Australian Government
Department of Defence
Science and Technology

An Evidential Network Approach Applied to Threat Evaluation in Above Water Warfare

Lloyd Hammond

Weapons and Combat Systems Division
Defence Science and Technology Group

DST Group-TR-3349

ABSTRACT

Threat prioritisation is a critical step in the detect-to-engage sequence during naval combat. As the warfighter's task requires the analysis of ever more complex scenarios, the ability to analyse all situational awareness information in a limited timeframe becomes more difficult, and the requirement for real-time tactical decision aids gains more prominence. The Evidential Network Technique is reviewed in this report with example analyses. In addition, a prototype threat evaluation model is presented for specific use in the above water warfare domain.

Published by

Weapons and Combat Systems Division
Defence Science and Technology Group
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: 1300 333 362

November 2017
AR-017-079

An Evidential Network Approach Applied to Threat Evaluation in Above Water Warfare

Executive Summary

Threat evaluation and prioritisation in the above water warfare (AWW) domain is a critical component of the Detect-to-Engage Sequence, and is typically undertaken by a Principle Warfare Officer or person(s) of equivalent training. In modern fire control systems, threat prioritisation can be performed in manual or automatic modes, or some combination thereof, at the discretion of warfare officers who oversee combat operations. Such decisions depend largely on the number and type of potential threats and the time available for tactical decision making. With potentially multiple targets and constantly updating situational awareness data from multiple sensors, the demands on combat system operators to prioritise threats in a timely manner can be severely tested. In such cases, the requirement for tactical decision aids gains more prominence.

A decision aid designed to facilitate prioritisation of threats would provide viable, rapid real-time response options for the warfighter to consider in parallel to his/her own threat prioritisation proposals.

This report is a review of the application of an Evidential Network, with the objective to develop a tactical decision aid for use in real-time AWW.

A MATLAB® algorithm produced by Benavoli et al. [1], which had only previously been utilised for threat evaluation in the air domain, was applied in this study to the AWW problem. However, the software requires further development to streamline its use, including the development of a Graphical User Interface (GUI).

The Evidential Network approach is more likely to provide realistic threat prioritisation results due to its capability for modelling uncertainty and ignorance in situational awareness. A notable downside is that this approach is significantly more mathematically complex.

The threat prioritisation study undertaken in this report goes hand-in-hand with a related previous study undertaken by the author in weapon target assignment [2]. The application of Evidential Network theory for Threat Evaluation, and further development of the related MATLAB algorithms, can be combined with the previous study, to automate the Threat Evaluation and Weapon Assignment process.
.

This page is intentionally blank.

Author

Lloyd Hammond
Weapons and Combat Systems Division

Lloyd Hammond was engaged in research in the area of Combat and Mission Systems for the Defence Science and Technology (DST) Group. Lloyd was based at the DST Group's site on Fleet Base West in Western Australia, where he undertook research into optimisation techniques for threat evaluation and weapon assignment in maritime combat scenarios. Lloyd also acted as a liaison for the Weapons and Combat Systems Division with the ANZAC Class Frigate Community located at Fleet Base West.

This page is intentionally blank.

Contents

1. Introduction

1.1 Threat Evaluation in Above Water Warfare

Threat evaluation is the process of identifying, classifying, and prioritising threat(s) according to the available situational awareness information. A naval weapons system provides threat evaluation before a weapon response plan is executed as part of the 'detect-to-engage' sequence. This report considers threat evaluation in the above water warfare (AWW) domain from the perspective of a single maritime asset. Given domain specific modifications, the approach discussed in this report could also be applied to the air, underwater and land domains.

In modern fire control systems, threat evaluation can be performed manually or automatically, at the discretion of the warfare officers who oversee combat operations. Such decisions depend largely on the nature and number of potential threats and the time available for tactical decision making. In comparing automatic and manual threat evaluation, a human in the loop may provide a safeguard against erroneous decisions; however, it may introduce unacceptable time delays.

Multiple sensor technologies rapidly feed various types of situational awareness data to combat system operators. Hence, the ability for operators to analyse and comprehend this data in real-time becomes a significant issue. The issue lends weight to the concept of making use of a decision support system. Such a system would facilitate the prioritisation of threats and provide viable, real-time response-options and threat prioritisation inferences for the warfighter to assess and consider. A threat evaluation decision support system must inevitably provide optimised decision options based on essentially the same information available to the warfare officer. The system must also be available in the command decision phase as highlighted in Figure 1-1. This report aims to describe algorithms which may underpin the development of a decision aid to support the threat prioritisation and engagement decisions.

1.2 Detect-to-Engage Sequence

A detect-to-engage sequence (DTES) is a critical set of events that occurs in warfare across all domains with a variety of military platforms and personnel, including submarines, surface ships, tanks and ground troops. A ship's weapons system's Fire Control System (FCS) performs a series of tasks as a part of a regular DTES [3]. These tasks begin with tracking operations to determine a threat's kinematics as part of the situation analysis, followed by identification, classification and end with a threat ranking:

1. Picture Compilation Task:
   - *typically undertaken by a Combat Systems Officer (CSO)*
   - *involves detection, tracking and classification of a contact*
     a. detect object (make contact)

   b. track object (accurately determine object's position and track)

   c. classify object (determine if air or surface track, and, if air, then classify as missile or aircraft)

   d. identify object as target or otherwise (e.g. identify friend or foe, etc.). Typically a manual decision.

2. Command Decision Task:
   - *typically undertaken by a Principal Warfare Officer (PWO)*
   - *produces a proposal and acceptance of action to defeat a threat*

   a. the object identification (see 1d above) straddles the picture compilation and command decision processes. Hence the PWO participates in this process.

   b. threat evaluation and prioritisation (if there are multiple targets)

   c. proposes action to neutralise a target (propose optimum assignment of weapon(s) to target)

   d. decide action (accept proposal / engagement decision).

3. Engagement Task:
   - *typically undertaken by a Fire Control Officer (FCO)*
   - *involves engagement of target and post-fire evaluation*

   a. engage target (employment of weapons)

   b. post Fire Evaluation (determine effectiveness of action)

The components of a DTES, as illustrated in Figure 1-1, will have varying emphases depending on the combat domain and the weapon systems platforms involved. Of particular importance in the context of this report is the 'Command Decision', where threat evaluation and prioritisation processes take place. This is also the step in the DTES where critical tactical decisions are decided by warfare officers through analysis of all available information. The subsequent step of the optimum assignment of weapons to targets has been covered in an earlier report by the author [2].

