervals in MG as seen in Table 4.1. However, only radars 4, 6, 8, 18, and 19 have intervals in MG whilst inside lethal range.

Table 4.2 shows that all of the jamming pulses for radar 4 are in coincidence and 95% of the jamming pulses for radar 8 are in a coincidence. The jamming percentage heat map in Figure B.1(c) shows that around half of the jamming pulses in the CPIs for both radars need to be transmitted to prevent detection. Therefore a majority of the required jamming pulses are in coincidence. The high coincidence rate, as seen in Figure B.1(b), is due to the very long pulse width of radar 4 and 8, compared to the other radars in the scenario.

The zone assessment per interval heat map in Figure B.1(d) shows that the zone assessment value is below that of other radars in the same interval. Thus the low zone assessment prevents jamming pulses linked to radar 4 and 8 to be selected at enough coincidences to inhibit detection as there are other jamming pulses for radars that are closer to the platform.

Radar 6 stays in the high modes in the first third of intervals, as it has a high coincidence rate but has a lower zone assessment value than the other radars that it will most likely find itself in a coincidence. The only instances where it is in MG and inside of lethal range is when radar 18 and 19 are in burnthrough thus the chance of jamming pulses for radar 6 being selected is relatively slim within a coincidence.

Table 4.2 show that radars 18 and 19 reaches the burnthrough range which correlates with the maximum jamming percentage value for both radars between intervals 21 and 31. Both of these threats will require every single pulse to be jammed, however, their modes increase at each interval as the platform is continuously being detected by both these radars. Both of the radars are in the lethal range, their modes increase to a maximum and the zone assessment values are also maximum due to the statement in (3.6). This causes a reaction to the other radars which will now be prevented from being selected in coincidences. The other radars will also start to increase in mode due to fewer pulses being selected for jamming. The other radars will be jammed sufficiently over all of their CPIs and revert to lower modes as soon as the platform moves out of the burnthrough ranges of radars 18 and 19.

Table 4.1 and Figure B.1(a) show that radars 7, 14, and 20 transition to TT often, with some going to MG over the course of the flight duration. These radars are all closely related in coincidences per interval rate and the zone assessment value. The pulse widths are also relatively long making the chance of being in coincidence high. The jamming pulses for these radars will be disregarded when in coincidence with radars in a higher mode, which will result in detections as they are not selected in a coincidence up until they also reach a higher mode of operation, where they will then get selected enough times to inhibit detection over the entire interval and drop down to a lower mode of operation. The mode transition cycle will thus repeat over the entire flight duration.

Table 4.1. Mode counter over total intervals and intervals in lethal range when only the mode and zone assessment parameters are being considered.

Radar	**Total intervals**				**Total intervals in lethal range**			
	TS	**TA**	**TT**	**MG**	**TS**	**TA**	**TT**	**MG**
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	34	3	13	16	33	3	2	6
5	64	1	1	0	63	1	1	0
6	37	4	14	11	36	1	4	3
7	38	15	13	0	37	6	3	0
8	30	27	5	4	29	27	5	4
9	59	6	1	0	58	6	1	0
10	64	1	1	0	63	1	1	0
11	46	19	1	0	20	1	1	0
12	64	1	1	0	0	0	0	0
13	48	12	6	0	46	7	2	0
14	16	25	23	2	7	5	2	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	57	5	4	0	56	5	4	0
18	59	3	3	1	48	3	3	1
19	59	3	3	1	47	3	3	1
20	5	6	26	29	0	0	0	0

Radars 1, 2, 3, 5, 10, 12, 15, and 16 goes from TT down to TS where they stay up until the end. Radars 9, 11, 13 and 17 transition mostly between TS and TA with some intervals in TT. This is due to the low jamming percentage and coincidences per interval. There are enough standalone pulses that are being jammed to inhibit detection.

4.3.1.2 Mode, range and lethal range assessment

The second test case adds the lethal range, L_i, binary parameter. This provides significant improvement to Test Case 4.3.1.1 which is seen in Figure B.2 and Table 4.3. Radar 4 transitions between TT and MG however they are not within the lethal range of the weapon system as of yet. However, the number of intervals in MG whilst the platform is inside of the lethal range have decreased significantly. Radar 4 decreased from 6 to 2, radar 6 decreased from 3 to 0, radar 8 decreased from 4 to 1, and radar 19 does not have any interval in MG. Only radar 18 has the same interval still in MG.

Most of the radars transition between TS and TA over the course of the flight duration, but radar 20 provides an interesting observation. As seen in Figure B.1(e) radar 20 never reaches

Table 4.2. Coincidences and zone assessment statistics.

	Coincidences		**Zone Assessment**				
Radar ID	**Mean**	**Median**	**Start**	**Mean**	**Median**	**Min**	**Max**
1	0.591	0.589	0.855	0.846	0.848	0.833	0.861
2	0.59	0.587	0.919	0.845	0.848	0.832	0.919
3	0.616	0.615	0.955	0.962	0.959	0.945	0.977
4	0.999	0.999	0.877	0.83	0.836	0.765	0.921
5	0.578	0.578	0.946	0.949	0.954	0.93	0.967
6	0.833	0.825	0.968	0.973	0.974	0.952	0.981
7	0.854	0.931	0.95	0.924	0.917	0.899	0.963
8	0.955	0.966	0.912	0.942	0.949	0.912	0.957
9	0.819	0.822	0.899	0.916	0.915	0.899	0.934
10	0.687	0.683	0.973	0.969	0.969	0.939	0.978
11	0.805	0.763	0.951	0.827	0.833	0.766	0.951
12	0.691	0.69	0.975	0.943	0.945	0.921	0.975
13	0.869	0.887	0.936	0.91	0.897	0.869	0.946
14	0.922	0.937	0.823	0.859	0.858	0.823	0.896
15	0.686	0.682	0.971	0.952	0.95	0.941	0.971
16	0.698	0.685	0.915	0.926	0.927	0.911	0.932
17	0.95	0.956	0.968	0.971	0.975	0.959	0.982
18	0.607	0.604	0.985	0.984	0.987	0.961	1.0
19	0.676	0.663	0.972	0.944	0.954	0.876	1.0
20	0.905	0.927	0.941	0.947	0.947	0.928	0.958

lethal range which means that it is less likely to be selected in a coincidence. Thus it will most likely be ignored in coincidences when other radars which are inside of the lethal range are also present. This results in radar 20 transitioning to MG and only returning to TT when it is the overall highest mode. However, radar 20 will continue to be in either MG or TT up until all radars are in TS, where it will only then transition to TS as well. As radar 20 is such a low risk to the platform it will move back up to the high lethality modes as soon as the modes of other radars, where the platform finds itself inside of the lethal range, goes up. The other radar modes are of higher importance to get back down than that of radar 20. Proving that adding lethal range provides the benefit from selecting threats where the platform is inside of the lethal range over the threats where the platform is out of harm.

4.3.1.3 Equal weights

In this test, all of the parameters of the mode assessment equation will be in play. All the weights will be equally distributed over the parameters. Preventing one or two parameters from having a higher influence.

Figure B.3(a) and Table 4.5 show better overall improvement than Figure B.2(a) as the intervals

Table 4.3. Mode counter over total intervals and intervals in lethal range when only the mode, zone assessment, and lethal range parameters are being considered.

Radar	**Total intervals**				**Total intervals in lethal range**			
	TS	**TA**	**TT**	**MG**	**TS**	**TA**	**TT**	**MG**
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	25	17	12	12	25	16	1	2
5	64	1	1	0	63	1	1	0
6	51	12	3	0	41	2	1	0
7	57	8	1	0	46	0	0	0
8	34	27	4	1	34	26	4	1
9	64	1	1	0	63	1	1	0
10	64	1	1	0	63	1	1	0
11	63	2	1	0	20	1	1	0
12	64	1	1	0	0	0	0	0
13	58	6	2	0	52	2	2	0
14	63	2	1	0	14	0	0	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	59	6	1	0	58	6	1	0
18	59	3	3	1	48	3	3	1
19	64	1	1	0	52	1	1	0
20	17	24	20	5	0	0	0	0

of the majority of radars are in TS. Radars 8 and 4 are only affected by radars 18 and 19 when they are in burnthrough. Otherwise, these radars are the majority of intervals in TS and TA.

Not every pulse of a radar in a high mode needs to be countered, it should depend on the minimum required jamming pulses to successfully inhibit detection. The jamming percentage value improves on the mode equation by preventing the selection of a jamming pulse from a high mode radar that has already been jammed with the required minimum jamming pulses.

Figure B.3(c) shows that the overall jamming percentage values for the majority of radars are relatively low. This poses a problem when using equal weights where the other parameters are configured to have high values. This results in the jamming percentage rate having far less impact than the other three parameters which reaches their maximum values far quicker. A pulse with either the mode, zone assessment value or lethal range flag at a high value will

Table 4.4. Mode counter over total intervals and intervals in lethal range when all parameters are weighted equally.

Radar	Total intervals				Total intervals in lethal range			
	TS	TA	TT	MG	TS	TA	TT	MG
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	57	4	3	2	37	3	2	2
5	64	1	1	0	63	1	1	0
6	54	11	1	0	43	1	0	0
7	61	4	1	0	46	0	0	0
8	38	22	4	2	37	22	4	2
9	64	1	1	0	63	1	1	0
10	64	1	1	0	63	1	1	0
11	64	1	1	0	19	1	1	0
12	64	1	1	0	0	0	0	0
13	59	5	2	0	53	1	2	0
14	64	1	1	0	14	0	0	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	59	4	3	0	58	4	3	0
18	59	3	3	1	48	3	3	1
19	64	1	1	0	52	1	1	0
20	30	26	8	2	0	0	0	0

always be chosen above a pulse with a high jamming percentage value but lower mode or zone assessment value. The next test case will show why the percentage jamming value is of high importance to the mode assessment equation and requires a more favourable weighting.

4.3.1.4 Jamming percentage only assessment

Figure B.4(a) shows just how important the jamming percentage parameter is to mode assessment. Only the pulse percentage parameter, with the average values shown in Figure B.4(c), is used for threat evaluation and prioritisation in each coincidence. Not only has it successfully reverted all of the initial TT modes to TS but it kept all of the radars at TS for the majority of the time over the scenario.

Figure B.4 shows just how well backward CPI analysis along with the jamming percentage works together to jam enough pulses in a CPI and prevent a single detection over an interval of 1 second. This level of jamming effectiveness is achieved without knowing when a CPI starts.

Table 4.5. Mode counter over total intervals and intervals in lethal range when only the jamming percentage parameter is used.

Radar	Total intervals				Total intervals in lethal range			
	TS	TA	TT	MG	TS	TA	TT	MG
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	56	3	4	3	36	2	3	3
5	64	1	1	0	63	1	1	0
6	64	1	1	0	44	0	0	0
7	64	1	1	0	46	0	0	0
8	57	3	4	2	56	3	4	2
9	64	1	1	0	63	1	1	0
10	64	1	1	0	63	1	1	0
11	64	1	1	0	19	1	1	0
12	64	1	1	0	0	0	0	0
13	64	1	1	0	53	1	1	0
14	64	1	1	0	14	0	0	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	57	3	4	2	56	3	4	2
18	59	3	3	1	48	3	3	1
19	59	3	3	1	47	3	3	1
20	62	3	1	0	0	0	0	0

The only issue with only using jamming percentage, as shown in Table 4.5, are radar 4, 8, and 17 being affected by radars 18 and 19 when they are in burnthrough. The high mode intervals for these radars last only for a short duration, however, the threat radars reach the MG mode inside the lethal range. The other three parameters are still required to assist the TIJ in calculating when it is of higher priority to counter radars when the platform is inside the lethal range.

4.3.1.5 Jamming percentage as the highest weighted parameter

Test Case 4.3.1.4 shows that the jamming percentage should have the highest weight as opposed to the other threats as it provides the best control over the threat radars by keeping the threats in the majority of the intervals at the lowest mode. Therefore, the jamming percentage is set to 0.7 to keep the jamming percentage high enough where the parameter has a strong impact on the mode assessment value.

The mode and lethal range parameters have been set to 0.15 and 0.1 respectively as their values increases with a higher step ratio. These two parameters will still provide adequate

Table 4.6. Mode counter over total intervals and intervals in lethal range when the jamming percentage is the highest parameter.

Radar	Total intervals				Total intervals in lethal range			
	TS	TA	TT	MG	TS	TA	TT	MG
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	60	4	2	0	40	3	1	0
5	64	1	1	0	63	1	1	0
6	64	1	1	0	44	0	0	0
7	64	1	1	0	46	0	0	0
8	64	1	1	0	63	1	1	0
9	64	1	1	0	63	1	1	0
10	64	1	1	0	63	1	1	0
11	64	1	1	0	19	1	1	0
12	64	1	1	0	0	0	0	0
13	64	1	1	0	53	1	1	0
14	64	1	1	0	14	0	0	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	64	1	1	0	63	1	1	0
18	59	3	3	1	48	3	3	1
19	63	2	1	0	51	2	1	0
20	64	1	1	0	0	0	0	0

influence on the mode assessment equation. The zone assessment parameter set to 0.05, should consist of the lowest weight as the parameter is the least important. This is due to the jamming percentage parameter also being affected by the distance between the platform and radar.

Figure B.5 and Table 4.6 provides the results from the weight adjustments. The adjusted weights provide the best overall performance. TIJ keeps the vast majority of intervals for all of the threat radars in TS over the entire duration of the scenario.

Radar 4 is only for a single interval in TT whilst inside of the lethal range and radar 8 is in ts throughout. It is only radar 18 whilst in burnthrough which is capable of reaching MG, but that is just for a single interval.

Jamming percentage should be the highest weighted parameter as it is the only parameter in the mode assessment equation to measure the threat radar at the lowest pulse level. This is in contrast to the other three parameters which mostly measures at a higher level. The radar mode parameter measures the threat radar's operational level, and the zone and lethal range parameters measure the range of the radar and weapon system. Thus, to provide the best possible jamming effectiveness the mode assessment algorithm should utilise the jamming percentage value to indicate the necessity of the jamming pulse should be transmitted and use the lethality identifiers of the mode of operation, lethal range, and current zone assessment to add the risk factor of the radar towards the platform.

The jamming window size for the mode assessment evaluation tests was kept at that of the pulse width. This provided a coincidence per interval rate for the threat radars to differ between 0.6 to 0.99 and the average coincidences per interval are $29,492$ with the median at $28,648$. The pulse widths of the threat radars which are a few microseconds or less will normally be in a coincidence consisting of two to three pulses. Only the radars with higher pulse widths will create a coincidence of more than three pulses.

4.3.2 Jamming window size test

The jamming window size of Test Case 4.3.1.5 was set to a perfect noise jamming window which only envelopes the pulse and not the surrounding bins. Test Case 4.3.1.5 provides the best case scenario of how efficient TIJ is in perfect circumstances. However, this is not realistic as provisions have to be made for varying TOA and where the cover pulse jamming also has to be reasonable larger than the pulse to take into account the slowly rising and trailing edges of the jamming pulse.

The size of the jamming window is important as a large window will create more coincidences as the large jamming windows coincide more regularly. However, the jamming window can not be too short as it may result in the transmission of the jamming pulse to miss the radar pulse completely. The following test cases will look at which jamming window size will best suit the TIJ. This is done by analysing the capability of jamming multiple threat radars with different jamming window sizes.

4.3.2.1 Jamming window equal to 10% of the PRI

As stated in [1] and [14] a typical jamming window is around 10% of the threat radar's PRI. For this test case, the jamming window is set at 10% of the duty cycle around the pulse. Provision is made where the jamming window is set to 1.5 times the pulse width where the duty cycle exceeds 10%.

Table 4.7. Jamming window size relations for radars 1 to 10.

		Pulse width		5% of PRI		10% of PRI		2.5 times the pulse width	
Radar ID	**Mode**	**Jamming window size [us]**	**Size factor to pulse width**	**Jamming window size [us]**	**Size factor to pulse width**	**Jamming window size [us]**	**Size factor to pulse width**	**Jamming window size [us]**	**Size factor to pulse width**
1	**TS**	0.337	1	25.15	74	50.3	150	0.59	1.75
	TA	0.337	1	28.65	85	57.3	170	0.59	1.75
	TT	0.337	1	25.15	75	50.3	150	0.59	1.75
	MG	0.337	1	28.65	85	57.3	170	0.59	1.75
2	**TS**	0.313	1	20.35	65	40.7	130	0.58	1.75
	TA	0.313	1	17.35	105.43	34.7	110.86	0.58	1.75
	TT	0.25	1	20.35	81.4	40.7	162.8	0.44	1.75
	MG	0.587	1	75.35	128.36	150.7	256.73	1.05	1.75
3	**TS**	0.5	1	26.65	103.3	53.3	106.6	0.88	1.75
	TA	0.5	1	28.3	56.6	56.6	113.2	0.88	1.75
	TT	0.5	1	23.3	46.65	46.6	93.3	0.88	1.75
	MG	6.4	1	9.6	1.5	9.6	1.5	11.2	1.75
4	**TS**	49	1	51.2	1.01	102.4	2.1	85.75	1.75
	TA	49	1	73.5	1.5	64	1.3	85.75	1.75
	TT	25	1	52.5	1.5	32	1.28	43.75	1.75
	MG	50	1	51.2	1.02	102.4	2.04	87.5	1.75
5	**TS**	0.24	1	12	50	24	100	0.42	1.75
	TA	0.18	1	11.5	63.8	23	127.7	0.315	1.75
	TT	0.175	1	10	57.14	20	114.3	0.306	1.75
	MG	1.75	1	9	5.15	18	10.3	3.06	1.75
6	**TS**	6.9	1	7	1.01	14	2.02	12.075	1.75
	TA	5.3	1	6	1.13	12	2.26	9.275	1.75
	TT	5	1	25.6	5.12	51.2	10.24	8.75	1.75
	MG	5	1	12.8	2.56	25.6	5.01	8.75	1.75
7	**TS**	12.5	1	50	4	100	8	21.875	1.75
	TA	12.5	1	70	5.6	140	11.2	21.875	1.75
	TT	0.9	1	1	1.1	2	2.2	1.575	1.75
	MG	0.2	1	0.6	3	1.2	6	0.35	1.75
8	**TS**	36	1	200	5.5	400	11	63	1.75
	TA	72	1	108	1.5	100	1.4	126	1.75
	TT	25	1	37.5	1.5	50	2	43.75	1.75
	MG	10	1	12.5	1.25	25	1.5	17.5	1.75
9	**TS**	10	1	15	1.5	15	1.5	17.5	1.75
	TA	7.5	1	11.25	1.5	11.25	1.5	13.125	1.75
	TT	5	1	7.5	1.5	7.5	1.5	8.75	1.75
	MG	4.5	1	6.75	1.5	5	1.1	7.875	1.75
10	**TS**	2.5	1	30	12	60	24	4.375	1.75
	TA	1.5	1	17	11.3	34	22.6	2.625	1.75
	TT	0.5	1	19	38	38	72	0.875	1.75
	MG	0.9	1	14.5	16.11	35	32.22	1.575	1.75

Tables 4.7 and 4.8 show that the pulse widths of the threat radars vary from a few nanoseconds to a few hundred microseconds. Whereas the PRI is dependent on the type of radar and PRF implemented. This will result in radar duty cycles ranging from small duty cycles less than a per cent to duty cycles over 10%.

However, as seen in Tables 4.7 and 4.8 of the total 80 modes 44 have a jamming window of more than 10 times the size of the pulse, and of those 44 jamming windows 14 has a jamming window of more than 100 times the pulse width. Thus it is not preferable to transmit such a large amount of noise energy where it is unnecessary. These large jamming windows may create unwanted attention with radars employing home on jam (HOJ) but this is outside the scope of the dissertation.

Table 4.8. Jamming window size relations for radars 11 to 20.