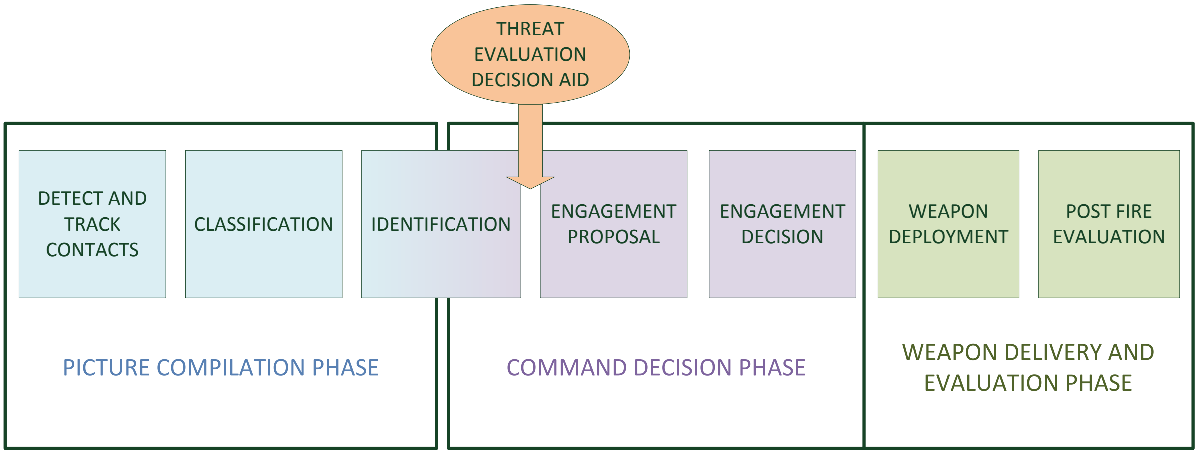


Figure 1-1 Detect-to-Engage Sequence (DTES) showing Threat Evaluation decision aid in Command Decision Phase.

The following section describes the approaches considered in this report for developing threat models, which would ultimately be incorporated within a tactical decision aid.

1.3 Developing a threat model for Anti-Air Warfare

In this section, different graphical network approaches that have previously been used for modelling AWW threat assessment in the maritime domain are reviewed. These models assume that in addition to other relevant information, one or more potential threats have been identified and that their track histories are available. The correct identification and subsequent prioritisation of track data is paramount, not only because there is a need to prioritise hostile threats, but also to avoid inadvertently targeting civilian or friendly aircraft, such as in the case of USS Vincennes [4] [5].

Combat systems commonly use algorithms based on military doctrine and in many cases rely on a set of ‘if-then’ rule-based decisions. However, a set of binary true/false, yes/no decision responses can lead to erroneous outcomes, particularly since real-world decision-making is based on sensor data that is inherently uncertain. It is therefore mathematically more appropriate to use algorithmic decision-making processes that incorporate the stochastic nature of inputs, rather than simplistic ‘if-then’ binary responses. As such, an Evidential Network technique is covered within this report.

This work is part of a DST Group task which considers the Threat Evaluation and Weapon Assignment (TEWA) problem in the case of a defended maritime asset with potentially multiple incoming threats. A previous report reviewed methodologies for the optimal assignment of weapons to targets for a naval asset in air warfare combat scenarios [2]. The problem of prioritising multiple incoming threats is a critical step prior to the allocation of weapons. In simple terms, it consists of ranking targets according to a number of factors, but predominantly, their hostile-behaviour and their ability to inflict damage to the defended asset.

The project's objective is the development of a tactical decision aid tool for threat evaluation, using algorithms to assess all input data to generate a prioritised threat list. Threat evaluation takes into account all available and relevant information for the known targets, including physical track information (position, altitude, course and speed), target intent and capability. Threat prioritisation is the ranking of threats according to their threat evaluations to assist warfighters with assigning and scheduling weapons.

1.4 Characterising Threats

In order to assess a threat, it is necessary to define exactly what the perceived threat is and what its characteristics are. By definition, a threat is something that represents a danger. In this report, the danger is not an absolute concept but is dependent on the defended asset's priorities. In other words, a threat may be accorded a higher priority to one defended asset as opposed to another depending on what its mission and defence capability are. Such subtleties become irrelevant if a fast approaching threat has the potential to destroy one's asset or assets. As Benavoli [6] states,

> Threat assessment estimates the degree of severity with which engagement events will occur and its significance in proportion to the perceived capability of the enemy to carry out its hostile intent.

There are a number of 'if-then' approaches that have been used to characterise and prioritise threats from the relatively simple "which threat is closest" or "which threat is likely to hit first" to a variety of stochastic methods employing heuristic algorithms. As with any decision-making technique, the more sophisticated the technique, the more computationally expensive it tends to become, with the underlying emphasis on the capability of real-time decision making being a critical factor.

Multiple threat targets are ubiquitous in modern combat situations. A weapon or a weapon-system/platform represented by a variety of weapons can be a target, and may possess different lethality, kinematics, trajectories, and ranges. Following track identification, it is critical for the warfighter to prioritise all targets by assessing all the available information and the subsequent target's response.

The severity and likelihood of a suspected threat is determined by its physical and behavioural attributes. Physical attributes such as capability and proximity are typically relatively straightforward to assess. They rely on the evaluation of a variety of sensor measurements, platform and weapon systems identification, physical proximity, speed, and environmental conditions. Behavioural attributes, such as a threat's hostile intent, are more difficult to determine, since they require evaluation of a threat's behaviour, including flight pattern, intent to use weapons, use of tracking devices, responses to interrogations, etc. In addition, threat assessment includes determining the geographical nature of the environment, if it is in a hostile air space or waterway, or if there is a heightened political situation or terrorist threat which may provide some clues as to a threat's intention.

1.5 Threat Input Data

Threat assessments are based on a range of input data, with some inputs carrying more significance and thus weighted more importantly than others. Input data sources include a range of organic (shipboard sensors, etc.) to inorganic information (typically background knowledge including political climate, hostile intent, ability to inflict damage, etc.).

As mentioned above, threat assessments are typically calculated based on the targets' proximity, capability and intent although the definitions of these parameters may vary:

1. Physical Proximity is a physical measure of the position of the threat in relation to the defended asset. This parameter is important to determine whether the threat is within range to release its weapons.
2. Capability is the ability of the target to inflict damage on the defended asset, despite the intent to inflict damage.
3. Intent is the aim of the target, i.e. whether or not it intends to inflict damage to the defended asset.

The capability and intent parameters differ in that capability is determined largely through sensor measurements. In contrast, determining a target's intent is largely subjective and depends on the target's behaviour, geography (e.g. is the asset in hostile territory?), as well as the overall political climate.

Opportunity has also been employed by some authors as a factor for assessing threats, either as a more general concept subsuming capability and intent [7] or as an additional parameter [8]. Opportunity largely depends on physical and environmental parameters conducive for a threat to proceed. The three classes of parameters most commonly used in threat evaluation are shown in Figure 1-2 with the respective input parameters for each of the three classes shown in Figure 1-3.

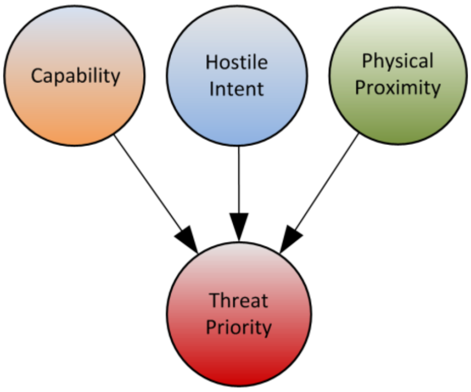
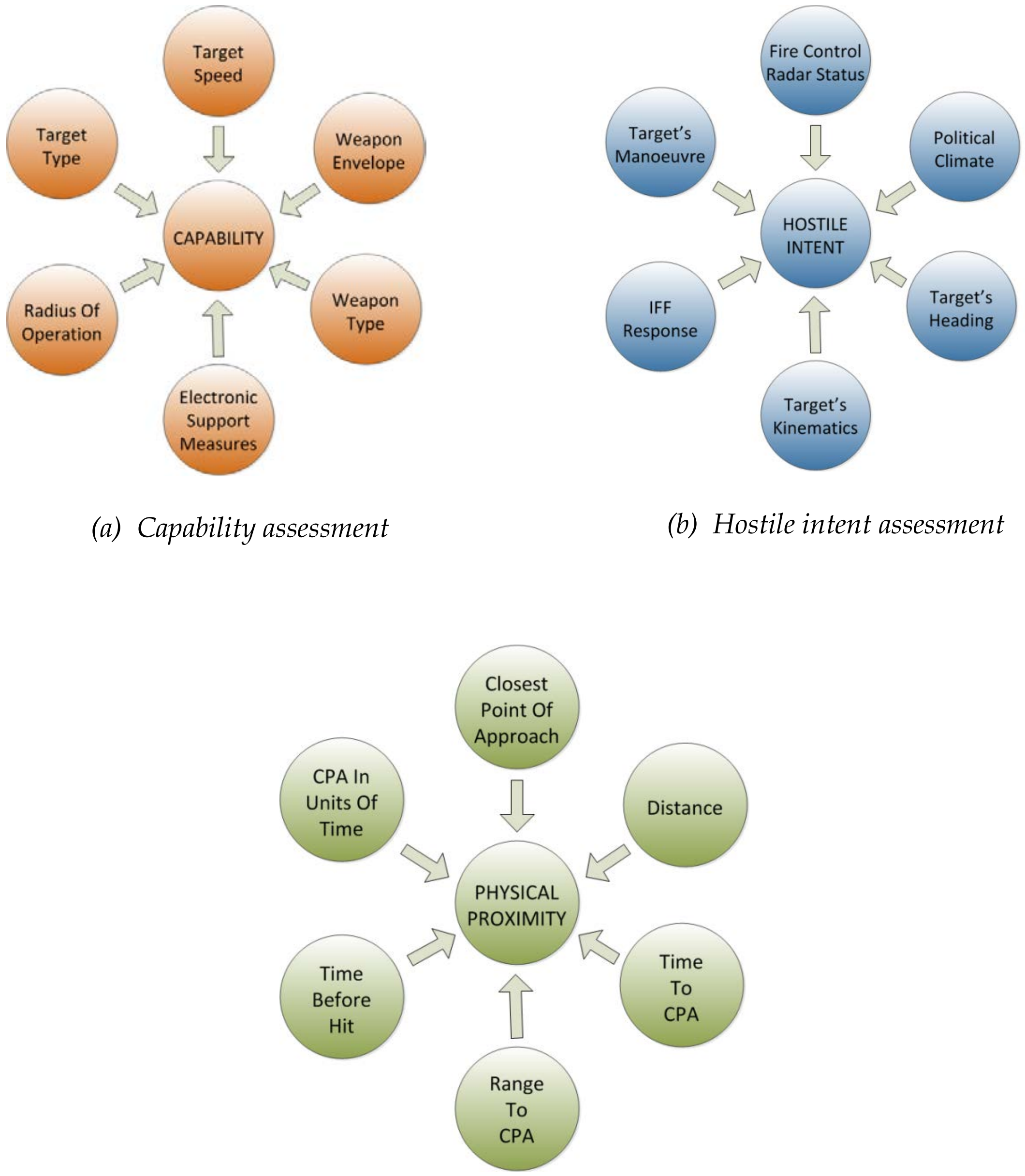


Figure 1-2 High level parameters frequently used in threat evaluation and prioritisation.



(a) Capability assessment

(b) Hostile intent assessment

(c) Physical proximity assessment

Figure 1-3 Parameters commonly used in threat evaluation for (a) Capability, (b) Hostile intent, and (c) Physical proximity determination. (CPA: Closest Point of Approach, IFF: Identify Friend or Foe).

1.6 Intent Parameters

The intent of a threat is its perceived objective, that is, its desire to inflict damage. Intent is the most difficult of the three classes (or types) of parameters to assess, since as mentioned, it can be largely subjective. However, there are means of assessing a threat's behaviour in conjunction with other pre-determined factors to evaluate threat intent. Intent parameters may include such considerations as:

- The overall political climate and consequent level of hostility.
- The status of the target's Fire Control Radar; i.e. if it is active.
- The target's response to an "Identify Friend or Foe" interrogation.
- The target's kinematics (i.e. motion related parameters including speed, direction, etc.)
- The target's heading (i.e. whether it is on a track to intercept or possibly attack the defended asset, whether it is on its known or intended flight path).
- The target's recent manoeuvres, i.e. if they conform to expectations.

1.7 Proximity Parameters

Proximity parameters provide an indicator of the threat's proximity to the defended asset [9] and its ability to launch weapons at the defended asset. Unlike intent parameters, proximity parameters are based on sensor measurements, typically taken on-board the defended asset and/or a nearby affiliated asset (e.g. an AEW&C[1], or other ships within a naval task group). Once the threat's position, speed and direction are determined, the threat's Closest Point of Approach (CPA) to the defended asset and related parameters can be estimated, assuming those parameters remain unchanged:

Closest Point of Approach (CPA)

The Closest Point of Approach (CPA) is the point where the target will be the closest that it can be to the defended asset, assuming that the velocities and directions of the defended asset and targets do not change. The CPA, as illustrated in Figure 1-4, is a spatial reference point.

[1] AEW&C: Airborne Early Warning and Control system typically used to perform command and control of the battlespace.

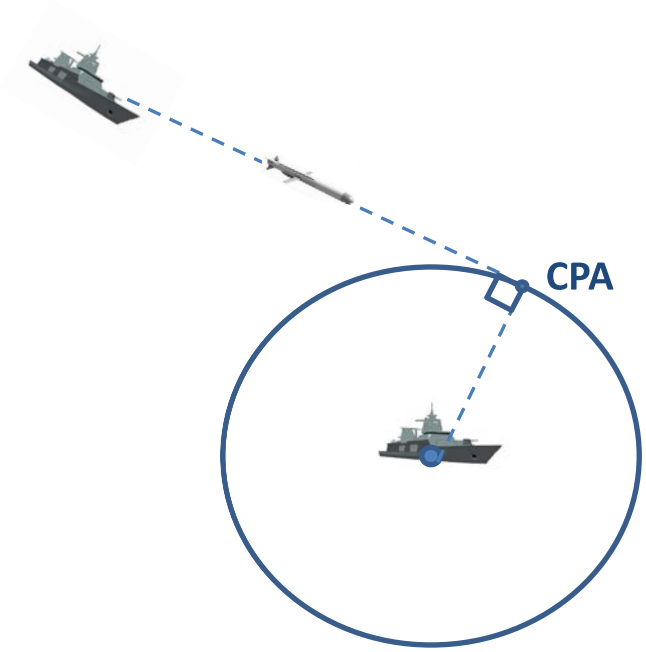


Figure 1-4 Schematic diagram showing CPA with respect to the target, weapon and the defended asset.

Time to CPA
Time to CPA (TCPA) is the time for the threat to reach the calculated CPA. If for example, there are two targets with similar destructive potency that both have the same CPA, the one with the quickest TCPA represents a greater threat.

CPA in units of time
In purely geometric terms, if a target was to head directly to the CPA and then take a hard 90 degree turn towards the defend asset, the time taken from the CPA to the defended asset is known as the CPA In Units Of Time (IUOT).