		Pulse width		5% of PRI		10% of PRI		2.5 times the pulse width	
Radar ID	**Mode**	**Jamming window size [us]**	**Size factor to pulse width**	**Jamming window size [us]**	**Size factor to pulse width**	**Jamming window size [us]**	**Size factor to pulse width**	**Jamming window size [us]**	**Size factor to pulse width**
11	**TS**	10	1	15	1.5	15	1.5	17.5	1.75
	TA	5	1	7.5	1.5	7.5	1.5	8.75	1.75
	TT	3	1	4.5	1.5	5	1.6	5.25	1.75
	MG	4	1	6	1.5	5	1.1	7	1.75
12	**TS**	2	1	40	20	80	40	3.5	1.75
	TA	1.5	1	20	13.3	40	26.6	2.625	1.75
	TT	0.5	1	20	40	40	80	0.875	1.75
	MG	0.75	1	25.5	34	51	68	1.3125	1.75
13	**TS**	15	1	125	8.3	250	16.6	26.25	1.75
	TA	10	1	62.5	6.25	125	12.5	17.5	1.75
	TT	5	1	6.25	3.125	12.5	6.25	8.75	1.75
	MG	5	1	12.5	6.25	25	5	8.75	1.75
14	**TS**	15.1	1	130	8.6	260	16.2	26.425	1.75
	TA	12.3	1	130	10.6	260	21.2	21.525	1.75
	TT	6.5	1	33.3	5.12	66.6	10.24	11.375	1.75
	MG	8	1	33.3	4.2	66.6	8.4	14	1.75
15	**TS**	2.45	1	66.65	27.2	133.3	54.4	4.286	1.75
	TA	2	1	65	32.5	130	65	3.5	1.75
	TT	0.45	1	22.5	50	45	100	0.788	1.75
	MG	1.2	1	20	16.6	40	33.2	2.1	1.75
16	**TS**	3	1	50	16.6	100	33.2	5.25	1.75
	TA	2	1	37.5	18.75	75	37.5	3.5	1.75
	TT	1.55	1	25	16.1	50	32.2	2.713	1.75
	MG	2.1	1	12.5	5.9	25	11.8	3.675	1.75
17	**TS**	15.4	1	61.1	4	122.2	8	26.95	1.75
	TA	12.75	1	56.1	4.4	112.2	8.8	22.313	1.75
	TT	10.88	1	45.55	4.18	91.1	8.37	19.04	1.75
	MG	9.98	1	14.97	1.5	12.2	1.2	17.465	1.75
18	**TS**	0.8	1	4.61	5.7	9.22	11.52	1.4	1.75
	TA	0.6	1	4.62	7.7	9.24	15.4	1.05	1.75
	TT	0.4	1	4.63	11.57	9.26	23.14	0.7	1.75
	MG	0.5	1	4.625	9.25	9.25	18.5	0.875	1.75
19	**TS**	3.2	1	4.8	1.5	4.8	1.5	5.6	1.75
	TA	4.1	1	6.15	1.5	6.15	1.5	7.175	1.75
	TT	3.55	1	5.325	1.5	5.325	1.5	6.212	1.75
	MG	2.9	1	4.35	1.5	4.35	1.5	5.075	1.75
20	**TS**	15	1	22.5	1.5	22.5	1.5	26.25	1.75
	TA	12	1	18	1.5	18	1.5	21	1.75
	TT	10	1	15	1.5	15	1.5	17.5	1.75
	MG	7	1	10.5	1.5	10.5	1.5	12.25	1.75

The other issue is the jamming window that has to cover a pulse width of a duty cycle that is more than 10%. The jammer has to now make provision for these pulses. It is not necessarily that these pulses have a large pulse width it is just that the radar is using a high PRF such as radars 9, 11, 20 and especially radar number 19 with both small pulse widths and PRIs.

As seen in Figure B.6(b) all the radars have a coincidence rate of over 80% per interval, with most above 90% and some radars having a coincidence rate of 100%. The TIJ is unable to inhibit enough CPIs overall the radars causing most of the radars to be in a high mode as seen in Figure B.6(a). This is also seen in Table 4.9 where the modes are the majority of intervals either in TT or MG.

The mean coincidences per interval is at $32,323$ with the median sitting at $31,425$. The mean

Table 4.9. Mode counter over total intervals and intervals in lethal range when the jamming window = 10% of the PRI.

Radar	Total intervals				Total intervals in lethal range			
	TS	TA	TT	MG	TS	TA	TT	MG
1	20	11	16	19	0	0	0	0
2	16	18	19	13	0	0	0	0
3	9	16	22	19	0	0	0	0
4	54	4	4	4	34	3	3	4
5	52	3	6	5	51	3	6	5
6	62	3	1	0	42	2	0	0
7	28	19	19	0	27	10	9	0
8	44	12	6	4	43	12	6	4
9	53	10	3	0	52	10	3	0
10	55	3	4	4	54	3	4	4
11	48	17	1	0	19	2	1	0
12	27	16	11	12	0	0	0	0
13	32	17	15	2	31	12	10	2
14	0	15	27	24	0	2	2	10
15	39	11	6	10	0	0	0	0
16	35	12	11	8	34	6	6	8
17	52	3	6	5	51	3	6	5
18	56	4	4	2	45	4	4	2
19	58	4	3	1	47	3	3	1
20	48	5	8	5	0	0	0	0

and median is well above that of the coincidence rate of the Test Case 4.3.1.5. Thus most of the pulses of each threat radar are in coincidence due to the large jamming windows. This in turn results in a large number of pulses enveloping one another due to the constraints of the jammer where only a single pulse can be chosen per coincidence a lot of pulses will be continuously disregarded.

However, the TIJ still tries to keep the modes of the threats where the platform is within lethal range as low as possible. The threat radars (especially radars 1, 2, 3, and 12) where the platform is outside the lethal range goes to MG in more intervals than the threats where the platform is inside of the lethal range. The TIJ will disregard the threats outside the lethal range and rather prioritise the threats inside a lethal range.

Interval 22 to 36 where the burnthrough occurs for radars 18 and 19 causes a lot of threat radars that are inside lethal range to go to MG It takes longer as opposed to the previous tests to revert these radars to a lower mode. This affects radars 4, 5, 8, 10, 13, 14, 16 and 17 to

Table 4.10. Mode counter over total intervals and intervals in lethal range when the jamming window = 5% of the PRI.

Radar	Total intervals				Total intervals in lethal range			
	TS	TA	TT	MG	TS	TA	TT	MG
1	9	17	25	15	0	0	0	0
2	39	19	7	1	0	0	0	0
3	10	21	24	11	0	0	0	0
4	56	3	4	3	36	2	3	3
5	59	3	3	1	58	3	3	1
6	64	1	1	0	44	0	0	0
7	40	15	11	0	36	6	4	0
8	51	7	5	3	50	7	5	3
9	56	6	4	0	55	6	4	0
10	59	5	2	0	58	5	2	0
11	47	18	1	0	20	1	1	0
12	35	15	11	5	0	0	0	0
13	42	13	11	0	41	8	6	0
14	1	20	30	15	0	3	4	7
15	50	6	5	6	0	0	0	0
16	44	9	10	3	43	3	5	3
17	55	4	4	3	54	4	4	3
18	57	3	4	2	46	3	4	2
19	59	3	3	1	47	3	3	1
20	53	3	6	3	0	0	0	0

transition to MG whereas the interval before and then after being in TS or TA. The platform is also inside the lethal range of all of these radars when they transition to MG even if only for a few intervals.

4.3.2.2 Jamming window equal to 5% of the PRI

Decreasing the jamming window to be 5% of the PRI improves the jamming effectiveness as opposed to a jamming window of 10% of the PRI as seen in Figure B.7(a). There are more intervals where the modes are in TS and TA in Table 4.10 than in Table 4.9, however, a high number of intervals are still in TT and MG. The coincidence rate of Figure B.7(b) is still over 80% per interval, with most of the radars having a coincidence rate over 95%.

The 5% PRI size factor compared to the radar pulse widths in Tables 4.7 and 4.8 is half that of the 10% PRI size factor but the size factor remains high. Therefore it can be concluded that depending on the PRI as a means to determine the jamming window size will result in high coincidence rates for each radar. This in turn will result in a lot of pulses being disregarded allowing the threat radars to have a higher chance to reach the detection probability over a

Table 4.11. Mode counter over total intervals and intervals in lethal range when the jamming window = 1.75 times the signal pulse width.

Radar	Total intervals				Total intervals in lethal range			
	TS	TA	TT	MG	TS	TA	TT	MG
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	56	3	4	3	36	2	3	3
5	64	1	1	0	63	1	1	0
6	59	5	2	0	39	4	1	0
7	42	15	9	0	37	6	3	0
8	51	5	6	4	50	5	6	4
9	59	5	2	0	58	5	2	0
10	64	1	1	0	63	1	1	0
11	45	19	2	0	20	1	1	0
12	64	1	1	0	0	0	0	0
13	46	12	8	0	45	7	3	0
14	18	26	22	0	6	5	3	0
15	63	2	1	0	0	0	0	0
16	63	2	1	0	51	2	1	0
17	56	3	4	3	55	3	4	3
18	59	3	3	1	48	3	3	1
19	59	3	3	1	47	3	3	1
20	53	4	6	3	0	0	0	0

CPI, detect the platform and proceed to the next mode of operation.

A window size more closely related to the pulse width or range bin is required to prevent large jamming window sizes overall and to keep the coincidence rate as low as possible. Thereby, having more standalone pulses will allow for a lower jamming percentage value when a pulse is in a coincidence.

4.3.2.3 Jamming window 1.75 times the size of the pulse width

It would rather be beneficial to arrange a jamming window around the pulse width of the threat radar. Configuring the jamming window size around the pulse width provides the jammer with the capability to allow just enough jamming energy over the pulse whilst still taking into account any error in pulse time-of-arrival.

For this test case, the jamming window size is 1.75 times the size of the pulse width. This allows for a jamming envelope exceeding the radar pulse by 0.75 times the radar pulse width, to provide for any variability in TOA. However, the jamming window size will be dependent on the ES system's capability to determine the correct TOA as well as for any PRF techniques used by the radar. For this dissertation, however, the TOA estimation is perfect and only stable PRIs are used.

Figure B.8 shows just how well the jamming effectiveness improves with a smaller jamming window. The coincidence rate per interval has decreased for most pulses and the coincidences per interval have also decreased to an average of $29,284$ with the median at $28,133$. The decrease in average and median as opposed to Test Case 4.3.1.5 is due to the radars differing in modes, therefore differing in waveforms, between the opposing tests. It can also be that coincidences that are close to one another in time but still separated have overlapped, due to the increase in the jamming window, creating new coincidences.

As seen in Table 4.11 the modes in the intervals start to represent more that of Table 4.6 than of Tables 4.9 and 4.10. The modes per interval are beginning to resemble that of Table 4.6. However, The jamming window is still too large and results in more jamming pulses to be in coincidence, especially the radars with larger pulse widths. The burnthrough at intervals 22 to 34 also influences the prioritisation. Radars closer to the platform and radars with high jamming percentages will be selected in a coincidence as opposed to these radars.

4.3.2.4 Jamming window with trailing edge just after the pulse trailing edge

The cover pulse does not need to extend after the pulse has ended by the same amount of time that the cover pulse is transmitted before the arrival of the pulse. This test case will use the same jamming window of Test Case 4.3.2.3 however the noise jamming cover pulse will stop at 5% of the length of the radar pulse width after the trailing edge of the radar pulse. This is to take into account the slow decrease of the trailing edge of the cover pulse.

From Figure B.9(a) and Table 4.12, the design of this jamming window provides slightly better jamming effectiveness than from Figure B.8(a) and Table 4.11. The majority of radars are in TS. Radars 7 and 14 transition back and forth between TS and TA whereas both were mostly transitioning between TA and TT in the previous test.

The decrease in the jamming window decreases the coincidences per interval average to $28,901$. This is due to fewer large jamming pulses which also results in fewer jamming pulses in a coincidence. jamming pulses that previously overlapped are now just short enough that they can be considered standalone.

Table 4.12. Mode counter over total intervals and intervals in lethal range when the jamming window has a cut-off of 5% after signal pulse falling edge.

Radar	**Total intervals**				**Total intervals in lethal range**			
	TS	**TA**	**TT**	**MG**	**TS**	**TA**	**TT**	**MG**
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	56	3	4	3	36	2	3	3
5	64	1	1	0	63	1	1	0
6	62	3	1	0	42	2	0	0
7	47	13	6	0	41	4	1	0
8	52	5	6	3	51	5	6	3
9	60	4	2	0	59	4	2	0
10	64	1	1	0	63	1	1	0
11	49	16	11	0	20	1	1	0
12	64	1	1	0	0	0	0	0
13	52	11	3	0	48	6	1	0
14	37	24	5	0	8	5	1	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	56	3	4	3	55	3	4	3
18	59	3	3	1	48	3	3	1
19	59	3	3	1	47	3	3	1
20	53	4	6	3	0	0	0	0

This causes the coincidences per interval rate in Figure B.9(b) to drop even further for the majority of radars, with some radars having a coincidence rate below 0.65. Thus fewer jamming pulses are now in coincidences and more are standalone as opposed to the other jamming window tests, resulting in a lower jamming percentage value for jamming pulses in coincidence.

This will result in the successful jamming effectiveness against all threats by the single-channel TIJ jammer. All of this is due to a shorter jamming window. However, decreasing the jamming window even further may result in erroneous time coordination between the reception of the radar pulse and transmitting the jamming pulse.

4.3.3 Ignoring burnthrough

Figures B.10(a) and B.11(a) show the results from the test when the jamming percentage and zone assessment values are set to 0 for only the threat radars (radars 18 and 19) where the platform is inside burnthrough. Thereby the threat radars inside burnthrough will be ignored whilst the rest are still calculated with the normal weight distributions. These results should be

Table 4.13. Mode counter over total intervals and intervals in lethal range when burnthrough is ignored for a jamming window = pulse width.

Radar	**Total intervals**				**Total intervals in lethal range**			
	TS	**TA**	**TT**	**MG**	**TS**	**TA**	**TT**	**MG**
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	58	5	3	0	38	4	2	0
5	64	1	1	0	63	1	1	0
6	64	1	1	0	44	0	0	0
7	47	13	6	0	46	0	0	0
8	58	5	3	0	57	5	3	0
9	63	2	1	0	62	2	1	0
10	64	1	1	0	63	1	1	0
11	64	1	1	0	19	1	1	0
12	64	1	1	0	0	0	0	0
13	61	4	1	0	53	1	1	0
14	64	1	1	0	14	0	0	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	60	4	2	0	59	4	2	0
18	56	3	3	4	45	3	3	4
19	59	3	3	1	47	3	3	1
20	64	1	1	0	0	0	0	0

compared with the results from Figure B.5(a) and Figure B.9(a) respectively. Both show that only the radars inside burnthrough will transition to MG with the previously affected radars staying below MG.

As seen in Table 4.13 only the intervals of radars 18 and 19 which are in burnthrough will go to MG. Table 4.14 only two intervals from radar 8 will transition to MG when inside of the lethal range. The intervals in TT differ only slightly with the total TT intervals in Table 4.14 being higher. However, these results provide the best performance from the TIJ against all of the previous tests.

As there is no other jamming technique or system that works alongside the single noise jamming system it is not advisable to just ignore the radar when the platform is inside burnthrough range. The jammer still needs to protect the platform from all of the radars. From this information, the platform should be equipped with multiple jammers or jamming channels to counter the burnthrough radars separately to not compromise the jamming effectiveness of

Table 4.14. Mode counter over total intervals and intervals in lethal range when burnthrough is ignored for a jamming window with a cut-off 5% after signal pulse falling edge.

Radar	Total intervals				Total intervals in lethal range			
	TS	TA	TT	MG	TS	TA	TT	MG
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	58	5	3	0	37	4	2	0
5	64	1	1	0	63	1	1	0
6	62	3	1	0	42	2	0	0
7	46	13	7	0	41	4	1	0
8	55	4	5	2	54	4	5	2
9	61	4	1	0	60	4	1	0
10	64	1	1	0	63	1	1	0
11	47	18	1	0	20	1	1	0
12	64	1	1	0	0	0	0	0
13	50	12	4	0	47	7	1	0
14	18	27	21	0	9	4	2	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	58	5	3	0	57	5	3	0
18	56	3	3	4	45	3	3	4
19	59	3	3	1	47	3	3	1
20	53	4	6	3	0	0	0	0

the other threat radars.

4.3.4 Varied radar sizes

All of the tests use the full 20 radars from Table A.1 to determine if the TIJ is capable of handling a large number of coincidences per interval and still maintaining jamming efficiency over the threats where most of their jamming pulses are in coincidence. Figures B.12, B.13 and B.14 show what the jamming effectiveness will be when fewer radars are present in the jamming channel.

Tables 4.15, 4.16, and 4.17 all show that the modes shift down from TT to TS. Only the first interval is in TT and there are no intervals in MG.

The coincidence per interval rate of radar 4 is higher than the rest of the radars with an overall value of around 0.5, as seen in Figure B.12. These low coincidence rates, where the average coincidences per second are 557 and the relatively low jamming percentage rate allow for most CPIs to be countered by just transmitting the standalone pulses. Adequate jamming can

Table 4.15. Mode counter over total intervals and intervals in lethal range against 5 coherent radars

Radar	Total intervals				Total intervals in lethal range			
	TS	TA	TT	MG	TS	TA	TT	MG
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	64	1	1	0	44	0	0	0
5	64	1	1	0	63	1	1	0

Table 4.16. Mode counter over total intervals and intervals in lethal range against 10 coherent radars

Radar	Total intervals				Total intervals in lethal range			
	TS	TA	TT	MG	TS	TA	TT	MG
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	63	2	1	0	43	1	0	0
5	64	1	1	0	63	1	1	0
6	64	1	1	0	44	0	0	0
7	64	1	1	0	46	0	0	0
8	64	1	1	0	63	1	1	0
9	64	1	1	0	63	1	1	0
10	64	1	1	0	63	1	1	0

be accomplished with a low number of threat radars as the coincidence rates are relatively low.

Competing against 10 threats radars as seen in Figure B.13 is also not a problem to the TIJ. The coincidence per interval rate has now increased, with the average coincidences per second being $6,742$, with more radars having a coincidence rate of 0.75 and higher. This still does not hinder the jamming effectiveness as the low jamming percentage of the threats allow for a vast majority of the CPIs to be countered successfully, allowing only the higher jamming percentage radars in the coincidences to be selected.

For 15 threats the average coincidences per interval have increased to $14,800$ however the TIJ is still able to easily maintain jamming effectiveness. As seen in Figure B.14 the coincidences per interval have increased for all the threats but just like the other two tests, the jamming percentage is low enough for most of the threats which result in adequate jamming over all

Table 4.17. Mode counter over total intervals and intervals in lethal range against 15 coherent radars

Radar	**Total intervals**				**Total intervals in lethal range**			
	TS	**TA**	**TT**	**MG**	**TS**	**TA**	**TT**	**MG**
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	63	2	1	0	43	1	0	0
5	64	1	1	0	63	1	1	0
6	64	1	1	0	44	0	0	0
7	64	1	1	0	46	0	0	0
8	64	1	1	0	63	1	1	0
9	64	1	1	0	63	1	1	0
10	64	1	1	0	63	1	1	0
11	64	1	1	0	19	1	1	0
12	64	1	1	0	0	0	0	0
13	64	1	1	0	53	1	1	0
14	64	1	1	0	14	0	0	0
15	64	1	1	0	0	0	0	0

of the CPIs. It is also seen that the TIJ has a far better jamming effectiveness rate against all threats when none are in the burnthrough range.

4.3.5 Signal detection error estimation test

From the jammer's point of view, the majority of radar parameters can be either measured or calculated except the signal detection parameters. The CPI, probability of detection and probability of false alarm are most probably unknown to the jammer. Therefore the user has to predict what these parameters values will be.

In the following tests, we will see what will happen to the jamming effectiveness if the signal detection values are either overestimated or underestimated. The error values in Tables 4.18, 4.19, and 4.20 will be used for each associated error estimation test.

The jamming window of Test Case 4.3.2.4 will be used with the mode assessment parameters of Test Case 4.3.1.5.

4.3.5.1 Error in CPI estimation

Overestimates of the CPI from Figure B.15 and Table 4.21 provides a close to similar picture as the result from Test Case 4.3.1.5. No radars except radar 8 have intervals in MG.

Table 4.18. Over and under estimation values of the radar CPI size.

Real radar CPI	Under estimated radar CPI	Over estimated radar CPI
256	128	512
128	64	256
100	64	256
64	32	128
50	32	128
32	16	64

Table 4.19. Over and under estimation values of the radar probability of detection.

Real radar P_d	Under estimated radar P_d	Over estimated radar P_d
0.9	0.8	0.999
0.8	0.5	0.9
0.5	0.3	0.8

Table 4.20. Over and under estimation values of the radar probability of false alarm.

Real P_{fa}	Over estimated P_{fa}	Under estimated P_{fa}
10^{-6}	10^{-10}	10^{-3}

The coincidence per interval rate for each threat of Figure B.15(b) has increased by a few points but it is still manageable. The jamming percentage rate of Figure B.15(c) has increased due to the higher CPI sizes.

Overestimating the CPI provides the benefit that the TIJ will determine that the radar will have higher integration gains due to coherent integration over the CPI. More pulses from the estimated CPI will need to be countered causing the jamming percentage rate to increase. However, there are disadvantages to overestimation as well as overestimating CPI may result in the TIJ disregarding pulses sequentially, as the jamming percentage is still low, which will allow the radar to detect the platform.

Underestimating the CPI provides severe issues for the TIJ. This is seen in Figure B.16 and Table 4.22 where all of the radars except for radars 1, 2, 3, and 5 are either in TT or MG. Underestimating the CPI causes the TIJ to predict a lower coherent integration gain. This in turn causes the TIJ to determine inferior jamming percentages where far fewer pulses are countered than required.

It is by far more advantageous to overestimate the size of the CPI and counter more pulses

Table 4.21. Mode counter over total intervals and intervals in lethal range when the CPI size is overestimated.

Radar	**Total intervals**				**Total intervals in lethal range**			
	TS	**TA**	**TT**	**MG**	**TS**	**TA**	**TT**	**MG**
1	64	1	1	0	0	0	0	0
2	62	2	2	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	64	1	1	0	44	0	0	0
5	54	9	3	0	45	1	0	0
6	64	1	1	0	44	0	0	0
7	54	9	3	0	45	1	0	0
8	33	27	4	2	32	27	4	2
9	64	1	1	0	63	1	1	0
10	64	1	1	0	63	1	1	0
11	63	2	1	0	20	1	1	0
12	64	1	1	0	0	0	0	0
13	40	20	6	0	39	15	1	0
14	34	23	9	0	10	3	1	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	62	3	1	0	61	3	3	0
18	64	1	1	0	53	1	1	0
19	64	1	1	0	52	1	1	0
20	62	3	1	0	0	0	0	0

than what is required. However, the noise jammer can only counter a certain CPI size of a radar with a certain set of parameters. Noise jamming will be negatively affected if more radar parameters are also high in value such as transmit power, pulse width, antenna gain, larger signal than noise bandwidth as well as a platform with a high RCS and at close distance. This will result in miss calculation of the detection and burnthrough range and required noise jamming energy to counter signals.

4.3.5.2 Error in probability of detection estimation

Not knowing the probability of detection does not have such a high impact on the jamming effectiveness of the TIJ. It is the minimum required probability of detection set by the TIJ at which the jammer must lower the probability of detection to that provides a problem.

Overestimating the probability of detection requires a higher minimum required probability of detection. As seen in Table 4.19 and Table 3.1 configuring a radars probability of detection to 0.9 will result in the minimum probability of detection being at 0.3. This will cause the area between the radar's real probability of detection and the TIJ's set minimum probability

Table 4.22. Mode counter over total intervals and intervals in lethal range when the CPI size is underestimated.

Radar	Total intervals				Total intervals in lethal range			
	TS	TA	TT	MG	TS	TA	TT	MG
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	40	25	1	0	0	0	0	0
4	0	0	1	65	0	0	0	44
5	40	25	1	0	40	24	1	0
6	0	0	1	65	0	0	0	44
7	0	0	33	33	0	0	22	23
8	0	0	1	65	0	0	1	64
9	0	0	25	41	0	0	24	41
10	0	0	33	33	0	0	32	33
11	0	0	1	65	0	0	1	21
12	0	0	1	65	0	0	0	0
13	0	0	22	44	0	0	22	33
14	0	1	3	62	0	0	0	14
15	0	12	13	41	0	0	0	0
16	19	26	10	11	18	20	5	11
17	0	0	1	65	0	0	1	64
18	15	8	12	31	5	7	12	31
19	0	0	25	34	0	0	20	34
20	0	0	1	65	0	0	0	0

of detection to be decreased if the radar's real probability of detection is for example at 0.7 or lower. Thus overestimating the probability of detection results in the minimum required probability of detection being underestimated.

This is also seen in Figure B.17 and Table 4.23 where more intervals are in TT or MG as opposed to Test Case 4.3.2.4. This is due to the jammer determining the probability of detection higher than the real value. More CPIs will reach the probability of detection while the TIJ believes it is successfully countering each threat.

Underestimating the probability of detection generates a lower minimum required probability of detection value. Using the same example from overestimation the TIJ sets the probability of detection to 0.8. The minimum probability of detection is then set to 0.2. Both are lower than the real radar's probability of detection resulting in more pulses in the CPI to be selected for jamming. Therefore the minimum required probability of detection is overestimated.

Table 4.23. Mode counter over total intervals and intervals in lethal range when the threat radar probability of detection is overestimated.

Radar	Total intervals				Total intervals in lethal range			
	TS	**TA**	**TT**	**MG**	**TS**	**TA**	**TT**	**MG**
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	33	12	14	5	33	2	4	5
5	64	1	1	0	63	1	1	0
6	58	6	2	0	38	5	1	0
7	39	15	12	0	37	6	3	0
8	51	4	6	5	50	4	6	5
9	56	6	4	0	55	6	4	0
10	64	1	1	0	63	1	1	0
11	44	19	3	0	19	1	1	0
12	63	2	1	0	0	0	0	0
13	49	11	6	0	45	6	4	0
14	35	25	6	0	7	5	2	0
15	63	2	1	0	0	0	0	0
16	53	2	1	0	51	2	1	0
17	55	3	5	3	54	3	5	4
18	56	4	4	2	45	4	4	2
19	57	3	4	2	45	3	4	2
20	46	9	7	4	0	0	0	0

As seen in Figure B.18 and Table 4.24 the TIJ will have higher percentage jamming rates as more pulses will need to be countered. Fewer intervals are in TT and MG when compared to Table 4.12. This is because the jammer predicts that the threat requires a lower SNR thus more pulses will need to be countered over the CPI. Therefore overestimating the minimum probability of detection provides a higher jamming percentage rate and thus resulting in more pulses in the CPI to be jammed.

4.3.5.3 Error in probability of false alarm estimation

As seen in Figures B.19 and B.20 neither over nor underestimating the probability of false alarm provide a reasonable advantage as opposed to the CPI and probability of detection error estimation tests. Furthermore, Tables 4.25 and 4.26 allow for more intervals to be in TT and MG than in Table 4.12. The effects of over and underestimation can be seen in the jamming percentage heat maps of Figure B.19(c) and Figure B.20(c).

Overestimation lowers the jamming percentage rate to lower than required. This is due to the estimation of the false alarm at 10^{-10} requiring a much higher SNR to reach the required

Table 4.24. Mode counter over total intervals and intervals in lethal range when the threat radar probability of detection is underestimated.

Radar	**Total intervals**				**Total intervals in lethal range**			
	TS	**TA**	**TT**	**MG**	**TS**	**TA**	**TT**	**MG**
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	57	3	3	3	37	2	2	3
5	64	1	1	0	63	1	1	0
6	64	1	1	0	44	0	0	0
7	60	4	2	0	46	0	0	0
8	57	3	4	2	56	3	4	2
9	64	1	1	0	63	1	1	0
10	64	1	1	0	63	1	1	0
11	64	1	1	0	20	1	1	0
12	64	1	1	0	0	0	0	0
13	59	6	1	1	50	4	1	0
14	51	14	1	0	12	2	0	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	59	3	3	1	58	3	3	1
18	61	3	2	0	50	3	2	0
19	63	2	1	0	51	2	1	0
20	60	5	1	0	0	0	0	0

probability of detection. Thus the radar needs a higher SNR than with the probability of false alarm of 10^{-6}. A higher required SNR requires more pulses or higher power to achieve detection. The jammer still transmits at the same energy resulting in fewer pulses needed to be transmitted, to achieve jamming effectiveness.

The maximum range decreases due to the higher SNR as fewer false alarms require a shorter distance, which causes the maximum detectable range and burnthrough range to decrease as well as can be seen in the zone assessment heat map of Figure B.19(d).

The majority of jamming percentage values are below 0.3 for most of the radars, as seen in Figure B.19(c), thus in the mode assessment equation, the lethal range and mode values become the deciding factors. However, as fewer pulses are determined to counter the threats less than what is required may be transmitted. This can cause problems with threats outside the lethal range as the TIJ may ignore pulses in the coincidence as it has determined that enough pulses in the CPI have been countered and that the platform is outside the lethal range.

Table 4.25. Mode counter over total intervals and intervals in lethal range when the threat radar probability of false alarm is overestimated.

Radar	Total intervals				Total intervals in lethal range			
	TS	TA	TT	MG	TS	TA	TT	MG
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	61	4	1	0	0	0	0	0
4	19	19	14	14	18	19	3	4
5	64	1	1	0	63	1	1	0
6	47	12	5	2	39	4	1	0
7	45	14	7	0	39	4	1	0
8	57	4	4	1	56	4	4	1
9	57	7	2	0	56	7	2	0
10	61	4	1	0	60	4	1	0
11	47	18	1	0	20	1	1	0
12	64	1	1	0	0	0	0	0
13	51	11	4	0	47	6	2	0
14	41	23	2	0	9	4	1	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	58	4	3	1	57	1	3	1
18	59	3	3	1	48	3	3	1
19	59	3	3	1	47	3	3	1
20	0	4	33	29	0	0	0	0

Underestimation increases the jamming percentage rate as the probability of false alarm is lower than what the real radar is set at. The required SNR is lowered which results in fewer pulses to reach the probability of detection. This causes a problem for the TIJ as more pulses need to be countered to keep it below the minimum probability of detection value.

The higher percentage jamming ratio causes a problem as the majority of threats are well above 0.75 as seen in the jamming percentage heat map in Figure B.20(c). The biggest issue is caused by the new set ranges, due to the low SNR the maximum range and burnthrough range is adjusted to be larger than what they are. This causes the zone assessment value, as seen in Figure B.20(d) to be close to 1. This in turn increases the mode assessment values for the threats as the radars will now be chosen more frequently than necessary.

4.3.6 Testing with the best possible radar signal detection estimations

From the tests above it is seen that decreasing the total pulses in a coincidence and the coincidence rate by using a small jamming window, overestimating the CPI, probability of false alarm and the TIJ required minimum required probability of detection provide the

Table 4.26. Mode counter over total intervals and intervals in lethal range when the threat radar probability of false alarm is underestimated.

Radar	**Total intervals**				**Total intervals in lethal range**			
	TS	**TA**	**TT**	**MG**	**TS**	**TA**	**TT**	**MG**
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	22	22	12	10	19	20	3	2
5	64	1	1	0	63	1	1	0
6	39	18	9	0	27	9	8	0
7	23	22	21	0	22	13	11	0
8	19	20	16	11	18	20	16	11
9	57	8	1	0	56	8	1	0
10	62	3	1	0	61	3	1	0
11	42	22	2	0	13	7	2	0
12	64	1	1	0	0	0	0	0
13	21	25	17	3	20	19	13	3
14	16	18	22	0	2	7	5	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	45	10	9	2	44	10	9	2
18	56	5	4	1	46	4	4	1
19	56	5	4	1	45	4	4	1
20	18	8	23	17	0	0	0	0

best results when error estimation is introduced. For this test, all of these factors have been joined together to observe what the outcome will be as seen in Figure B.21. Using the error estimations which provides the best possible advantage to the TIJ has provided one of the best outcomes as shown in Table 4.27.

Table 4.27 provides better results than that of Table 4.12 and is close to the results of Table 4.6. Most notably is the intervals where burnthrough of radars 18 and 19 caused a lot of issues at other threats has resulted in only radars 8, 14 and 20 to transition once into MG before moving back to TT and lower.

The higher estimated CPI size and the lowered minimum probability of detection values result in more jamming pulses required to counter the CPI. The overestimated probability of false alarm decreases the burnthrough range resulting in just the minimum jamming pulses per interval to be high at the real burnthrough range, preventing those pulses to have a constantly large mode assessment value at each coincidence. This in turn allows for other pulses to also

Table 4.27. Mode counter over total intervals and intervals in lethal range for the best estimates.

Radar	**Total intervals**				**Total intervals in lethal range**			
	TS	**TA**	**TT**	**MG**	**TS**	**TA**	**TT**	**MG**
1	64	1	1	0	0	0	0	0
2	64	1	1	0	0	0	0	0
3	64	1	1	0	0	0	0	0
4	64	1	1	0	44	0	0	0
5	64	1	1	0	63	1	1	0
6	64	1	1	0	44	0	0	0
7	56	7	3	0	44	2	0	0
8	33	30	2	1	33	29	2	1
9	64	1	1	0	63	1	1	0
10	64	1	1	0	63	1	1	0
11	64	1	1	0	19	1	1	0
12	64	1	1	0	0	0	0	0
13	41	20	5	0	40	14	1	0
14	42	17	6	1	40	14	1	0
15	64	1	1	0	0	0	0	0
16	64	1	1	0	52	1	1	0
17	63	2	1	0	62	2	1	0
18	64	1	1	0	53	1	1	0
19	64	1	1	0	52	1	1	0
20	51	12	2	1	0	0	0	0

be selected at the coincidence.

However, the error estimations presented here are configured to be conservative. These conservative values still provide jamming effectiveness over the majority of intervals for all of the threats. Increasing these estimations further will result in the jammer providing more jamming resources to be allocated to that threat radar or radars. The CPI size may be increased by such a high amount that the other threats will start to be disregarded in a coincidence. By further estimating the possible probability values with the high CPI will degrade the overall jamming effectiveness resulting in issues like what has been seen when burnthrough occurs at a radar. Multiple radars are affected when one radar has a very high mode assessment value that could have been lowered if reasonable estimations have been used.

CHAPTER 5 CONCLUSION

It is shown that the TIJ can handle a large number of coincidences per one-second interval to maintain jamming effectiveness over multiple threats even when the majority of all of the pulses are in coincidence.

Threat evaluation and prioritisation are performed through the use of the mode assessment calculation. Mode assessment provides the means to determine which pulse in a coincidence should be countered through the utilisation of the threat radar mode of operation, the assessment of the ranges, a lethal range flag and the jamming percentage parameter.

The jamming percentage parameter determines the minimum number of pulses to counter per CPI, depending on the jamming equation for intermittent jamming power and the radar equation required to determine the maximum SNR. Percentage jamming is calculated by using backward CPI analysis where each pulse is set as the end of the CPI, as the start time of the CPIs is unknown. The current jamming percentage calculation affects the future jamming percentage estimations. The results show that the jamming percentage parameter has the biggest effect during threat evaluation and prioritisation. This is due to the percentage value altering from coincidence to coincidence depending on the standalone pulses that will be jammed, the total pulses in coincidence, and the required minimum jamming pulses. The jamming percentage parameter is more changeable than the mode, lethal range and zone assessment parameters which will mostly be constant throughout the interval or change slightly.

The only parameter that negatively impacts the mode assessment threat evaluation is the zone assessment parameter when the platform manoeuvres inside the burnthrough range. Both the jamming percentage and zone assessment parameter relies on the range parameters. The jamming percentage is dependent on the power levels of the radar signal and jammer signal as both powers are reliant on the distance between platform and threat. The zone assessment value is dependent on the platform in relation to the maximum detectable range and burnthrough range. Thus both parameters will be at maximum when the platform is inside the burnthrough range. These maximum parameters cause the lower valued pulses in coincidence to be disregarded as this radar will have the highest priority value. However, the zone assessment parameter is needed to determine where the platform is in regards to the range zones from the threat radar. Setting the zone assessment parameter as the lowest weight provides better evaluation over all of the pulses in coincidence.

Military intelligence services can gather intelligence on enemy radar modes, detection and lethal ranges, and waveform parameters. They are far easier to obtain than the signal detection parameters required to determine the jamming percentage value. However, the results show that determining the highest pulse in a coincidence can not be measured by the mode and range parameters alone. The fundamental part of determining the highest priority pulse in a coincidence depends on the jamming effectiveness of the CPI. A radar is successfully countered when the jammer knows the amount of noise energy required against coherently integrated signals, by lowering the probability of detection well below the required value. This provides the jammer with the capability to determine how many pulses need to counter in a CPI.

Overestimating the CPI size provides the benefit where the TIJ will determine that the radar has a higher integration gain due to an increase in coherent integration over the CPI. Overestimation results in more pulses from the overestimated CPI to be countered thereby creating a higher number of jamming pulses per CPI and a higher jamming percentage rate. However, underestimating the CPI causes the TIJ to predict a lower coherent integration gain which will cause the TIJ to determine an inferior jamming percentage where far fewer pulses are countered than what is required.

It is better to overestimate the minimum required probability of detection required to determine the percentage jamming value for the TIJ. The radar's probability of detection is most likely not known, however, the minimum probability of detection will provide the jammer with a known value used to determine the required minimum jamming pulses needed to inhibit detection in a CPI.

The probability of false alarm estimation is the parameter that a user can get as close to correct as possible. Over- and underestimation provides problems to the jammer in different ways. Overestimation may result in the jammer transmitting fewer pulses than what is required. Underestimating pulses increases the range of measurements which causes the mode assessment calculation to select the pulses that are incorrectly calculated as being close to burnthrough.

Overestimation is beneficial for all three signal detection parameters. However, overestimation still needs to be made conservatively. An increase in overestimation requires more jamming resources to be allocated to the radar resulting in the jamming percentage being skewed in favour of the highly overestimated radar. An overtly high overestimation value will result in wrongful prioritisation in coincidences as the pulse with an unnecessarily high jamming percentage is selected above pulses from radars can be of higher prioritisation.

For jamming effectiveness to hinder detection the jamming window size must be short enough to prevent an increase in the coincidence rate and keep the number of pulses in the coincidence as low as possible. Higher coincidence rates with a high rate of pulses in a coincidence are caused when the jamming window size is dependent on waveform parameters like the PRI. Radar PRIs are rather long ranging from microseconds to milliseconds. Relying on the jamming window size to be dependent on PRI will result in the jamming window length being ten to a hundred times larger than the actual pulse. Therefore, if the jamming window is rather dependent on the pulse width as opposed to the PRI then the TIJ will experience fewer coincidences and pulses in coincidence.

If the noise jammer is unable to counter a radar, due to high processing gain or the platform being inside the burnthrough range, then another jamming technique is required alongside noise jamming for TIJ. By using jamming techniques such as deception jamming may alleviate the strain of such conditions faced by the noise jammer where threat radars whose signal processing and integration schemes prevent the noise jammer from posing any hindrance in signal detection. The addition of noise and deception jamming will provide the TIJ to task each jamming type according to their jamming effectiveness against opposing radars.

5.1 RECOMMENDATION FOR FUTURE RESEARCH

5.1.1 TIJ and ESM interface

This dissertation assumes a perfect ES system, however, this is far from the case. Missed pulse detections, wrongful threat classification, clutter, intercepted signal reflections from the platform, signals under the MDS, etc., all play a part in the error of signal detection and classification. Moreover, ES systems have to capture and classify multitudes of the concurrent operating enemy and friendly radars (and the variety of radar modes per radar system) and communication systems, all varying within range, frequency, amplitude, pulse width and PRF. Threat radars are designed to detect targets at the lowest sensitivity possible with added protection against jamming systems. Examples of the electronic protection (EP) measure that radars may come equipped with, to increase the SNR of the receiver and protect and identify jamming are:

- pulse compression,
- coded waveforms,
- frequency hopping,
- Home-on-Jamming,
- integrated air-defence system (IADS),
- multi function radar,
- PRF jitter,
- PRF stagger,
- side lobe blanking,
- waveform diversity,
- clutter, and
- beam steering.

A lot of research has been done on PRI trackers and how to detect signals and classify the correct threat systems. Future research will be beneficial in determining the effectiveness and reliability of the TIJ system using ES systems with varying degrees of error rates in pulse characteristic measurements (especially TOA measurements and predictions) and threat classification.

All of the threat radars in the dissertation is set to locked-on. Each time interval, within a frequency range, will consist of the maximum amount of possible pulses of each threat radar available. But how will scanning patterns affect the sequence of time interval patterns? It is important to decrease the SNR of each threat radar as low as possible in their set jamming state. However, it is unclear how the TIJ will adapt to a threat only emitting over a short period in the interval. Research and experimentation are required to determine if the time interval duration should vary and/or if the states and frequency bands should be able to shift in a state sequence. This is to ensure that every one of the threat system's SNR (locked-on or scanning) will decrease the required amount in each state sequence.

Another area of concern for the TIJ controller is the detection of unknown threats. Threat systems are mobile and enemy combatants will manoeuver these systems around depending on their mission and objectives. This may result in the current knowledge of the threat situation at a given area being inaccurate. The current TIJ controller only works with information of known threat systems. Research is required to look at how to handle unknown threat systems that are not in the threat library.

5.1.2 Zone assessment

This dissertation assumes a constant RCS platform with perfect antennas in an idealised environment. The problem arises when large range error ellipses are measured as well as the addition of more losses (environment, platform ES and threat system receiver) and other factors (polarisation, main beam and side lobes). The zone values will be compromised if the platform can not determine the real range within a small error. It would be beneficial for the future scope of work for the zone assessment model on how to use range measurements affected by losses, clutter, and imperfect antennas providing large error ellipses.

5.1.3 Mode assessment

The aim of mode assessment as a model is to be interchangeable, with the resultant values to be normalised or exist within a predetermined range. There exist multiple different threat evaluation techniques to monitor and assess radar threats. The TIJ controller proposed in this dissertation derives the mode assessment (3.7) from an already peer-reviewed and tested threat evaluation technique (2.60). This technique is adequate for threat evaluation, however, future research can be beneficial in developing more finer resolution mode assessment techniques that focus on the pulse detection level of each radar mode. Other methods such as Bayesian reasoning and multiple artificial intelligence methods can be equipped, but as stated this model should be interchangeable in nature.

5.1.4 Effects from intermittent jamming

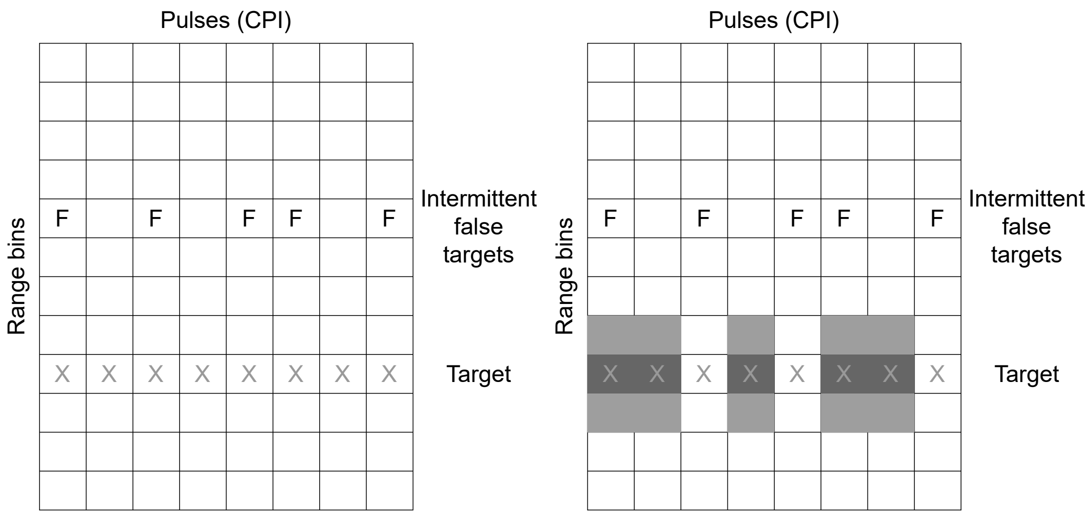
In this dissertation, intermittent jamming is studied as a way to determine the minimum amount of pulses required to hinder detection in a CPI. However, effects such as on-off jamming were disregarded.