Time before hit
Time before hit (TBH) is the predicted total time taken for a target to hit the defended asset:

$$\text{TBH} = \text{TCPA} + \text{CPA IUOT}.$$

By way of example, an algorithm (written by the author in MATLAB) was used to calculate the four CPA related parameters discussed above. Figure 1-5 provides an output of the MATLAB program showing positional parameters for a target (at T0) in relation to a Defended Asset (DA at time=0, DA0). Actual numbers are listed in the table below. The algorithm can calculate CPA parameters for multiple targets and overlay them on the same diagram.

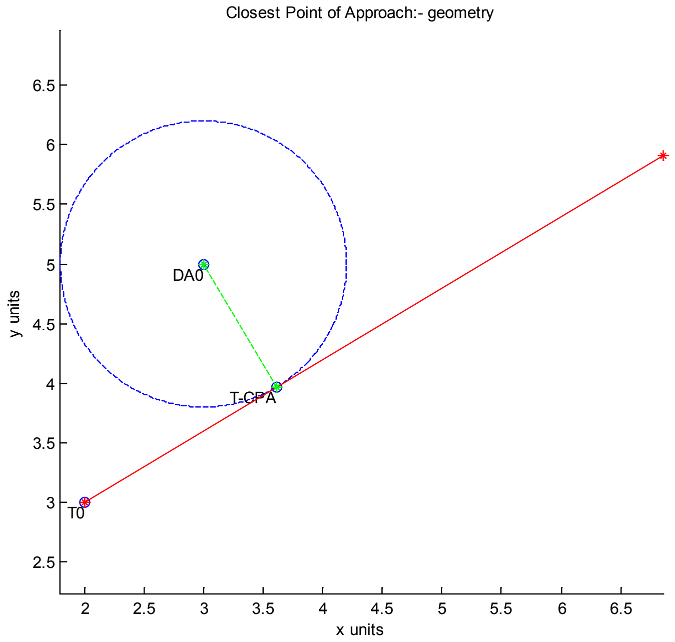


Figure 1-5 MATLAB plot of Target at t=0 (T0), CPA and Defended Asset (DA0).

Table 1-1 MATLAB Output for CPA parameters.

Target position (x, y)	Target Velocity (x, y)	Asset Position (x, y)	Asset Velocity (x, y)	TCPA	Target CPA	DA – CPA distance	CPA IUOT	TBH
(2.0, 3.0)	(5.0, 3.0)	(3.0, 5.0)	(0.0, 0.0)	0.32s	(3.6, 4.0)	1.20 units	0.21s	0.54s

1.8 Capability Parameters

As defined above, the intent of a threat pertains to its desire or will to inflict damage. Capability is the target's ability to inflict that damage. It relates to physical parameters, including the type of threat (e.g. missile type), whether the defended asset is within the target's weapon engagement range and its fuel capacity (as a reflection on its radius of operation). Many of these parameters can be deduced once the target type has been identified.

The determination of capability, in addition to intent and proximity parameters will be discussed further in the following sections in relation to the two approaches discussed in the report. It is worth noting that some of the physical measurement and organic parameters are common to these threat parameters. For example, the type of target is used to determine its physical capability as well as its proximity parameters.

2. Threat Modelling Options

In addition to Evidential Networks, a range of approaches have previously been applied to develop optimised threat prioritisation models, including Rules-Based Algorithms and Bayesian Network techniques.

Threat models frequently have a rules-based algorithm (RBA) at their core. An RBA is essentially a set of questions used to make decisions based on the available information. In effect, in the case of a threat model, this is a decision tree process where information about the target's proximity, capability and intent ultimately provide a quantitative threat level. However, an RBA doesn't readily contend with stochastic, or worse still, incomplete data. Since most threat information gathered from sensor outputs and intelligence analysis is of a stochastic nature, RBAs are unsatisfactory for anything other than simple 'if-then' deterministic assessments. Consequently, other techniques such as Bayesian Networks and Evidential Networks,[2] which are based on Bayesian probability theory and Dempster-Shafer theory respectively, are used to deal with stochastic information.

2.1 Logical Rule-Based Algorithms

Threat Evaluation models in their simplest form can be expressed as decision tree diagrams, as illustrated in the hypothetical example shown in Figure 2-1, where logical if-then statements (sometimes referred to as implication rules) with 'yes-no' or 'true-false' outcomes can be used to yield threat prioritisation decisions. Logical rules-based algorithms are deterministic, that is, it is assumed outcomes follow events with certainty. As in [10], using sensor measurements and/or other indicators, a set of rules can be developed into a decision tree. For example:

IF IFFS=N AND PLATFORMTYPE= NM THEN THREAT =2
IF FLIGHTPLAN= N AND EVASIVEMANVRE = N THEN THREAT=3

Such implication rules are deterministic with binary outcomes. That is, the query produces True/False, Yes/No, On/Off type results. As mentioned in the previous chapter, it is more likely that outcomes are stochastic in nature, that is, if A then *probably* B is more realistic than if A then B. Uncertainty in implication rules will be discussed further in Section 3.2.

The threat evaluation decision tree diagrams typically require a number of questions to be answered before a final threat assessment can be obtained. Each 'if-then' query leads to another 'if-then' or 'if-then-else' query as shown by the example in Figure 2-1 until a result is obtained. For example, If IFFS=N then QUERY PLATFORMTYPE. If PLATFORMTYPE=MILITARY then QUERY FCRSTATUS, etc.

[2] Although the techniques mentioned here have differences, they also share similarities. For example, Bayesian and Evidential Networks are both Valuation-Based Systems that used acyclic graphical methods.

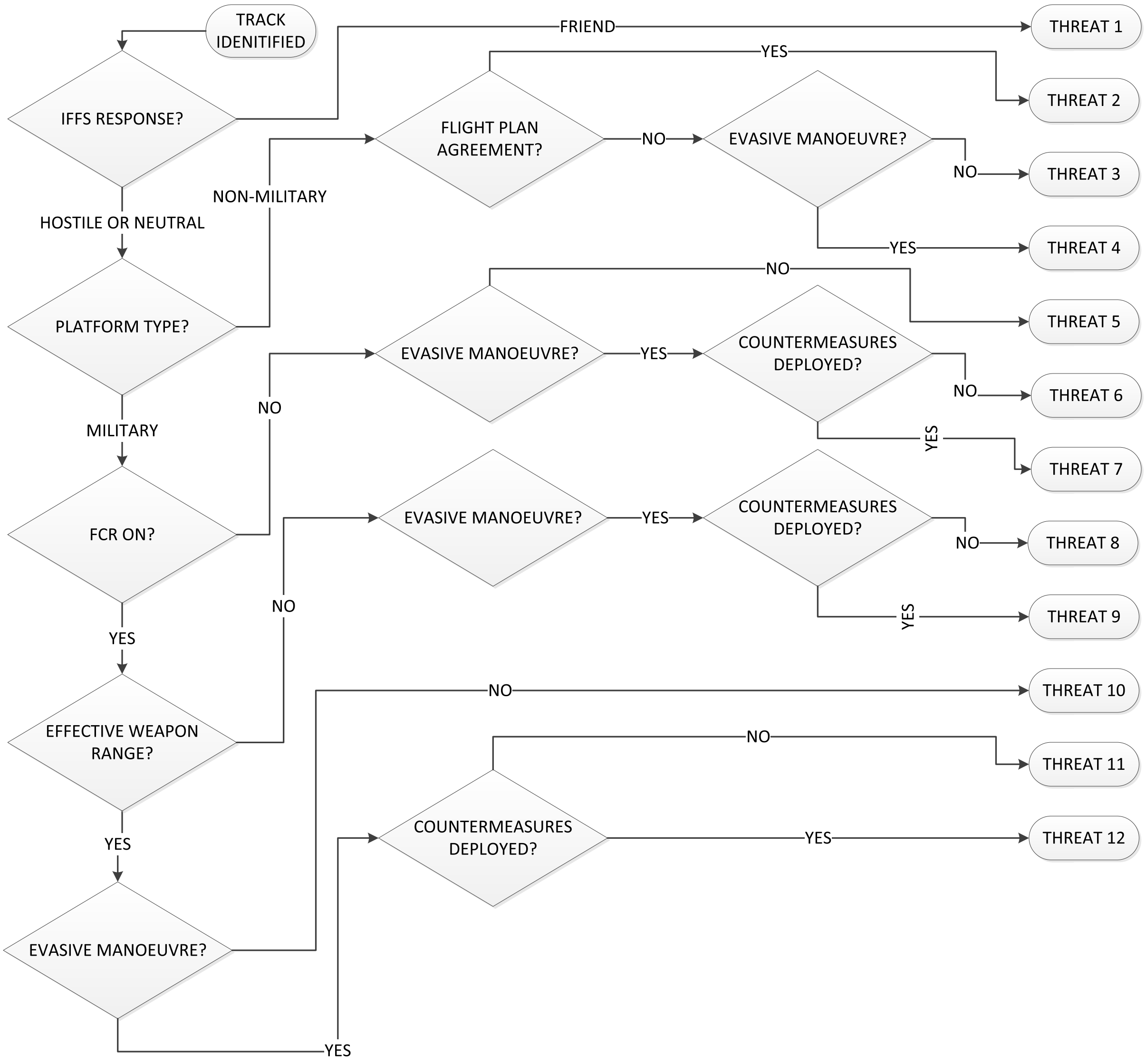


Figure 2-1 Example of a fictitious threat evaluation RBA decision tree with Threats 1 to 12 being the lowest to highest threat ratings, respectively.

2.2 Bayesian Networks

A Bayesian Network is one of a number of options used in the process of threat modelling. A Bayesian Network is a graphical representation of the joint probability distribution of a set of random variables, with their conditional dependencies represented by directed edges, and associated conditional probability tables. The nodes represent random variables and the edges form a directed acyclic graph (DAG), i.e. a directed graph without directed cycles. Whereas the implication rules for RBAs had deterministic outcomes, the implication rules for Bayesian Networks are necessarily stochastic by nature. Bayesian Networks assume that all required data, including domain knowledge and evidence, can be represented by probability functions. As discussed in the next section, this is not always possible.

Bayes' theorem is used as the calculus for updating probabilities based on new evidence. Bayes' Theorem may be derived from the formula for the joint probability of A and B where $p(A,B) = p(A|B)\,p(B)$ and $p(A|B)$ is known as the *posterior* probability, i.e. the probability that hypothesis 'A' holds after considering the effect of evidence 'B', and $p(B)$ is the probability of observing the evidence 'B'.

Given that

$$p(B,A) = p(B|A)\,p(A)$$

and:

$$p(A,B) = p(B,A),$$

it follows that

$$p(A|B)\,p(B) = p(B|A)\,p(A).$$

Assuming that $p(B) > 0$, this may be re-written as

$$p(A|B) = \frac{p(B|A)\,p(A)}{p(B)}$$

which is referred to as Bayes' Theorem. The term $p(B|A)$ is called the likelihood. It is the probability of the circumstantial evidence 'B' assuming the hypothesis 'A' is true. $p(A)$ is the *prior* probability of event 'A' occurring. Or a more literal translation is:

$$Posterior\ Prob.(of\ A\ given\ B) = \frac{Likelihood\ (of\ B\ given\ A) \times Prior\ Prob.(of\ A)}{Prob.of\ circumstantial\ evidence\ (B)}$$

To use Bayes Theorem, it is assumed that the prior probability exists and the circumstantial evidence exists (or can be learnt) [11]. In the case of three variables, A, B and C illustrated in Figure 2-2, Bayes' Theorem can naturally be extended using the chain rule to:

$$p(A,B,C) = p(C)\,p(B|C)\,p(A|B,C)$$

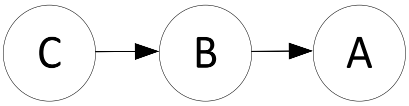


Figure 2-2 Example network used for the chain rule.

Given that B is conditionally dependent on C, then the above rule can be written in this case as:

$$p(A,B,C) = p(C)\,p(B|C)\,p(A|B)$$

The chain rule can be expressed more generally as:

$$p(x_1, x_2, \dots, x_n) = p(x_1)\, p(x_2|x_1)\, p(x_3|x_1, x_2) \dots, \times\, p(x_n|x_1, x_2, \dots, x_{n-1})$$
$$= \prod_i^n p(x_i|x_1, x_2, \dots, x_{i-1})$$

(where $p(x_i|\emptyset = \mathrm{p}(x_i)$).

The chain rule can be generalised to any Bayesian network. In particular, it can be shown that

$$p(x_1, x_2, \dots, x_n) = \prod_i^n p(x_i|pa(x_i))$$

where $pa(x_i)$ denotes the set of variables which correspond to the parent nodes of x_i in the Bayesian network (refer to e.g. [9], Eq. 4 or [11]). For example, consider Figure 2-2 where both B and A are dependent on C. In this case the chain rule above is directly applicable. The chain rule can be readily applied to any number of Bayesian Networks.

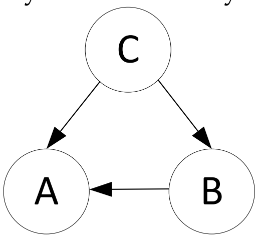


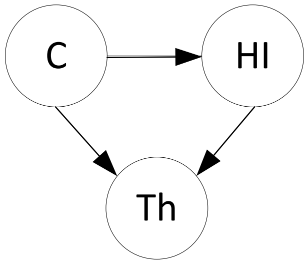
Figure 2-3 Example network used for second chain rule example.

Applying the chain rule to the network in Figure 2-3 yields:

$$p(A, B, C) = p(C)\, p(B|C) p(A|B, C)$$

As an example of using Bayesian Network for threat evaluation, Figure 2-4 shows the likelihood of a potential threat (Th) being modelled as conditionally dependent to its possible capability (C) and hostile intent (HI). Furthermore, the possible hostile intent and threat level are both dependent upon the target's capability. Probabilities associated with each variable are listed in the conditional probability tables (CPTs) adjacent to each node. The probability that the target is a threat given the a-priori probabilities is calculated below.

P(C = T)	P(C = F)
0.9	0.1



C	P(HI = T)	P(HI = F)
T	0.7	0.3
F	0.2	0.8

C	HI	P(Th = T)	P(Th = F)
T	T	1.0	0.0
F	T	0.2	0.8
T	F	0.1	0.9
F	F	0.0	1.0

Figure 2-4 Simple 3 node (C, HI, Th) Bayesian Network threat problem showing related nodal probabilities.