On-off jamming is a form of power management jamming that is used to disrupt the active gain control (AGC) of the threat radar system. This jamming method forces the AGC to adjust the amplifier gain to the jamming bursts rather than the received reflected signals. On-off jamming aims to transmit jamming signals during the on period at a power level that is at the limit of the receiver amplifier. This causes the AGC to decrease the amplification of the received signal gain to try and compensate for the jamming signals. However, the reflected signals will still be lost due to the power saturation caused by the jamming signals. At the off period, the AGC is too low that received signal energy will not be amplified above the noise threshold [11].

5.1.5 Intermittent deception jamming

The research conducted for this dissertation only focuses on noise jamming however the effect of intermittent deception jamming, shown in Figure 5.1(a), should also be studied. Deception jamming has the advantage over noise jamming as the deception signal consists of the same characteristics of the radar's signal. This allows the deception signal voltage to also be squared when determining the SNR, whereas noise is averaged. Therefore intermittent deception jamming over a CPI will still obtain a higher SNR than what the echo signal can achieve.

Furthermore, the combination of intermittent noise jamming and intermittent deception jamming, as shown in Figure 5.1(b), can be advantageous for an EW system. Intermittent noise jamming will lower the probability of detection of the echo signals whilst the intermittent deception jamming signals can transmit enough pulses to maintain a constant probability of detection of the false target. Intermittent jamming will allow this technique to be used against multiple threats as not every echo signal needs to be jammed and the SNR of the deception signals over a CPI can be predicted to transmit the required deception pulses.



(a) Intermittent deception jamming **(b)** Intermittent deception and noise jamming

Figure 5.1. Implementing intermittent jamming in a CPI

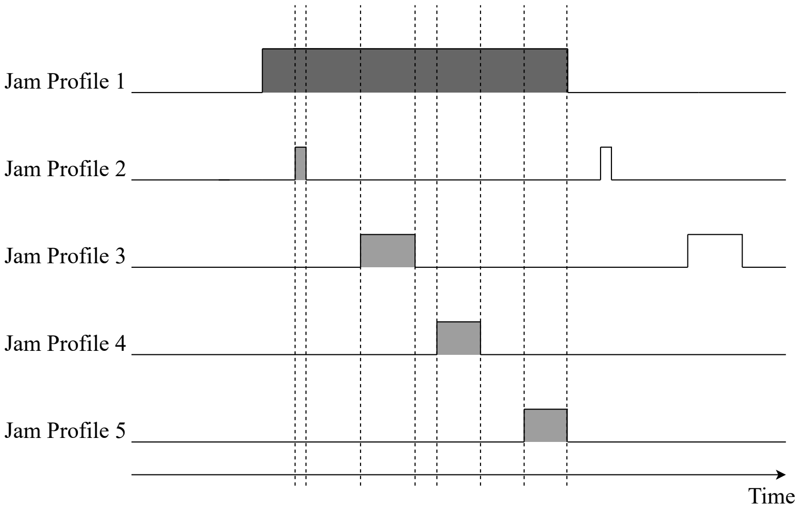


Figure 5.2. Single jammer pulse enveloping multiple standalone jammer pulses.

5.1.6 Coincidence scenarios

Multiple coincidence scenarios exist especially with jamming pulses having large pulse widths. Large pulse widths cause larger jamming windows which in turn envelope multiple jamming pulses. At some of these coincidences, it may be more advantageous to disregard the large pulse thereby resulting in the rest of the pulses being standalone and can be jammed as seen in Figure 5.2. A large jamming pulse as seen in Figure 5.3 may envelope multiple pulses from the same jamming envelope. Or as seen in Figure 5.4 a pulse may combine two coincidences into a single coincidence which may result in the pulse joining the others into a single coincidence to be selected as opposed to possibly two pulses being selected.

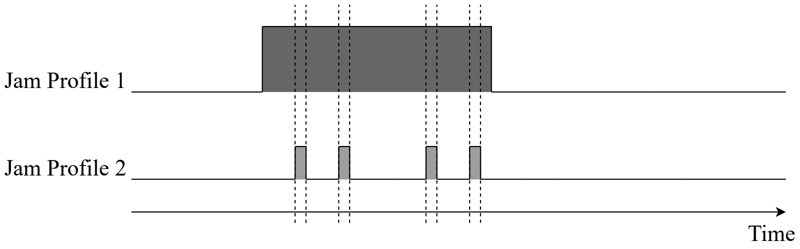


Figure 5.3. Single jammer pulse enveloping multiple jamming pulses of the same jamming envelope.

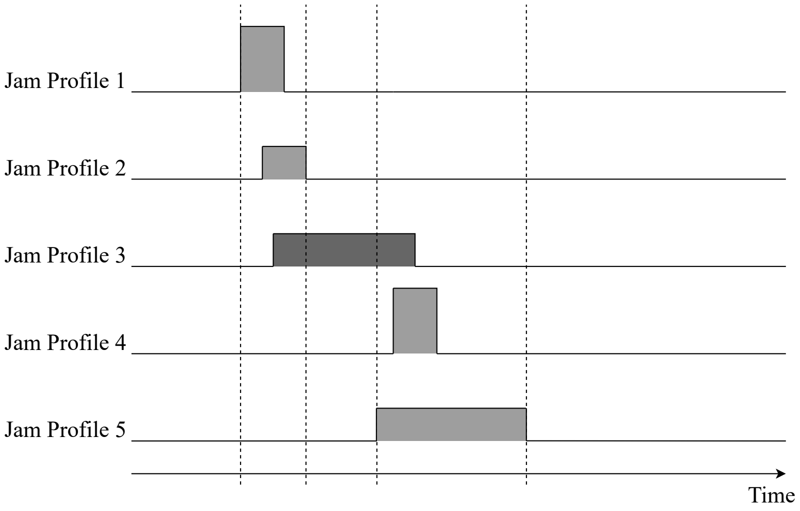


Figure 5.4. Jamming pulses joining two separate coincidences together.

Handling these types of scenarios in the future may be of benefit to the jamming effectiveness of the affected threat radars. Further analysis on these types of jamming pulses may be performed before the mode assessment algorithm to determine if these types of jamming pulses can be disregarded for the greater good of jamming effectiveness.

REFERENCES

[1] D. Schleher, *Introduction to Electronic Warfare*, 1st ed. Dedham, MA: Artech House, 1986.

[2] P. Kaszerman, “Frequency of pulse coincidence given n radars of different pulse widths and PRF’s,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-7, no. 5, pp. 1013–1014, 1971.

[3] N. Ahmed and H. Huang, “Distributed jammer network: Impact and characterization,” in *IEEE Military Communications Conference (MILCOM)*, 2009, pp. 1–6.

[4] “Radar and electronic warfare systems,” Janes. https://chembio.janes.com/ (accessed: September 1, 2020).

[5] J. Haystead, “Cognitive/adaptive learning requirements drive continuous advancement of DRFM technology,” *Journal of Electronic Defense*, vol. 42, no. 11, pp. 46–56, 2019.

[6] B. Zhang and W. Zhu, “Research on decision-making system of cognitive jamming against multifunctional radar,” in *IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 2019, pp. 1–6.

[7] C. Kopp, “The anatomy of the tacjammer,” Australian Aviation. http://www.ausairpower.net/TE-Tacjammer.html (accessed: April 19, 2021).

[8] G. T. Demos and M. S. Weprin, “Probability of pulse coincidence in a multiple radar environment,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-19, no. 4, pp. 635–640, 1983.

[9] S. Stein and D. Johansen, "A statistical description of coincidences among random pulse trains," *Proceedings of the IRE*, vol. 46, no. 5, pp. 827–830, 1958.

[10] D. A. Ephrath, "Atmospheric loss considerations in radar range equations," in *Digest on Antennas and Propagation Society International Symposium*, vol. 2, 1989, pp. 831–833.

[11] R. N. Lothes, M. B. Szymanski, and R. G. Wiley, *Radar Vulnerability to Jamming*. Norwood, MA: Artech House, 1990.

[12] J. Knowles, "Technology survey: a sampling of EW and SIGINT antenna systems," *Journal of Electronic Defense*, vol. 42, no. 8, pp. 31–40, 2019.

[13] R. A. Poisel, *Electronic Warfare Target Location Methods*, 2nd ed. Norwood, MA: Artech House, 2012.

[14] D. K. Barton, Ed., *Radar Equations for Modern Radar*. Norwood, MA: Artech House, 2013.

[15] L. Blake, *Radar Range-Performance Analysis*. Norwood, MA: Artech House, 1986.

[16] M. I. Skolnik, *Radar Handbook*, 2nd ed. New York: Mcgraw Hill, 1990.

[17] J. Eaves and E. Reedy, Eds., *Principles of Modern Radar*. New York: Van Nostrand Reinhold, 1987.

[18] F. E. Nathanson, J. P. Reilly, and M. N. Cohen, *Radar Design Principles: Signal Processing and the Environment*, 2nd ed. Mendham, New Jersey: SciTech Publishing, 1999.

[19] G. W. Stimson, *Introduction to Airborne Radar*, 2nd ed. New Jersey: SciTech Publishing, 1998.

[20] D. L. Adamy, *EW101: A first course in Electronic Warfare*, 1st ed. Boston, MA: Artech House, 2001.

[21] J. K. Kayani and A. J. Hashmi, “Comparative study of non-coherent pulse compression and non-coherent pulse integration techniques for radars,” in *14th International Radar Symposium (IRS)*, vol. 2, 2013, pp. 696–701.

[22] M. A. Richards, *Fundamentals of Radar Signal Processing*, 1st ed. New York: McGraw-Hill, 2005.

[23] M. A. Richards, J. A. Scheer, and W. A. Holm, *Principles of Modern Radar: Basic Principles*. Edison, NJ: SciTech Publishing, 2010, vol. 1.

[24] A. Golden, *Radar Electronic Warfare*. Washington, DC: AIAA, 1987.

[25] D. Orlando, “A novel noise jamming detection algorithm for radar applications,” *IEEE Signal Processing Letters*, vol. 24, no. 2, pp. 206–210, 2017.

[26] A. Zaimbashi and A. Sheikhi, “CFAR detectors in presence of jammer noise,” in *10th International Conference On Information Science, Signal Processing And Their Applications*, vol. 1, no. 1, 2010, pp. 426–429.

[27] D. K. Barton and S. A. Leonov, Eds., *Radar Technology Encyclopedia*. Norwood, MA: Artech House, 1998.

[28] E. P. Blasch, J. J. Salerno, and G. P. Tadda, “Measuring the worthiness of situation assessment,” in *Proceedings of the 2011 IEEE National Aerospace and Electronics Conference (NAECON)*, 2011, pp. 87–94.

[29] Qu Changwen and He You, “A method of threat assessment using multiple attribute decision making,” in *6th International Conference on Signal Processing, 2002.*, vol. 2, 2002, pp. 1091–1095.

[30] N. R. Osner and W. P. du Plessis, “Threat evaluation and jamming allocation,” *IET Radar, Sonar Navigation*, vol. 11, no. 3, pp. 459–465, 2017.

[31] N. R. Osner, “Countermeasure allocation and load-out optmisation,” Ph.D. dissertation, University of Pretoria, Pretoria, South Africa, 2019.

[32] N. Okello and G. Thorns, “Threat assessment using Bayesian networks,” in *6th International Conference of Information Fusion*, vol. 2, 2003, pp. 1102–1109.

[33] X. T. Nguyen, “Threat assessment in tactical airborne environments,” in *5th International Conference on Information Fusion (FUSION 2002)*, vol. 2, 2002, pp. 1300–1307.

[34] M. L. Hinman, “Some computational approaches for situation assessment and impact assessment,” in *5th International Conference on Information Fusion (FUSION 2002)*, vol. 1, 2002, pp. 687–693.

[35] G. Even, M. Halldórsson, L. Kaplan, and D. Ron, “Scheduling with conflicts: Online and offline algorithms,” *Journal of Scheduling*, vol. 12, pp. 199–224, 2009.

[36] “Mutual exclusion scheduling,” *Theoretical Computer Science*, vol. 162, no. 2, pp. 225 – 243, 1996.

[37] J. Mallett and L. Brennan, “Cumulative probability of detection for targets approaching a uniformly scanning search radar,” *Proceedings of the IEEE*, vol. 51, no. 4, pp. 596–601, 1963.

[38] J. Knowles and H. Swedeen, “Technology survey: a sampling of radar jammer,” *Journal of Electronic Defense*, vol. 43, no. 7, 2019.

ADDENDUM A THREAT RADARS

The page is intentionally left blank.

Table A.1. Simulator radar threat table

Radar ID	Weapon Range [km]	F_n [dB]	Mode	Peak power [kW]	Gain [dB]	Frequency [MHz]	Pulse width [µs]	PRI [µs]	CPI	Missed Pulses	Pd	Pfa
1	50	8.5										
			TS	25	30	9000	0.337	503.337	128	35	0.5	10e-6
			TA	25	30	9000	0.337	573.337	128	30	0.5	10e-6
			TT	25	30	9000	0.337	503.337	128	31	0.9	10e-6
			MG	25	30	9000	0.337	573.337	128	25	0.9	10e-6

Table A.1 continued from previous page

Radar ID	**Weapon Range [km]**	F_n **[dB]**	**Mode**	**Peak power [kW]**	**Gain [dB]**	**Frequency [MHz]**	**Pulse width [µs]**	**PRI [µs]**	**CPI**	**Missed Pulses**	**Pd**	**Pfa**
2	75	7										
			TS	200	25	4700	0.313	407.313	64	54	0.5	10e-6
			TA	200	25	4700	0.313	347.313	64	48	0.8	10e-6
			TT	200	25	4700	0.25	407.25	128	78	0.9	10e-6
			MG	200	25	4700	0.587	1507.587	128	48	0.9	10e-6

Table A.1 continued from previous page

Radar ID	Weapon Range [km]	F_n [dB]	Mode	Peak power [kW]	Gain [dB]	Frequency [MHz]	Pulse width [µs]	PRI [µs]	CPI	Missed Pulses	Pd	Pfa
3	40	7										
			TS	25	31	5000	0.5	533.5	128	60	0.9	10e-6
			TA	25	31	5000	0.5	566.5	64	48	0.8	10e-6
			TT	25	31	5000	0.5	466.5	64	44	0.8	10e-6
			MG	25	31	5000	6.4	31.4	32	9	0.9	10e-6

Table A.1 continued from previous page

Radar ID	Weapon Range [km]	F_n [dB]	Mode	Peak power [kW]	Gain [dB]	Frequency [MHz]	Pulse width [µs]	PRI [µs]	CPI	Missed Pulses	Pd	Pfa
4	100	7										
			TS	100	15	8000	49	1073	64	20	0.5	10e-6
			TA	100	15	8000	49	689	64	18	0.5	10e-6
			TT	100	15	8000	25	345	128	32	0.8	10e-6
			MG	100	15	8000	50	1074	64	28	0.8	10e-6

Table A.1 continued from previous page

Radar ID	**Weapon Range [km]**	F_n **[dB]**	**Mode**	**Peak power [kW]**	**Gain [dB]**	**Frequency [MHz]**	**Pulse width [µs]**	**PRI [µs]**	**CPI**	**Missed Pulses**	**Pd**	**Pfa**
5	50	7										
			TS	45	27	10000	0.240	240.24	128	50	0.5	10e-6
			TA	45	27	10000	0.180	230.18	128	90	0.9	10e-6
			TT	45	27	10000	0.175	200.175	128	75	0.8	10e-6
			MG	45	27	10000	1.75	181.75	64	12	0.9	10e-6

Table A.1 continued from previous page

Radar ID	**Weapon Range [km]**	F_n **[dB]**	**Mode**	**Peak power [kW]**	**Gain [dB]**	**Frequency [MHz]**	**Pulse width [µs]**	**PRI [µs]**	**CPI**	**Missed Pulses**	**Pd**	**Pfa**
6	100	7										
			TS	200	25	2500	6.9	146.9	64	12	0.8	10e-6
			TA	200	25	2500	5.3	125.3	64	21	0.9	10e-6
			TT	200	25	2500	5	517	64	15	0.8	10e-6
			MG	200	25	2500	5	261	64	18	0.9	10e-6

Table A.1 continued from previous page

Radar ID	**Weapon Range [km]**	F_n **[dB]**	**Mode**	**Peak power [kW]**	**Gain [dB]**	**Frequency [MHz]**	**Pulse width [µs]**	**PRI [µs]**	**CPI**	**Missed Pulses**	**Pd**	**Pfa**
7	150	7										
			TS	42	27	3000	12.5	1012.5	64	30	0.9	10e-6
			TA	42	27	3000	12.5	1412.5	64	25	0.9	10e-6
			TT	42	27	3000	0.9	20.9	256	130	0.8	10e-6
			MG	42	27	3000	0.2	12.2	256	150	0.9	10e-6

Table A.1 continued from previous page

Radar ID	Weapon Range [km]	F_n [dB]	Mode	Peak power [kW]	Gain [dB]	Frequency [MHz]	Pulse width [µs]	PRI [µs]	CPI	Missed Pulses	Pd	Pfa
8	150	7										
			TS	50	22	3000	36	4036	32	12	0.5	10e-6
			TA	50	22	3000	72	1072	64	15	0.9	10e-6
			TT	50	22	3000	25	525	64	20	0.8	10e-6
			MG	50	22	3000	10	260	128	40	0.9	10e-6

Table A.1 continued from previous page

Radar ID	**Weapon Range [km]**	F_n **[dB]**	**Mode**	**Peak power [kW]**	**Gain [dB]**	**Frequency [MHz]**	**Pulse width [µs]**	**PRI [µs]**	**CPI**	**Missed Pulses**	**Pd**	**Pfa**
9	145	7										
			TS	10	34	9200	10	60	64	20	0.5	10e-6
			TA	10	34	9200	7.5	57.5	64	15	0.5	10e-6
			TT	10	34	9200	5	55	64	12	0.5	10e-6
			MG	10	34	9200	4.5	54.5	64	14	0.5	10e-6

Table A.1 continued from previous page

Radar ID	**Weapon Range [km]**	F_n **[dB]**	**Mode**	**Peak power [kW]**	**Gain [dB]**	**Frequency [MHz]**	**Pulse width [µs]**	**PRI [µs]**	**CPI**	**Missed Pulses**	**Pd**	**Pfa**
10	80	7										
			TS	150	28	5000	2.5	602.5	64	17	0.8	10e-6
			TA	150	28	5000	1.5	341.5	64	10	0.9	10e-6
			TT	150	28	5000	0.5	380.2	128	10	0.8	10e-6
			MG	150	28	5000	0.9	350	64	12	0.9	10e-6

Table A.1 continued from previous page

Radar ID	**Weapon Range [km]**	F_n **[dB]**	**Mode**	**Peak power [kW]**	**Gain [dB]**	**Frequency [MHz]**	**Pulse width [µs]**	**PRI [µs]**	**CPI**	**Missed Pulses**	**Pd**	**Pfa**
11	100	7										
			TS	150	22	8000	10	59	64	18	0.9	10e-6
			TA	150	22	8000	5	50	64	20	0.9	10e-6
			TT	150	22	8000	3	52.9	128	12	0.8	10e-6
			MG	150	22	8000	4	53.75	128	5	0.9	10e-6

Table A.1 continued from previous page

Radar ID	Weapon Range [km]	F_n [dB]	Mode	Peak power [kW]	Gain [dB]	Frequency [MHz]	Pulse width [μs]	PRI [μs]	CPI	Missed Pulses	Pd	Pfa
12	30	8.5										
			TS	20	35	9375	2	802	32	5	0.9	10e-6
			TA	20	35	9375	1.5	401.5	32	8	0.9	10e-6
			TT	20	35	9375	0.5	400.5	64	4	0.9	10e-6
			MG	20	35	9375	0.75	512.75	64	3	0.9	10e-6

Table A.1 continued from previous page

Radar ID	Weapon Range [km]	F_n [dB]	Mode	Peak power [kW]	Gain [dB]	Frequency [MHz]	Pulse width [µs]	PRI [µs]	CPI	Missed Pulses	Pd	Pfa
13	80	4										
			TS	15	35	7500	15	2515	32	5	0.9	10e-6
			TA	15	35	7500	10	1260	32	8	0.9	10e-6
			TT	15	35	7500	5	130	64	12	0.9	10e-6
			MG	15	35	7500	5	230	64	9	0.9	10e-6

Table A.1 continued from previous page

Radar ID	**Weapon Range [km]**	F_n **[dB]**	**Mode**	**Peak power [kW]**	**Gain [dB]**	**Frequency [MHz]**	**Pulse width [µs]**	**PRI [µs]**	**CPI**	**Missed Pulses**	**Pd**	**Pfa**
14	50	9										
			TS	50	15	2200	15.1	215.1	64	25	0.9	10e-6
			TA	50	15	2200	12.3	2612.3	64	18	0.9	10e-6
			TT	50	15	2200	6.5	672.5	64	12	0.9	10e-6
			MG	50	15	2200	8	674	64	19	0.9	10e-6

Table A.1 continued from previous page

Radar ID	**Weapon Range [km]**	F_n **[dB]**	**Mode**	**Peak power [kW]**	**Gain [dB]**	**Frequency [MHz]**	**Pulse width [µs]**	**PRI [µs]**	**CPI**	**Missed Pulses**	**Pd**	**Pfa**
15	80	9										
			TS	130	31	3100	2.45	1335.45	50	5	0.9	10e-6
			TA	130	31	3100	2	1302	50	8	0.9	10e-6
			TT	130	31	3100	0.45	450.45	100	12	0.9	10e-6
			MG	130	31	3100	1.2	401.2	50	9	0.9	10e-6