Abbreviating variables for clarity purposes, e.g. Th=T (true), Th=F (false) to Th, Th', respectively, and using the chain rule described above, it can be shown that

$$\begin{aligned} p(Th) = {} & p(C)p(HI|C)\,p(Th|HI,C) + p(C')p(HI|C')\,p(Th|HI,C') \\ & + p(C)p(HI'|C)\,p(Th|HI',C) + p(C')p(HI'|C')\,p(Th|HI',C') \end{aligned}$$

P(Th) = 0.90 x 0.70 x 1.0 + 0.10 x 0.20 x 0.20 + 0.90 x 0.30 x 0.10 + 0.10 x 0.80 x 0.0 = 0.661

$$\begin{aligned} \text{and } p(Th') = {} & p(C)p(HI|C)\,p(Th'|HI,C) + p(C')p(HI|C')\,p(Th'|HI,C') \\ & + p(C)p(HI'|C)\,p(Th'|HI',C) + p(C')p(HI'|C')\,p(Th'|HI',C') \end{aligned}$$

P(Th') = 0.90 x 0.70 x 0.0 + 0.10 x 0.20 x 0.80 + 0.90 x 0.30 x 0.90 + 0.10 x 0.80 x 1.0 = 0.339

In other words, the probability that the target being observed is a threat is 66.1% based on the capability and hostile intent information.

3. Evidential Networks

3.1 Introduction

There are a considerable amount of underlying concepts and theories behind Evidential Networks including belief function theory, basic belief assignments, valuation based systems, and Dempster-Shafer Theory. Such theories and concepts will not be expanded in detail since they are comprehensively covered by many authors, including Shenoy, Dempster, and Shafer amongst others. Dempster [12] introduced the theory of belief functions, which was later advanced by Shafer [13]. Valuation Based Systems were developed by Shenoy [14] as a means to compute uncertainty in expert systems[3]. These underlying concepts and Evidential Networks are introduced below with additional references.

3.2 Dempster-Shafer Theory

Dempster-Shafer Theory (DST) [19] (sometimes referred to as the DST of Evidence, or simply Evidence Theory), can be viewed as an extension form of probability theory for representing and combining evidence [20]. However, in DST, the counterparts of probabilities can be assigned to sets of events, rather than single events, with the latter being the case for Probability Theory. One significant aspect of DST is its ability to cope with varying levels of precision and uncertainty regarding sets of events [21].

Whereas probabilities between 0 and 1 are assigned to events in classical probability theory, weighted masses are employed in DST. The masses are not probabilities, but weightings given to an event or subset of events. DST is better suited to representing knowledge in real-world systems, since it allows for a level of ignorance or uncertainty regarding the knowledge of states [1]. The trade-off is that DST tends to be more mathematically complex than Bayesian Networks.

As mentioned above, DST comes to the fore when dealing with uncertainty in evidence and is particularly useful in the propagation of information through an Evidential Network. Dempster [13] developed a methodology for combining beliefs derived from independent pieces of evidence, whereas Shafer [14] was able to determine degrees of belief for decisions calculated from subjective probabilities from a related decision or question.

In a similar manner to Bayesian Network Theory, DST can have a degree of belief in an event ranging from 0 to 1, as shown in Figure 3-1.

[3] "In artificial intelligence, an expert system is a computer system that emulates the decision-making ability of a human expert. Expert systems are designed to solve complex problems by reasoning about knowledge, represented primarily as if-then rules rather than through conventional procedural code." [29]

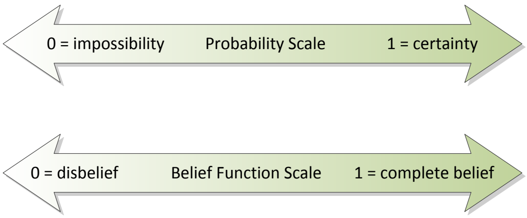


Figure 3-1 Comparison of probability and belief function scales, respectively.

However, the belief in an event and the corresponding disbelief in DST need not necessarily sum to unity. Furthermore, where there is no evidence for belief or disbelief, then both values could be zero, representing a lack of any type of evidence. In this way, DST incorporates 'ignorance' into a model, as shown visually using the barycentric triangle[4] in Figure 3-2. In this case the three vertices are represented by belief, disbelief and ignorance, respectively.

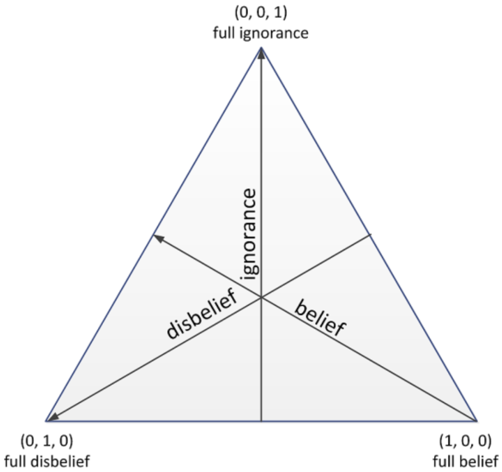


Figure 3-2 Barycentric triangle – a convenient way to express confidence in evidence.

DST is well explained in numerous references [1] [21] [22]. The fundamental parameter in DST is referred to as the basic belief assignment (BBA), otherwise known as the mass function, m(A). A BBA represents a belief about the possible value of a variable. Mathematically, m(A) is the proportion of all relevant evidence that supports the belief in element A, where A is the member of the power set. The power set, or 'frame of discernment' (denoted $\Theta = 2^{\Omega}$) is the set of all possible subsets of the set of all possible conclusions. For example, if $A = \{x_1, x_2, x_3\}$ then belief in A is given by:

$$Bel(A) = m(x_1, x_2, x_3) + m(x_1, x_2) + m(x_2, x_3) + m(x_1, x_3) + m(x_1) + m(x_2) + m(x_3)$$

[4] A barycentric coordinate system is one in which the location of a point of a triangle is denoted as the centre of mass (barycentre) of three quantities placed at each of the vertices. These quantities are usually of unequal mass.

Any of these mass subset values could be zero, which indicates ignorance rather than a lack of belief, in the element A.

3.2.1 Uncertainty in Implication Rules

The implication rules used in Evidential Networks are reasonably complicated and differ from those used in conventional Bayesian Networks. The background theory is well covered by others [1] [23] [24] [25] so the following is essentially an overview of some basic theory supported by examples which will be used in subsequent chapters in this report.

Conditional probabilities are typically defined as 'if-then' statements. For example, if the sky is cloudy, then it will rain; in simple terms, if A then B. However, it is more realistic to say, if it is cloudy, then there is a 95% chance it will rain, or if A then *probably* B. Furthermore, our uncertainty could be described over a range of values, such as, if it is cloudy, then there is a 70 to 90% chance it will rain.

To explore the uncertainty implication rules and notation further, we begin by assuming that we wish to determine the true value of 'x'. The frame of discernment, $\Theta = \{x_1, x_2, \ldots, x_n\}$ defines a finite set of all possible values of 'x'. In other words, the frame defines the set of all values for which we believe our variable 'x' could belong to.

If $A \subseteq \Theta$, then m(A) is the part of the belief that supports A, that is, that the true value of 'x' is within A. Put in another way, we know that the true value of 'x' resides somewhere within A, but we don't know which subset of A this might be, at least not without further information. So a function is referred to as a basic belief assignment (BBA) if it meets the following two criteria [6].

1. $m(\emptyset) = 0$ (i.e. no belief is committed to Ø)
2. $\sum_{A \subseteq \Theta} m(A) = 1$ (i.e. the total belief has a measure of unity)

Implied Belief can be written as: if A ⇒ B (If A then B).