Table A.1 continued from previous page

Radar ID	Weapon Range [km]	F_n [dB]	Mode	Peak power [kW]	Gain [dB]	Frequency [MHz]	Pulse width [µs]	PRI [µs]	CPI	Missed Pulses	Pd	Pfa
16	125	7										
			TS	150	25	2250	3	1003	64	12	0.5	10e-6
			TA	150	25	2250	2	752	64	15	0.5	10e-6
			TT	150	25	2250	1.55	501.55	64	18	0.5	10e-6
			MG	150	25	2250	2.1	252.1	64	9	0.5	10e-6

Table A.1 continued from previous page

Radar ID	Weapon Range [km]	F_n [dB]	Mode	Peak power [kW]	Gain [dB]	Frequency [MHz]	Pulse width [µs]	PRI [µs]	CPI	Missed Pulses	Pd	Pfa
17	150	5										
			TS	50	31	5200	15.4	1237.4	64	12	0.9	10e-6
			TA	50	31	5200	12.75	1134.75	64	15	0.8	10e-6
			TT	50	31	5200	10.88	921.88	64	18	0.8	10e-6
			MG	50	31	5200	9.98	131.98	64	9	0.9	10e-6

Table A.1 continued from previous page

Radar ID	**Weapon Range [km]**	F_n **[dB]**	**Mode**	**Peak power [kW]**	**Gain [dB]**	**Frequency [MHz]**	**Pulse width [µs]**	**PRI [µs]**	**CPI**	**Missed Pulses**	**Pd**	**Pfa**
18	25	5										
			TS	26	20	1910	0.8	93	128	20	0.8	10e-6
			TA	26	20	1910	0.6	93	128	35	0.8	10e-6
			TT	26	20	1910	0.4	93	128	24	0.8	10e-6
			MG	26	20	1910	0.5	93	128	9	0.8	10e-6

Table A.1 continued from previous page

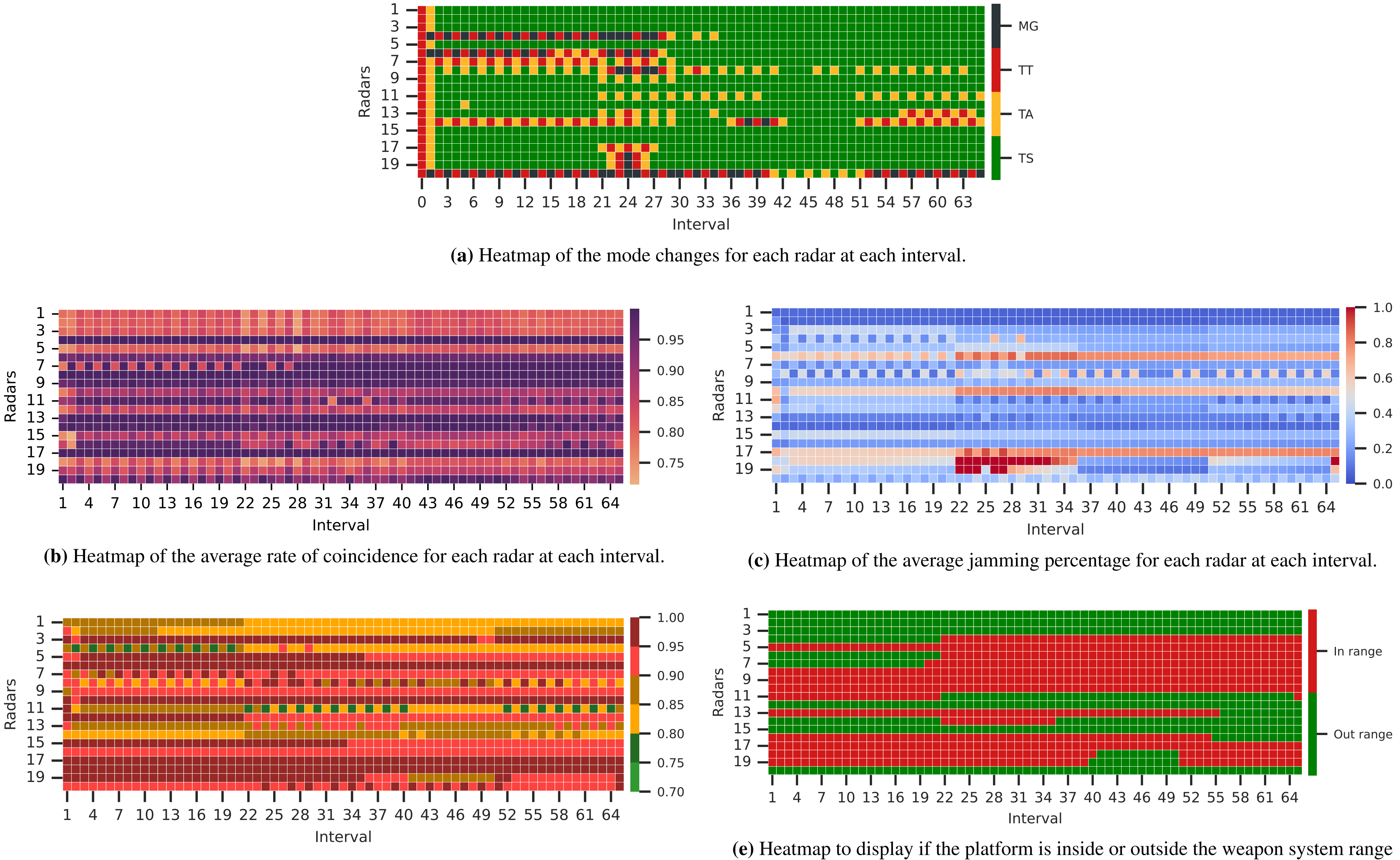
Radar ID	Weapon Range [km]	F_n [dB]	Mode	Peak power [kW]	Gain [dB]	Frequency [MHz]	Pulse width [µs]	PRI [µs]	CPI	Missed Pulses	Pd	Pfa
19	25	2										
			TS	47	15	6350	3.2	32	64	10	0.8	10e-6
			TA	47	15	6350	4.1	32	64	14	0.8	10e-6
			TT	47	15	6350	3.55	30	64	13	0.8	10e-6
			MG	47	15	6350	2.9	28	32	14	0.5	10e-6

Table A.1 continued from previous page

Radar ID	Weapon Range [km]	F_n [dB]	Mode	Peak power [kW]	Gain [dB]	Frequency [MHz]	Pulse width [µs]	PRI [µs]	CPI	Missed Pulses	Pd	Pfa
20	50	4										
			TS	6.5	28	8750	15	65	128	25	0.9	10e-6
			TA	6.5	28	8750	12	58	128	30	0.9	10e-6
			TT	6.5	28	8750	10	50	128	35	0.9	10e-6
			MG	6.5	28	8750	7	42	128	38	0.9	10e-6

ADDENDUM B TEST RESULTS

The page is intentionally left blank.



(a) Heatmap of the mode changes for each radar at each interval.

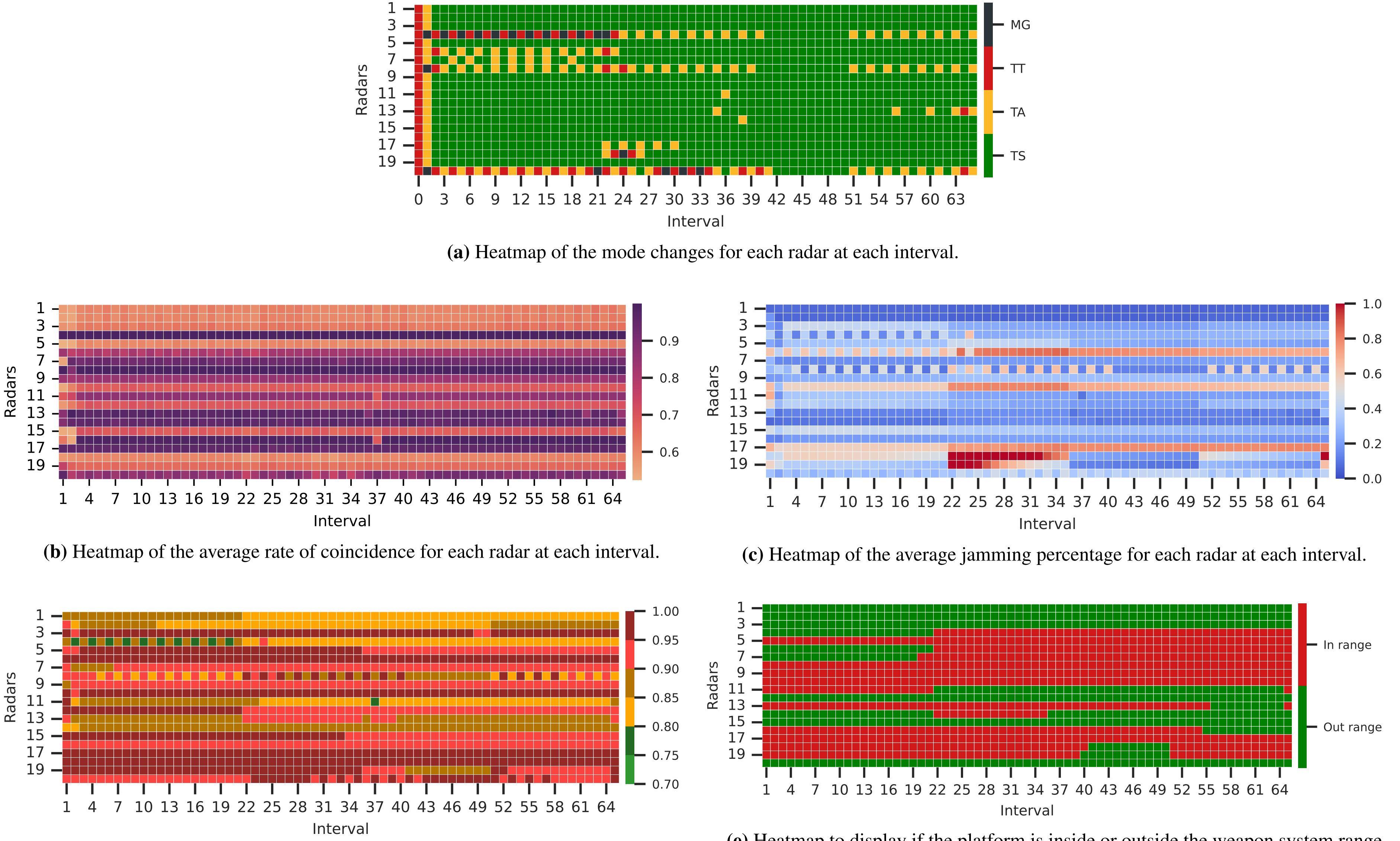
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.1. Mode assessment test with weights set at $W_s = 0.5, W_r = 0.5, W_l = 0, W_j = 0$ and jamming window = pulse width.



(a) Heatmap of the mode changes for each radar at each interval.

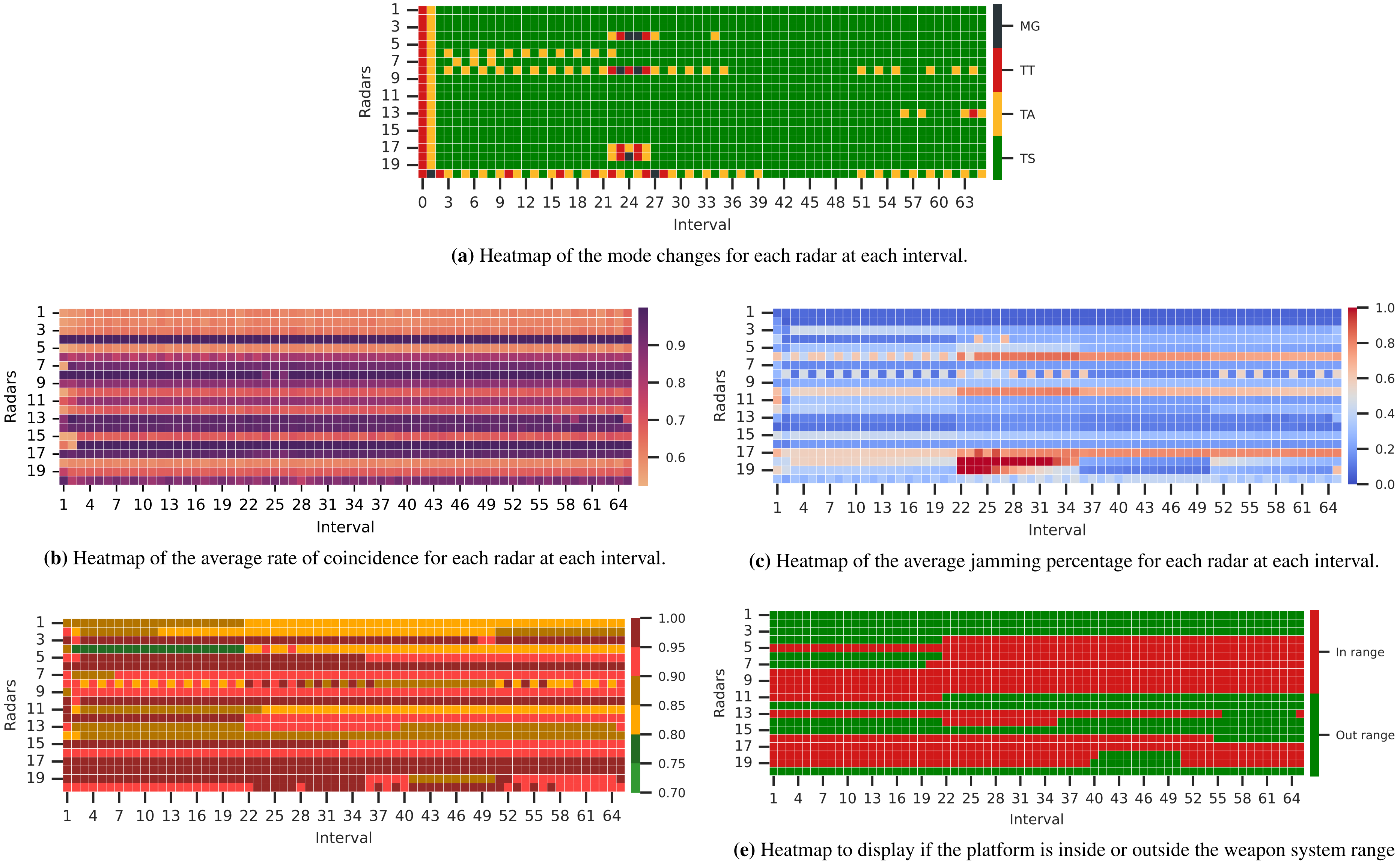
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.2. Mode assessment test with weights set at $W_s = 0.33, W_r = 0.33, W_l = 0.34, W_j = 0$ and jamming window = pulse width.



(a) Heatmap of the mode changes for each radar at each interval.

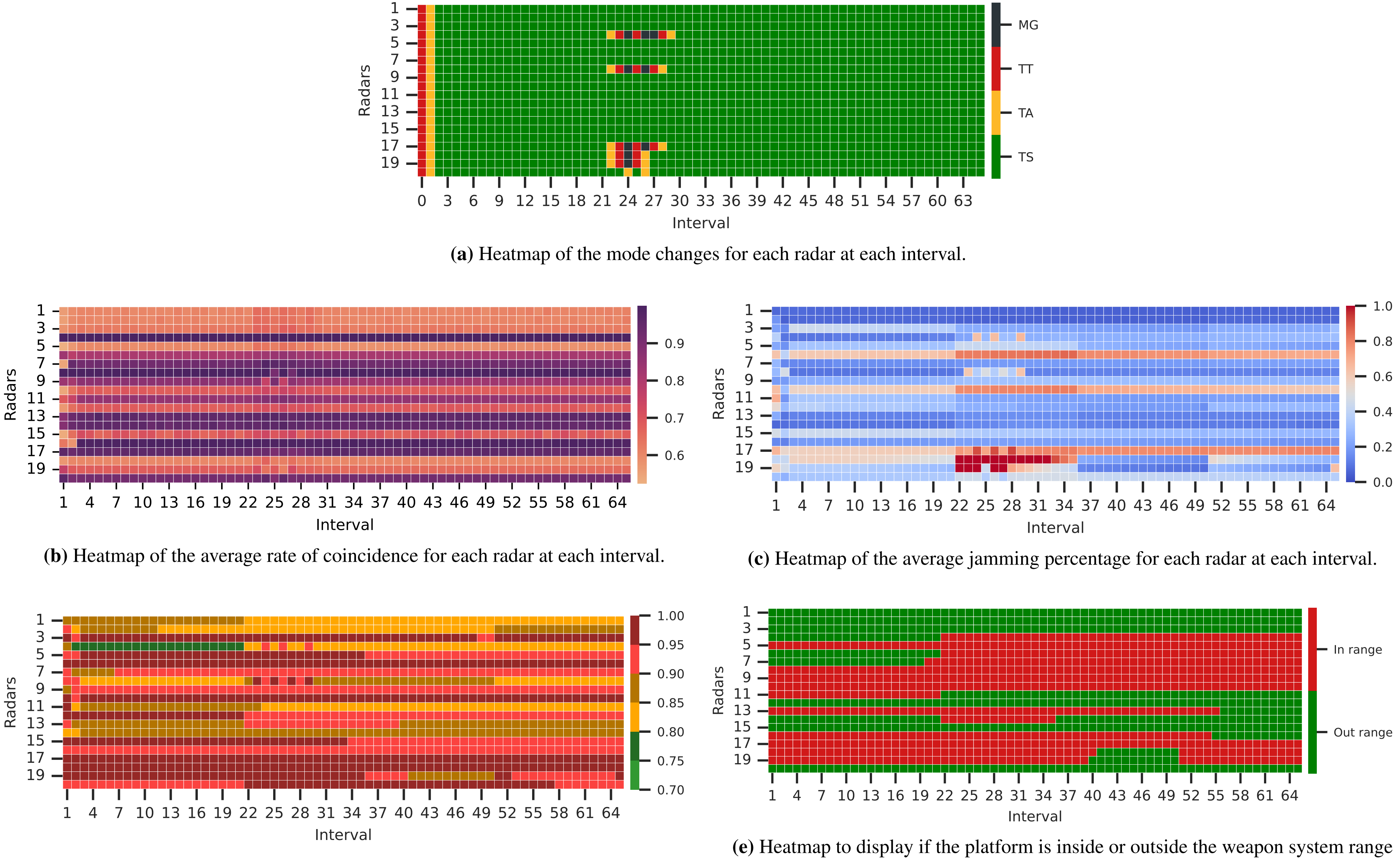
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.3. Mode assessment test with with weights set at $W_s = 0.25, W_r = 0.25, W_l = 0.25, W_j = 0.25$ and jamming window = pulse width.



(a) Heatmap of the mode changes for each radar at each interval.

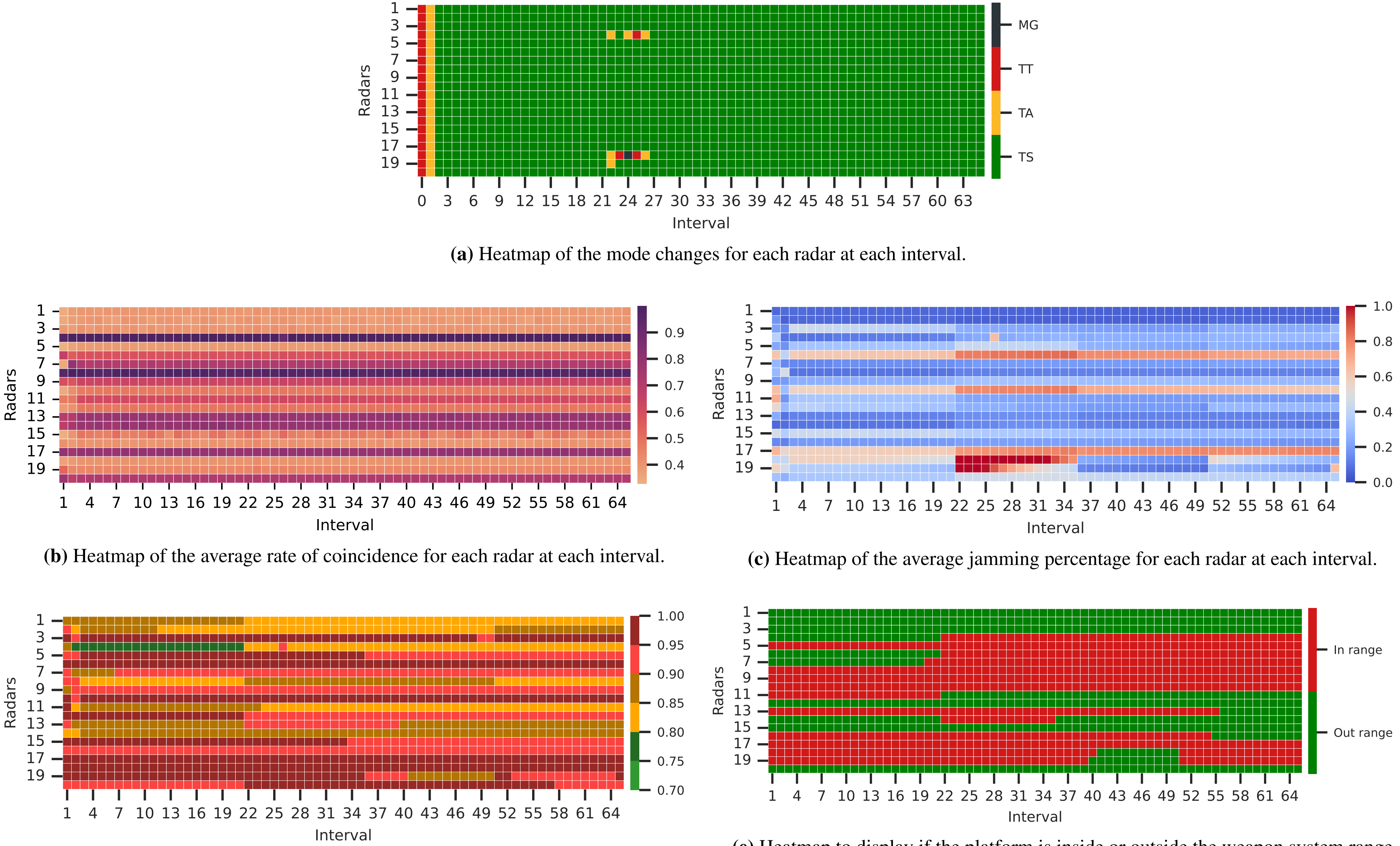
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.4. Mode assessment test with weights set at $W_s = 0.0, W_r = 0.0, W_l = 0.0, W_j = 1.0$ and jamming window = pulse width.



(a) Heatmap of the mode changes for each radar at each interval.

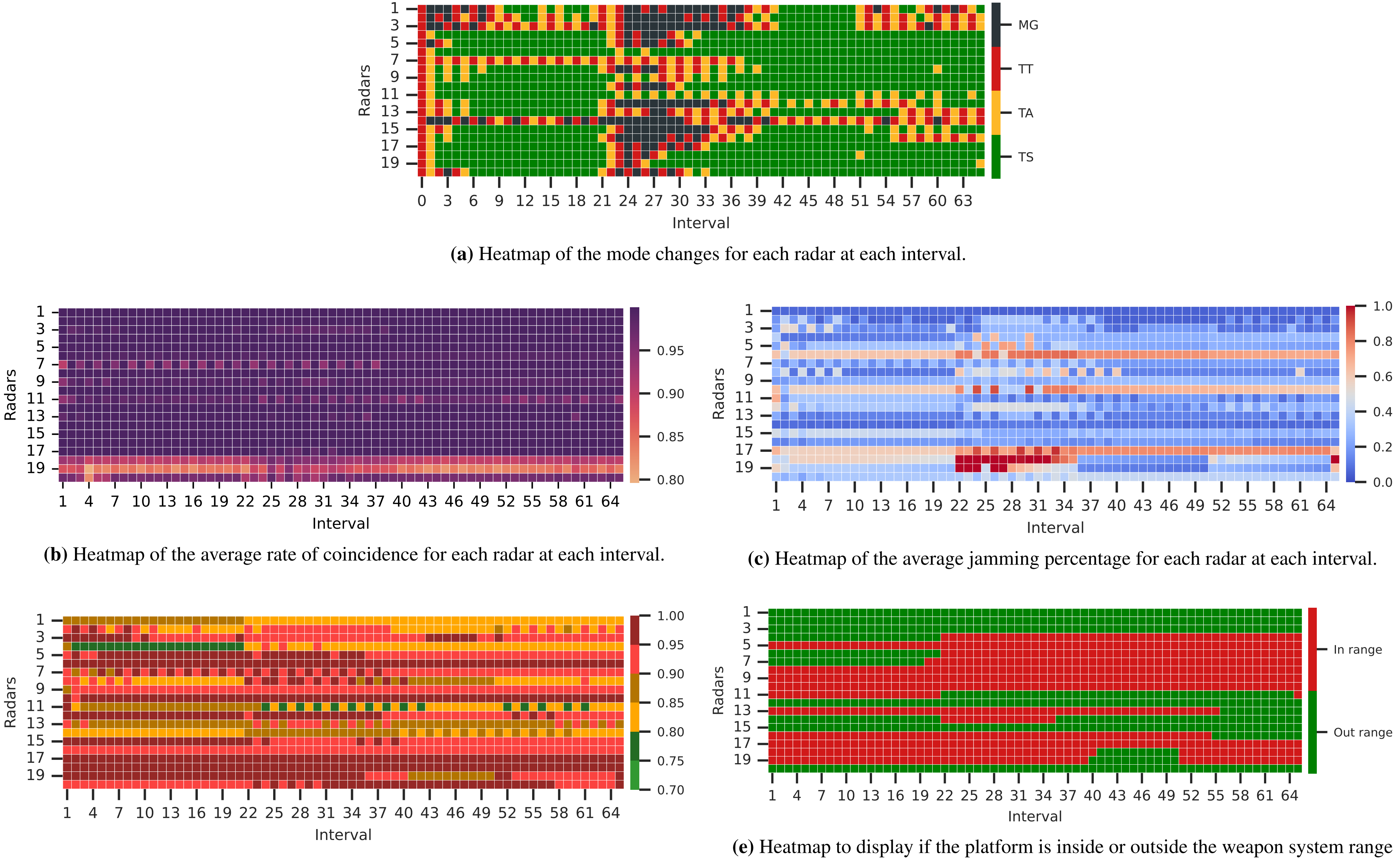
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.5. Mode assessment test with weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window = pulse width.



(a) Heatmap of the mode changes for each radar at each interval.

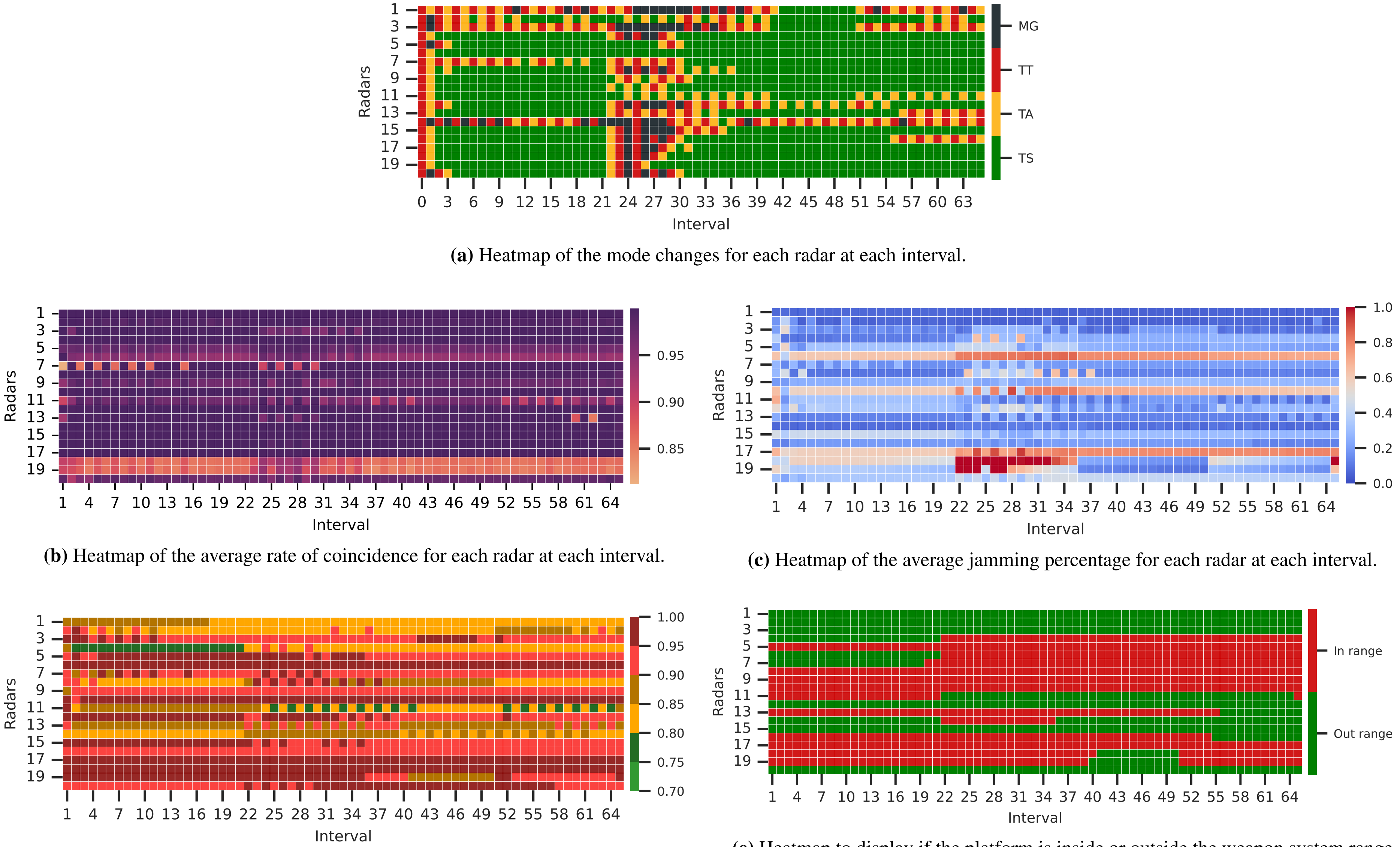
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.6. Mode assessment test with weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window = 10% of PRI.



(a) Heatmap of the mode changes for each radar at each interval.

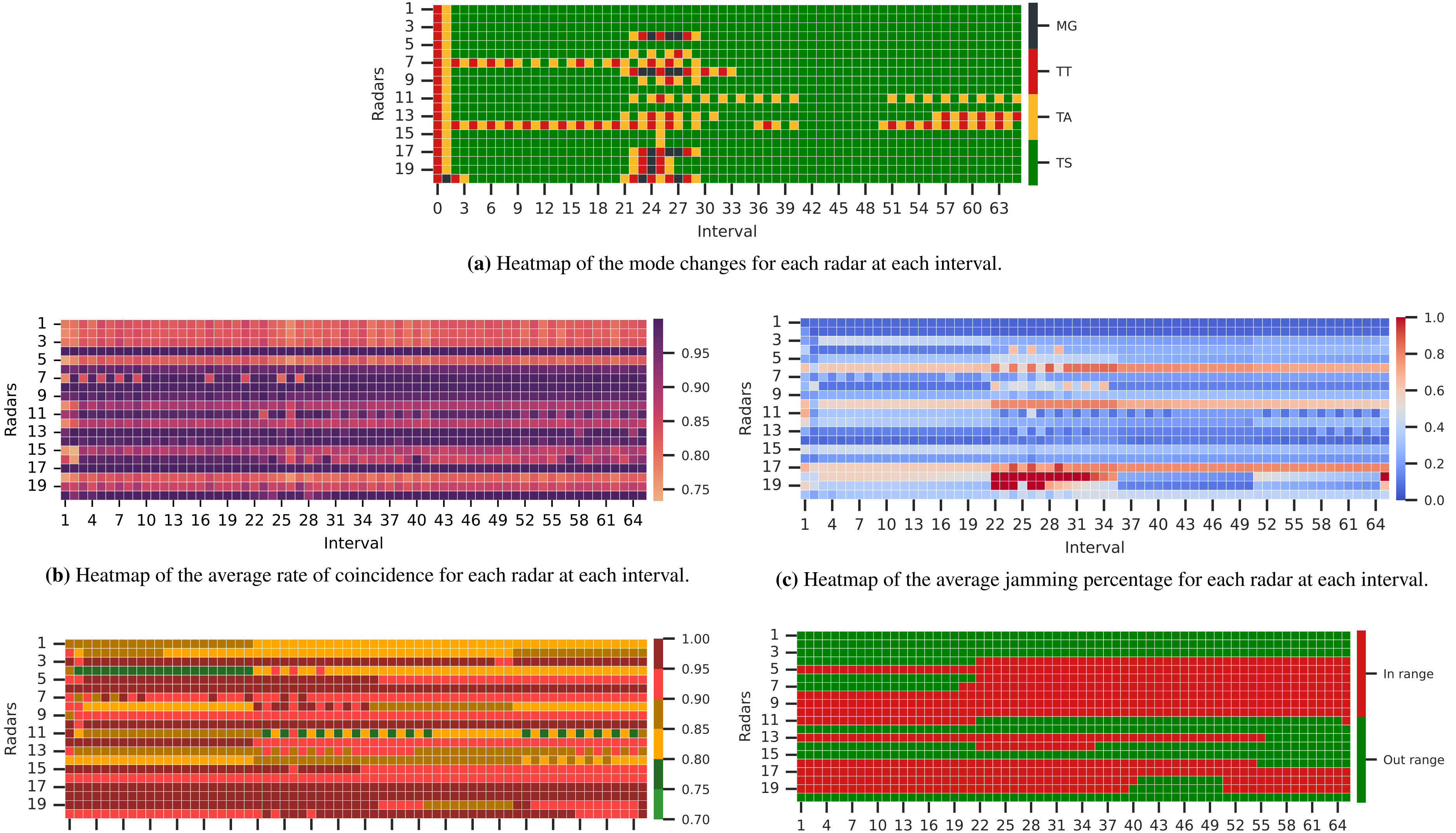
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.7. Mode assessment test with weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window = 5% of PRI.



(a) Heatmap of the mode changes for each radar at each interval.

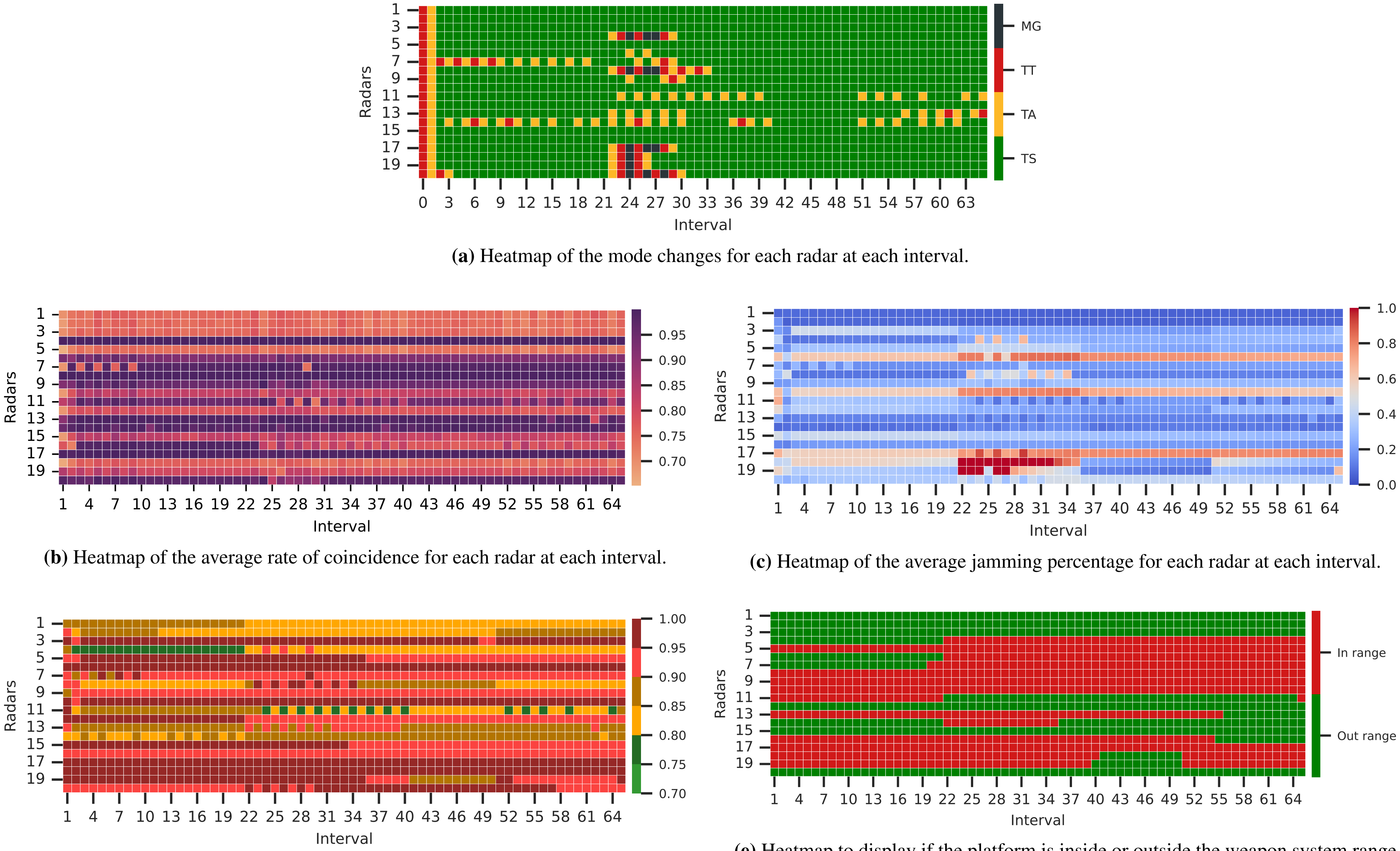
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.8. Mode assessment test with weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window = 1.75 times the signal pulse width.



(a) Heatmap of the mode changes for each radar at each interval.

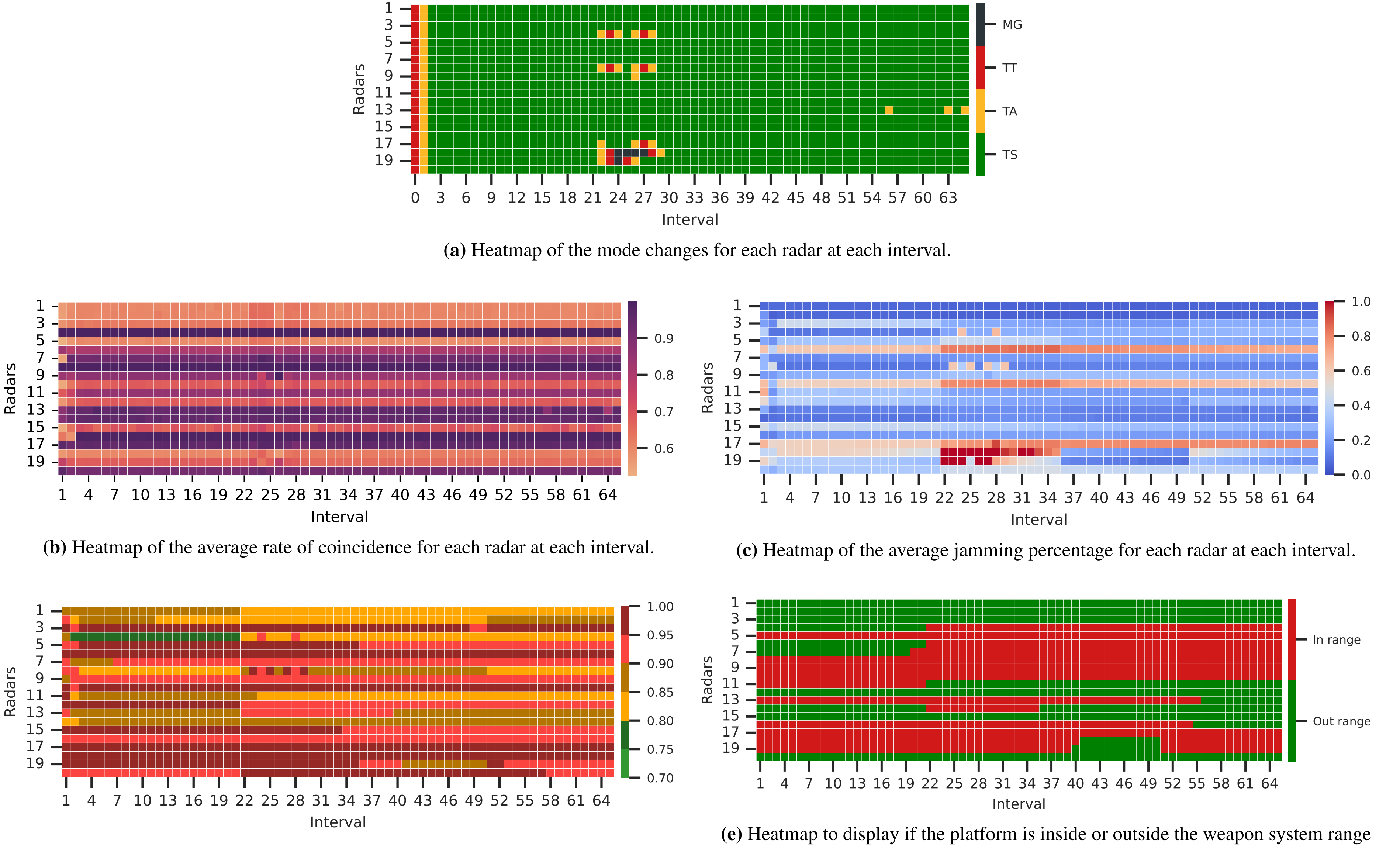
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.9. Mode assessment test with weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window with cut-off 5% after signal pulse falling edge.



(a) Heatmap of the mode changes for each radar at each interval.