For example, there is a belief that if the target's fire control radar (FCR) is detected as being active (i.e. turned on), then the target will release a weapon.

So in this example:	$A = FCR$ (active).	$A' = \overline{FCR}$, (inactive).
	B = W (weapon released).	$B' = \overline{W}$ (no weapon released).

Implied belief with uncertainty can be written as: if A ⇒ B with confidence α (If A then *probably* B):

For example, there is a belief with at least 90% confidence that if the target's FCR is active, it will release a weapon.

As stated, an uncertain implication rule is an expression of the form, if A ⇒ B with confidence α, which can be expressed mathematically as [6]:

$$m_3^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ 1 - \alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

So belief with 90% (α = 0.90) confidence that if the target's fire control radar (FCR) is active, a weapon will be released (W).

The variable set is Φ = {FCR, W}

The corresponding frames of discernment for the two variables, FCR (status of fire control radar) and W (status of weapon launch), are:

$\Theta_{\mathrm{FCR}} = \{\mathrm{FCR}, \overline{\mathrm{FCR}}\}$ with domain: $D_{FCR} = \{on, off\}$

$\Theta_{\mathrm{W}} = \{\mathrm{W}, \overline{\mathrm{W}}\}$ with domain: $D_W = \{true, false\}$

if FCR ⇒ W with a confidence of at least 0.90 (i.e. α):

$$m_3^{D_{FCR} \cup D_W}(C) = \begin{cases} 0.90 & C = (FCR \times W) \cup \left(\overline{FCR} \times \Theta_{D_W}\right) \\ 0.10 & C = \Theta_{D_{FCR} \cup D_W} \end{cases}$$

That is, if the warfighter believes that if he detects a target's FCR is active, then the target has launched a weapon against his vessel with a confidence of 90%. The remaining 10% accounts for the warfighter's lack of knowledge, that is, this 10% belief is assigned across both variable domains.

Instead of specifying confidence above (or below) a level, it is also possible to specify a range of confidence. If A and B belong to two disjoint domains, D_1 and D_2, where D_1 and D_2 have frames of discernment, Θ_{D1} and Θ_{D2}, respectively, then the occurrence of event A indicates that event B is likely to occur with a confidence level between α and β. This theory is well covered by [1] [6].

For example, the warfighter may believe with a confidence of between 70 to 90% that if the target's FCR is active, then a weapon will be launched. Expressed in mathematical terms, if A ⇒ B, with a confidence between α and β:

$$m_3^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ 1 - \beta & C = (A \times \bar{B}) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ \beta - \alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

For this example:

$$m_3^{D_{FCR} \cup D_W}(C) = \begin{cases} 0.70 & C = (FCR \times W) \cup \left(\overline{FCR} \times \Theta_{D_W}\right) \\ 0.10 & C = (FCR \times \bar{W}) \cup \left(\overline{FCR} \times \Theta_{D_W}\right) \\ 0.20 & C = \Theta_{D_{FCR} \cup D_W} \end{cases}$$

That is, if the warfighter believes that if he detects a target's FCR is active, then the target has launched a weapon against his vessel with a confidence of more than 70% and less than 90%. The warfighter's belief indicates that there is a 10% chance that a weapon will not be launched if the FCR is active. The 20% confidence interval accounts for the warfighter's uncertainty or lack of detail about where the actual true value lies within the 70 to 90% range of possibilities across both variable domains. The uncertainty rules discussed above will be used later in this report to develop Evidential Networks.

3.3 Valuation Based Systems

A Valuation-Based System (VBS) [15], [16], [17] is a representation of a set of random variables that represent physical parameters and their relationships in a real-world system or domain. Similarly to Bayesian Networks, random variables are captured by nodes and their relationships by links/edges.

VBSs differ from Bayesian Networks in a number of ways:

- Valuations need not be probabilities. Valuations are associated with each link, which represent our *a priori* information and domain knowledge.
- Message passing schemes are used to propagate Basic Belief Assignment (BBA) information (evidence and uncertainty) through the network
- Mathematical operators can be used to simplify the network information (combination and marginalisation)
- The fusion algorithm is used to marginalise / focus knowledge within the VBS to a smaller (and therefore coarser) domain, by successively deleting variables and is especially effective for static frameworks.
- BBA's manage lack of information / ignorance whereas Bayesian Networks cannot distinguish between the cases where the probabilities are all equal, and when where there is total ignorance.

If the valuations in a VBS are given in the form of BBA's then this type of VBS is referred to as an Evidential Network which is the only type of VBS considered here. The following sections discuss the attributes and the analysis methods applied to Evidential Networks.

3.4 Belief Functions, Combination and Marginalisation

In a Bayesian Network, the arcs (links) between nodes (variables) represent the conditional probabilistic relationship between two nodes. In an Evidential Network, the links between nodes represent joint valuations on the product space of the nodes. A joint valuation [18] is the combination of all valuations in the entire Evidential Network although joint valuations can be determined for two or more nodes (i.e. up to the entire Evidential Network).

Computing the joint valuation for an entire network becomes increasingly computationally expensive as the size of the network grows. An alternative approach is to perform 'local computations' on sections of the network through a process of combination and marginalisation.

Combination is a process which combines or aggregates knowledge, whereas marginalisation is an operation which marginalises a variable, thereby coarsening the information to a smaller domain. Marginalisation and combination are irreversible operations.

3.4.1 Combination

Combination is a process that aggregates knowledge relating to a particular event. The data may come from repetitive measurements, from a single source, or from multiple sources. The combination of two BBA's can be performed using Dempster's Rule of Combination:

If m_1 and m_2 are mass functions, their combination is denoted by $m_1 \otimes m_2$ and is defined as followed:

For an empty set ∅

$$(m_1 \otimes m_2)(\emptyset) = 0$$

For a non-empty set A

$$(m_1 \otimes m_2)(A) = c \sum_{B \cap C = A} m_1(B)\, m_2(C)$$

where c is the normalising constant (i.e. sometimes $m_1(B)m_2(C) > 0$).

$$c = 1 - \sum_{B,C: B \cap C = \emptyset} m_1(B)\, m_2(C)$$

3.4.2 Marginalisation

Marginalisation is a process that coarsens knowledge, eliminating variables that aren't specifically required in the current analysis, resulting in a smaller (i.e. coarser) domain. More specifically, marginalisation is the projection of a BBA (defined on a domain D) to a BBA defined on a coarser domain, D' (D'⊆ D). It is only possible to marginalise to a coarser domain once the variables to be eliminated have been expressed in the same domain.

3.5 Joint Valuations

As mentioned in Section 3.4, in order to evaluate an Evidential Network, it is necessary to determine the joint valuation of the associated network where joint valuations can be determined for two or more nodes, up to the entire Evidential Network. The most appropriate method for evaluating a network depends on whether it is a static or dynamic network.

3.5.1 Fusion Process for Static Networks

The fusion algorithm permits calculation of the marginal of the joint valuation of a network without computing the entire network's joint valuation, which is far more computationally efficient.

The fusion process involves the stepwise marginalisation of variables given in an elimination sequence, the sequence potentially having a significant effect on the overall computation speed. By recursively performing the fusion process, all required variables can be marginalised, leaving the variable of interest (e.g. threat level) remaining. Once marginalised, a network cannot be reversed to its prior state. Hence the fusion process is only suitable if the network's BBA's are static (i.e. invariant over time).