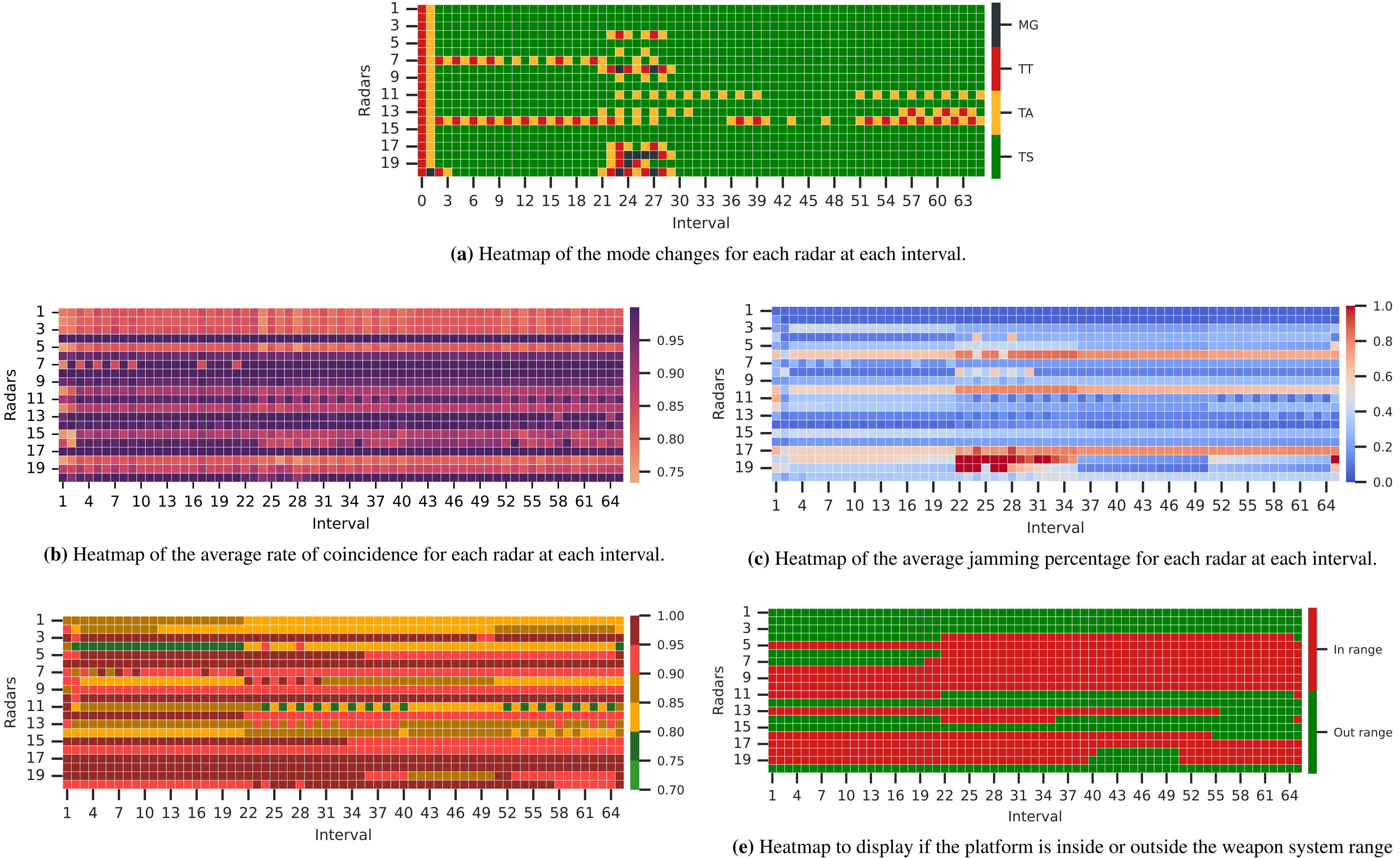
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.10. Ignoring radars in burnthrough test with weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and and jamming window = pulse width.



(a) Heatmap of the mode changes for each radar at each interval.

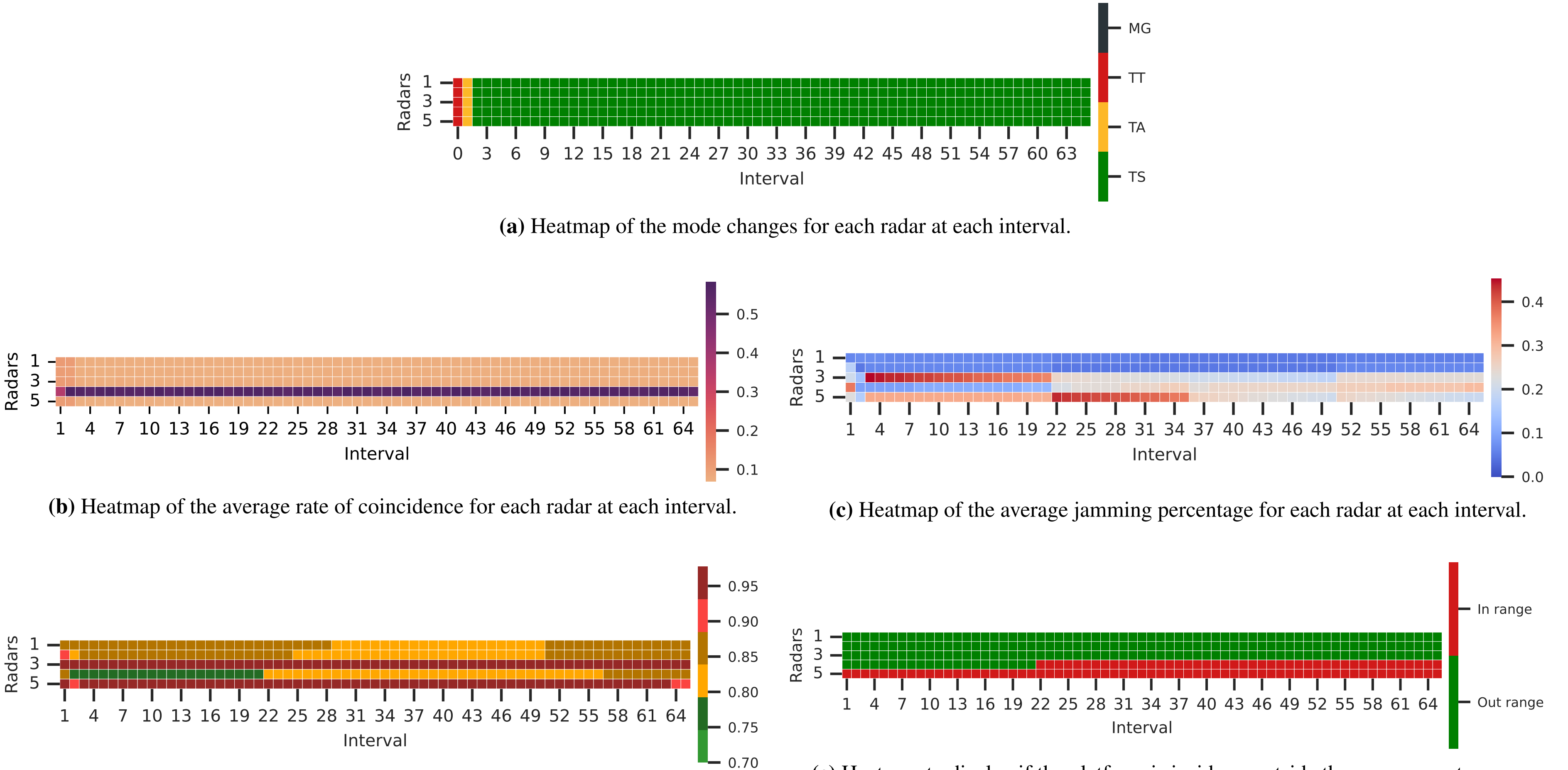
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.11. Ignoring radars in burnthrough test with weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window with cut-off 5% after signal pulse falling edge.



(a) Heatmap of the mode changes for each radar at each interval.

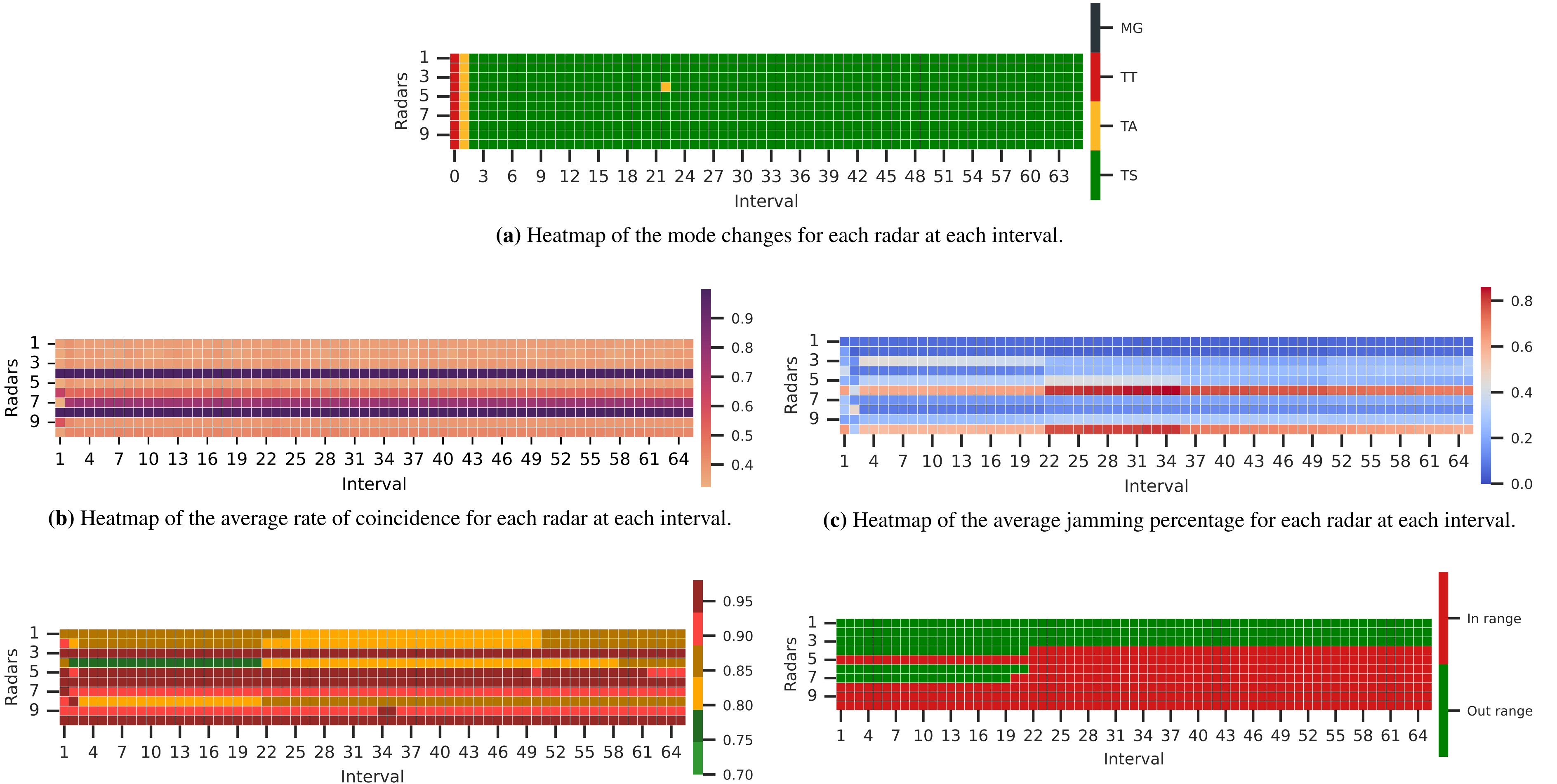
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.12. Single jammer channel against 5 coherent radars with weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window with cut-off 5% after signal pulse falling edge



(a) Heatmap of the mode changes for each radar at each interval.

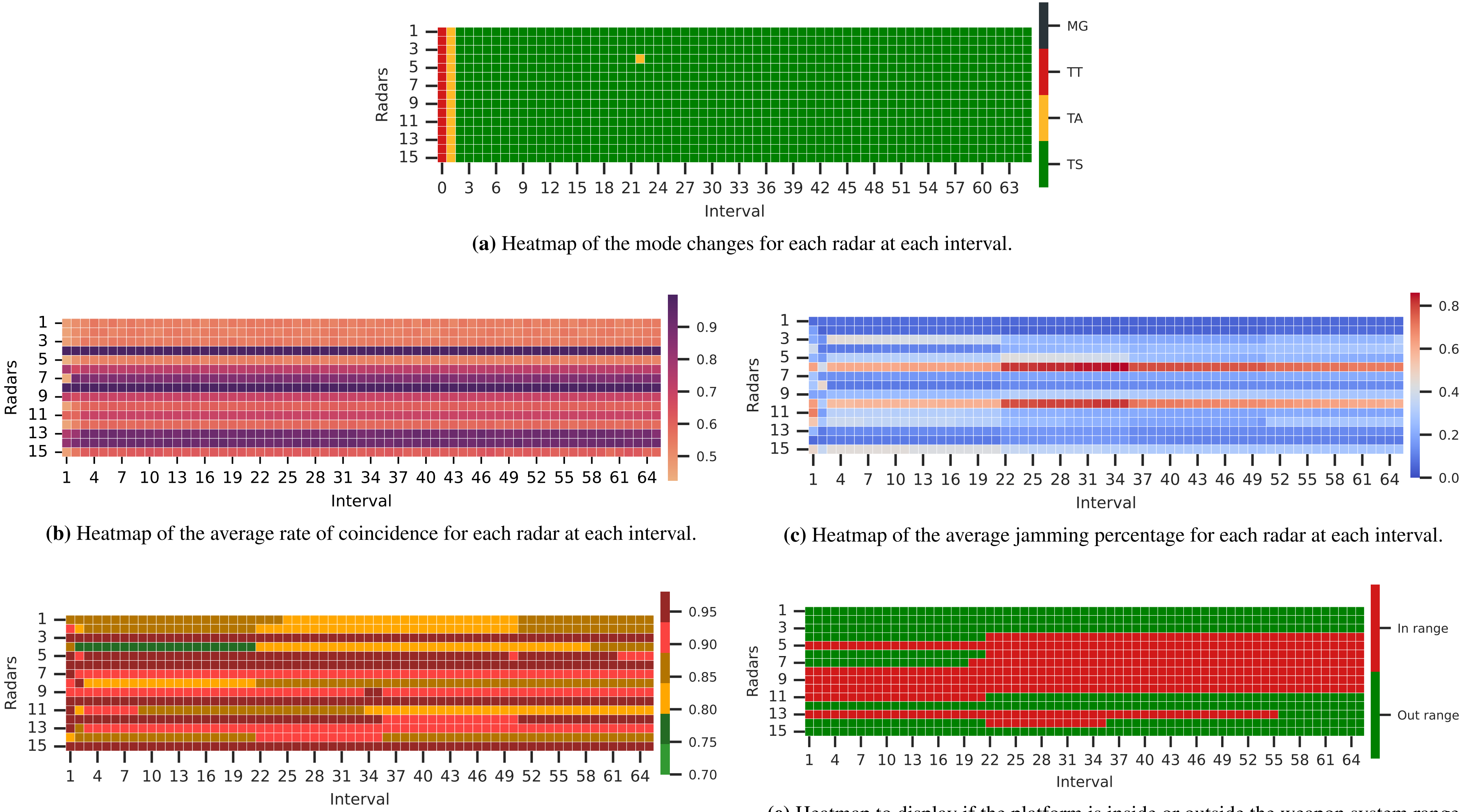
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.13. Single jammer channel against 10 coherent radars with weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window with cut-off 5% after signal pulse falling edge



(a) Heatmap of the mode changes for each radar at each interval.

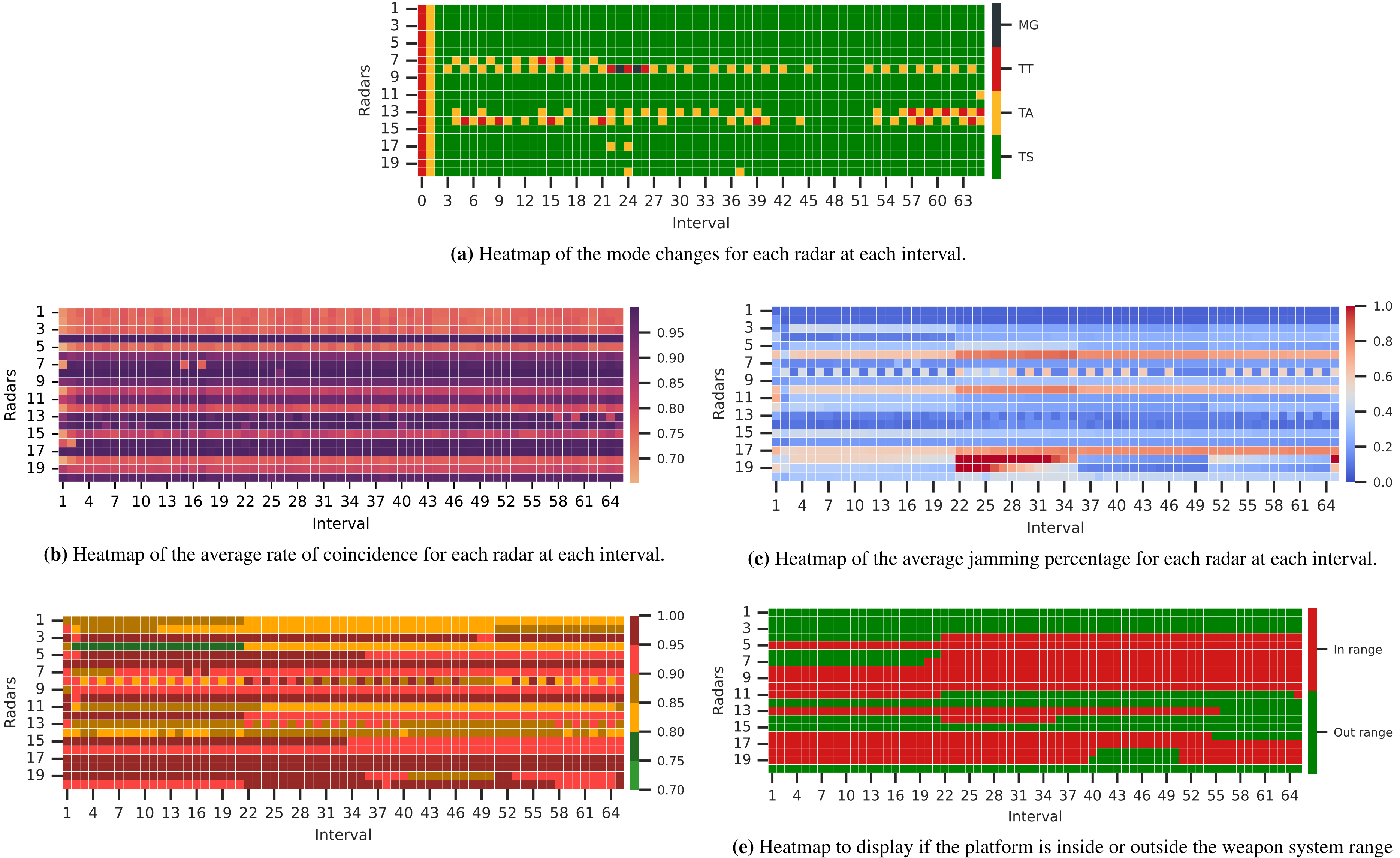
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.14. Single jammer channel against 15 coherent radars with weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window with cut-off 5% after signal pulse falling edge



(a) Heatmap of the mode changes for each radar at each interval.

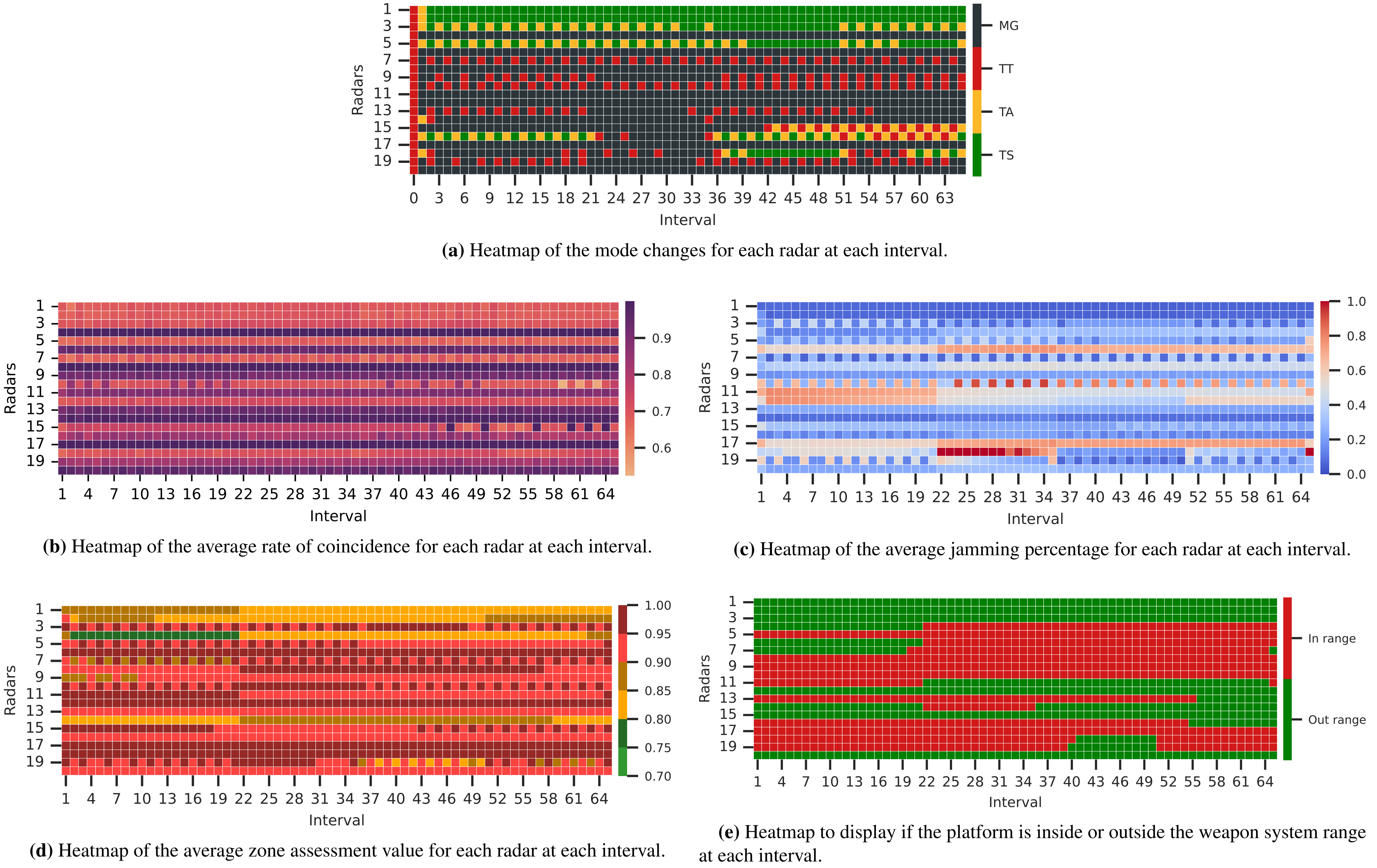
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.15. Overestimation of the CPI size for all threats with mode assessment weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window with cut-off 5% after signal pulse falling edge



(a) Heatmap of the mode changes for each radar at each interval.

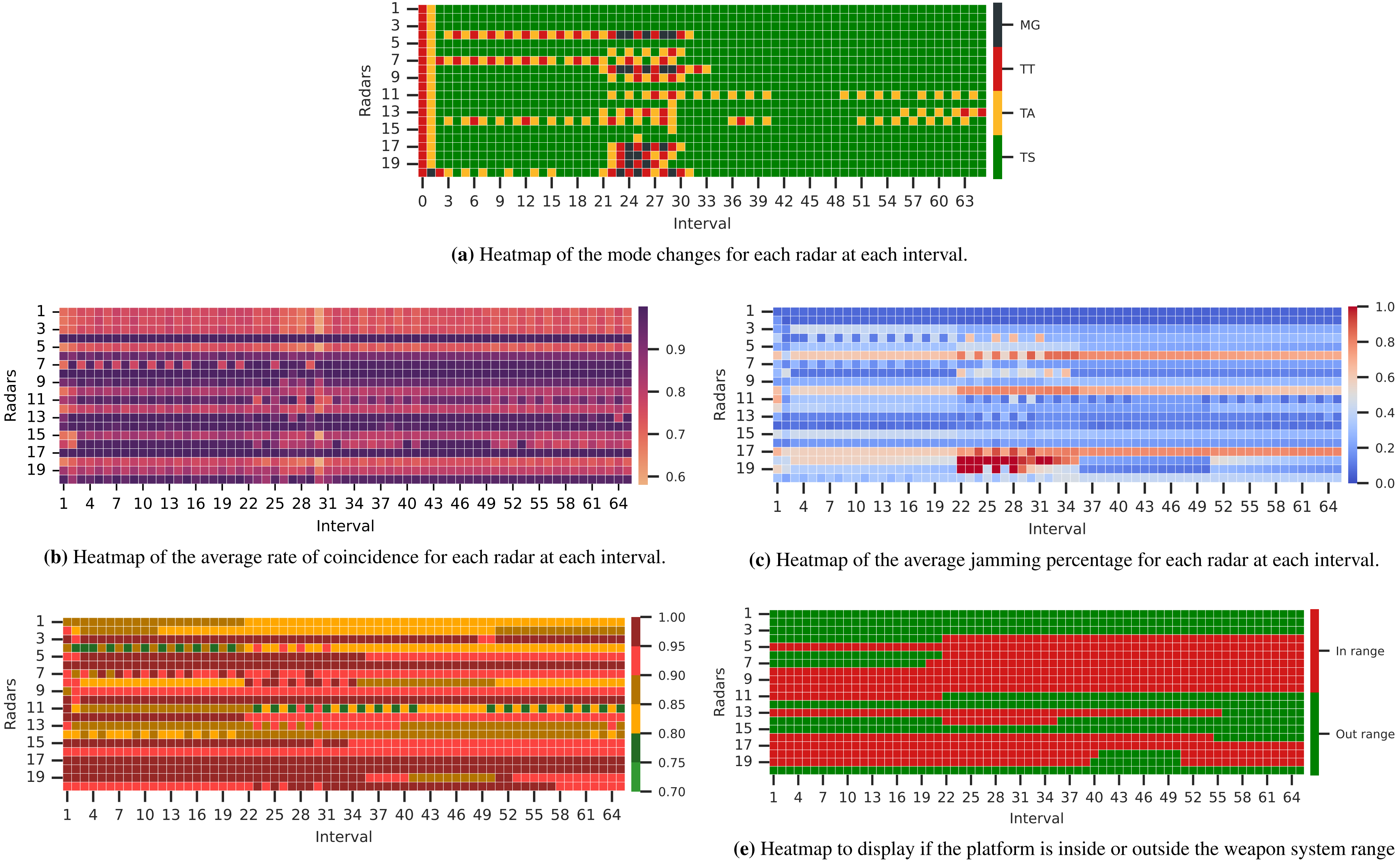
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.16. Underestimation of the CPI size for all threats with mode assessment weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window with cut-off 5% after signal pulse falling edge



(a) Heatmap of the mode changes for each radar at each interval.

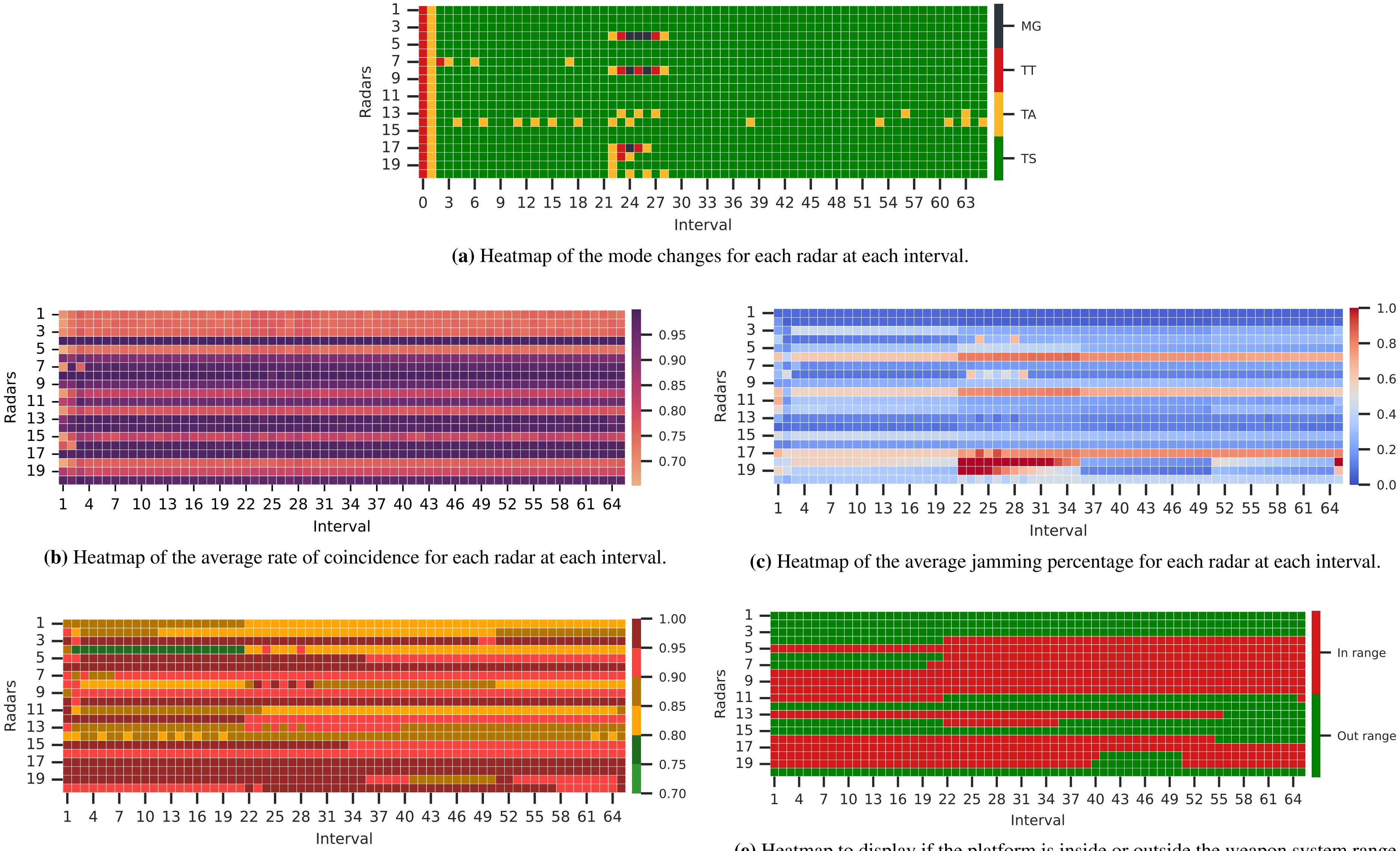
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.17. Overestimation of the probability of detection for all threats with mode assessment weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window with cut-off 5% after signal pulse falling edge



(a) Heatmap of the mode changes for each radar at each interval.

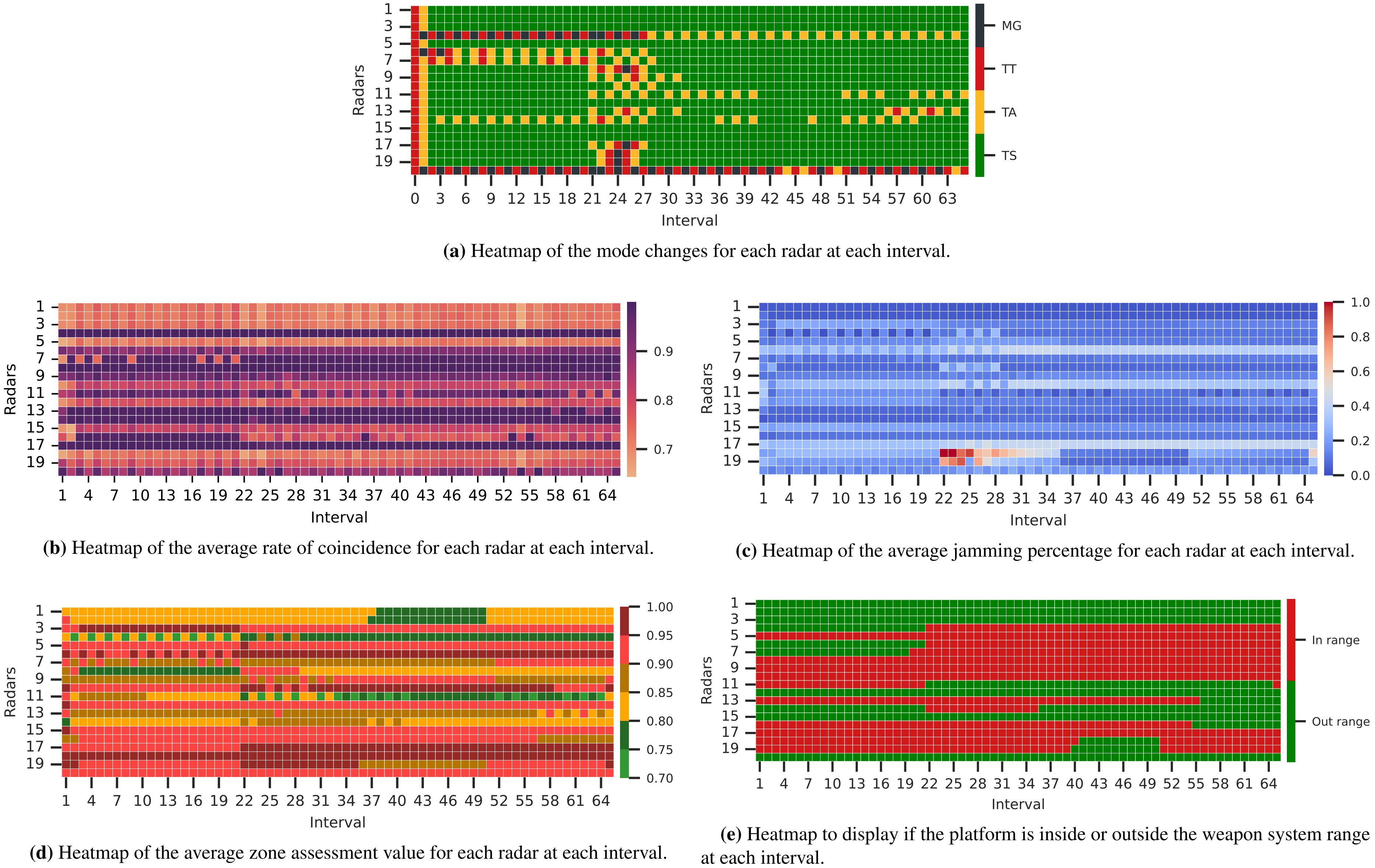
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.18. Underestimation of the probability of detection for all threats with mode assessment weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window with cut-off 5% after signal pulse falling edge



(a) Heatmap of the mode changes for each radar at each interval.

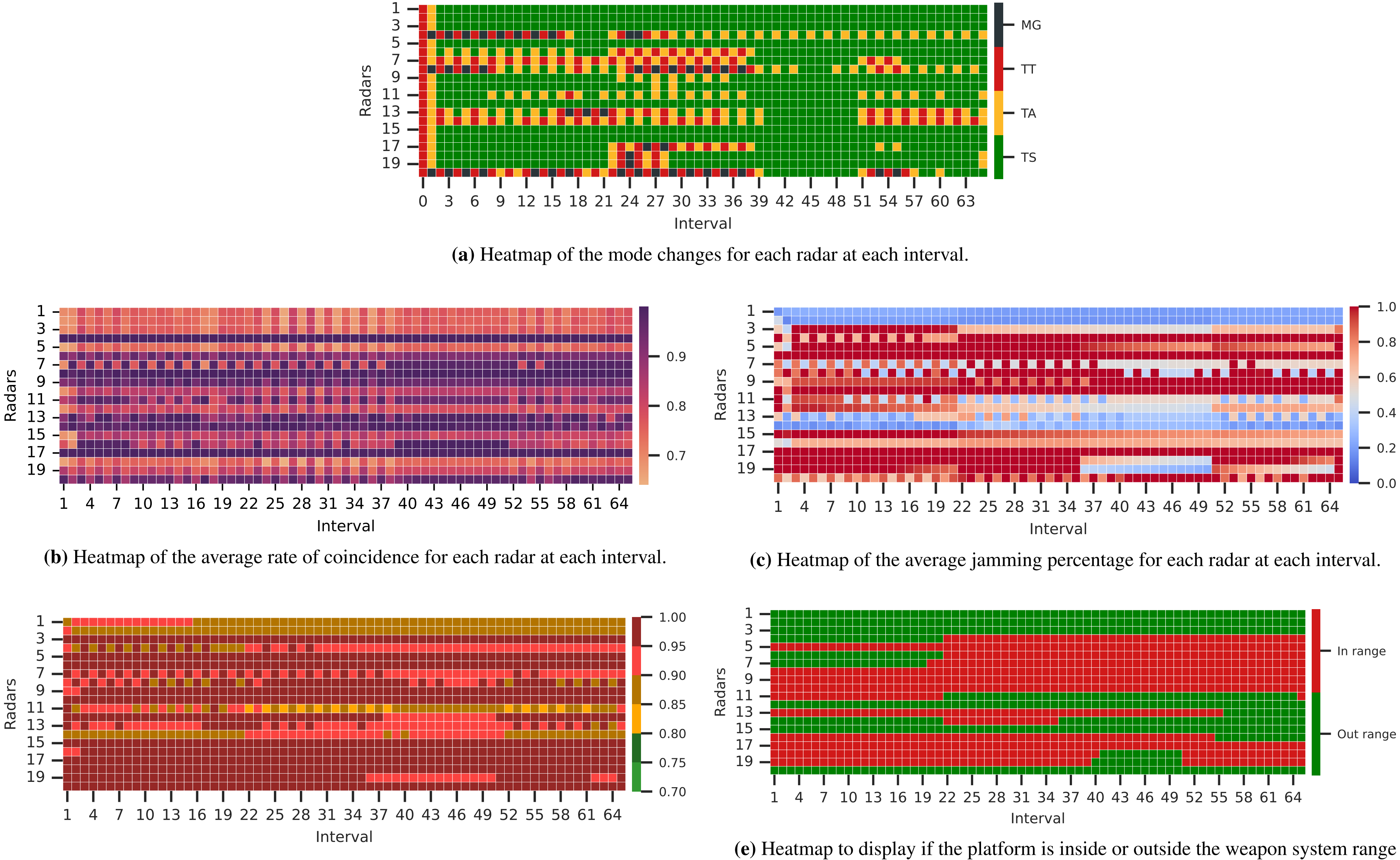
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.19. Overestimation of the probability of false alarm for all threats with mode assessment weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window with cut-off 5% after signal pulse falling edge



(a) Heatmap of the mode changes for each radar at each interval.

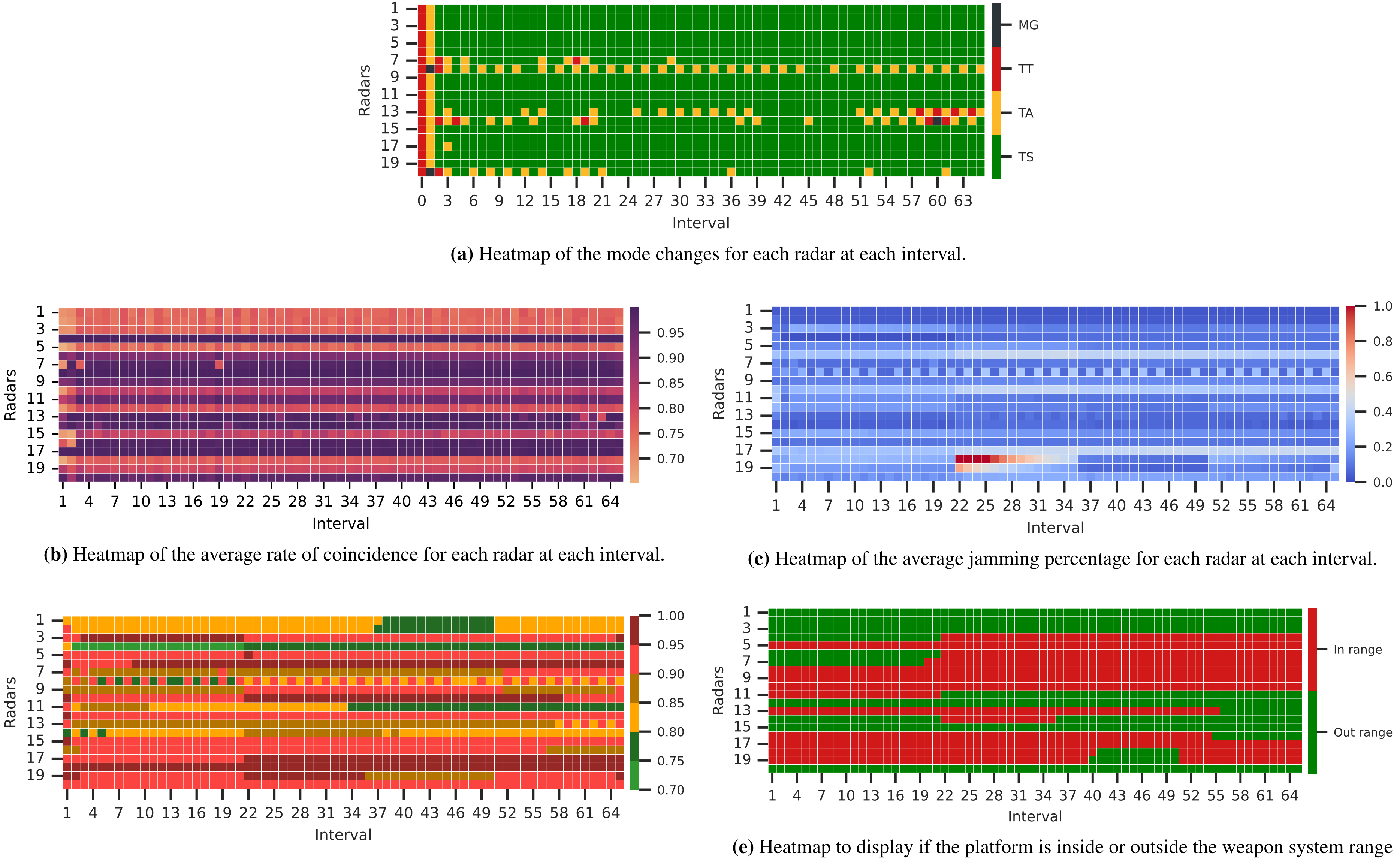
(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.20. Underestimation of the probability of false alarm for all threats with mode assessment weights set at $W_s = 0.15, W_r = 0.05, W_l = 0.1, W_j = 0.7$ and jamming window with cut-off 5% after signal pulse falling edge



(a) Heatmap of the mode changes for each radar at each interval.

(b) Heatmap of the average rate of coincidence for each radar at each interval.

(c) Heatmap of the average jamming percentage for each radar at each interval.

(d) Heatmap of the average zone assessment value for each radar at each interval.

(e) Heatmap to display if the platform is inside or outside the weapon system range at each interval.

Figure B.21. Configuring the TIJ with the best possible estimations and jamming window size.