If the BBA's do vary with time, then the fusion process is no longer appropriate, since the full joint valuation would need to be undertaken whenever a single valuation is altered. In the cases where BBA's do vary with time, it is more efficient to undertake local computations using a binary join tree (BJT).

3.5.2 Binary Join Trees for Dynamic Networks

Dynamic networks are the same as static networks except that at least one of the BBA values is updated. Any update of the BBA values requires computation of the joint valuation of the network. It is possible to compute the 'joint valuation' of an entire Evidential Network using the fusion process, although such a 'brute force' approach can be computationally expensive and consequently inefficient, particularly in the case of real-time threat prioritisation problems. There are ways around this problem, including using a BJT.

A join tree is a graphical network representation that facilitates the use of the fusion algorithm for network evaluation. A BJT is a join tree where each node has at most, three neighbours, that is, one parent and two children. It is called 'binary' since its construction process is based on utilising the fusion algorithm in a manner that all combinations between BBA's should be performed on a binary, i.e. two-by-two, basis.
We can recompute the marginal of an Evidential Network more efficiently if the network is represented in the form of a BJT. An example Bayesian Network is presented in Figure 3-3 with its BJT representation in Figure 3-4, calculated using Benavoli's MATLAB Evidential Network software.

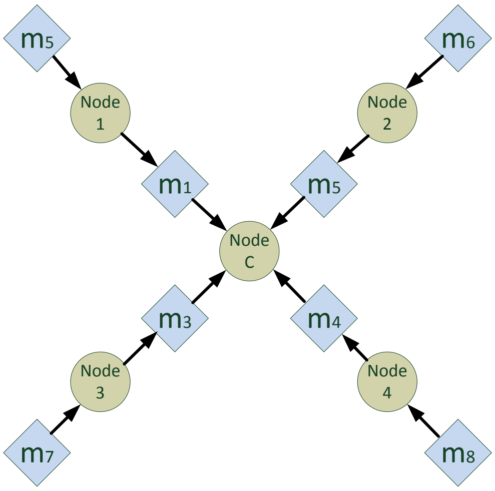


Figure 3-3 An example Evidential Network containing 5 nodes, which include a central parent node and 4 adjacent leaf nodes. BBA's are shown in blue diamonds. This related BJT is shown in Figure 3-4.

It is more likely that variables will be expressed on disjoint domains so that before Dempster's Rule of Combination can be applied, it is necessary to first extend both BBA's to the joint domain. This is so that their information is represented on the same domain without essentially altering the information.

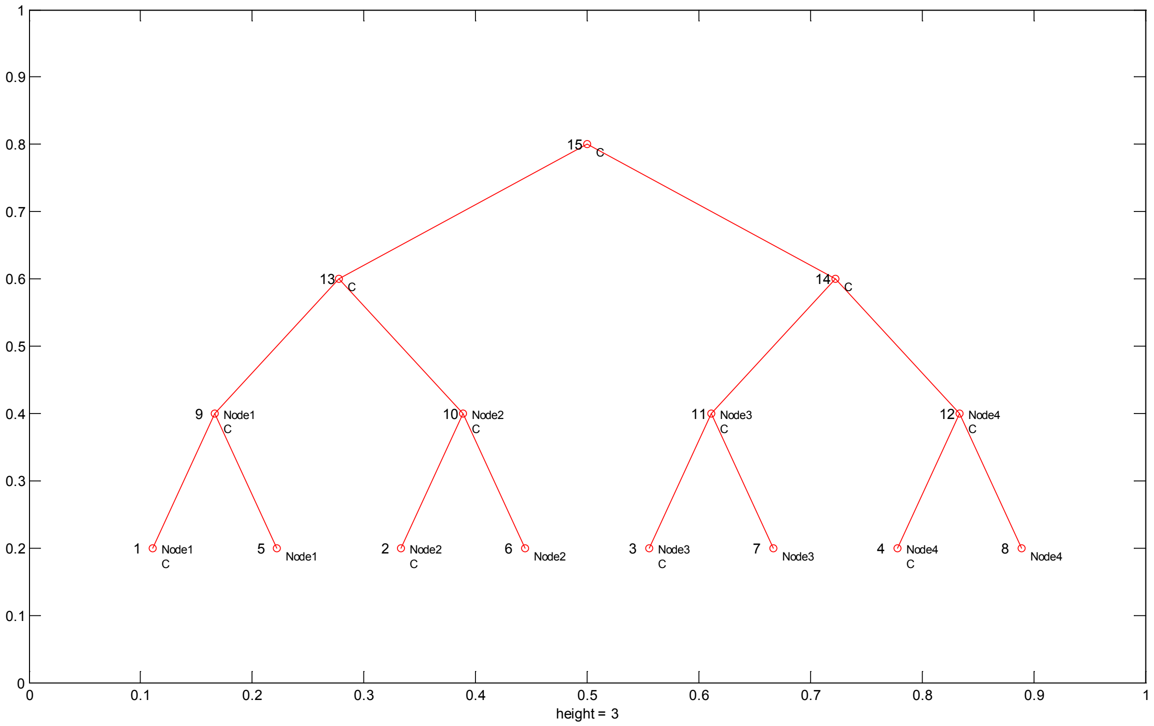


Figure 3-4 The BJT derived using Benavoli's Evidential Network MATLAB algorithm.

3.6 Pignistic Transformations

Since belief functions aren't probabilities, they are impractical for decision making purposes. Hence belief measurements require mapping to an equivalent probability measure. A common means of doing this is by using a pignistic transformation. If m^D is a BBA on the subset of variables, D (having frame of discernment, Θ_D), then the pignistic transform of m^D is defined as [26]:

$$BetP = \sum_{\theta \epsilon A \subseteq \Theta_D} \frac{1}{|A|} \frac{m^D(A)}{\left(1 - m^D(\emptyset)\right)}$$

where *BetP* is called the pignistic probability function and is a measure of probability that can be used for decision making purposes [1]. The transformation between the belief function and the pignistic probability function is referred to as the pignistic transformation [27].

4. Threat Evaluation Using Evidential Networks

4.1 Introduction

This section describes a solution to the threat evaluation problem which is based on Evidential Networks. The solution is referenced in Benavoli et. al. [1] [6][23]. However, this report presents more detailed workings compared to the original publication. The individual steps required in the Evidential Network solution are detailed in the sub-sections below.

4.1.1 Assemble List of Relevant Parameters

The first step is to identify and define all the relevant parameters and associated frames (i.e. the set of all possible values for each parameter) to be used in the Evidential Network. Table 4-1 lists these parameters with their associated frames as well as their minimum and maximum values.

Table 4-1 Evidential Network parameters, their associated symbols and frame descriptions.

Parameter	**Symbol**	**Frame**	**Frame Min**	**Frame Max**
Threat	T	{0, 1, …, 10}	lowest threat	highest threat
Hostile Intent	HI	{0, 1, …, 6}	benign	maximum hostility
Capability	C	{0, 1, …, 4}	no capability	highest capability
Evasive Manoeuvre	EM	{0, 1}	False	True
Fire Control Radar *(i.e. intention to fire a weapon)*	FCR	{0, 1}	OFF	ON
Counter-measures *(e.g. deception, jamming, chaff)*	CM	{0, 1}	False	True
Political Climate	PC	{0, 1}	Peace	War
Not a Friend	NF	{0, 1}	False	True
Identify Friend or Foe	IFF	{0, 1}	False	True
Flight Plan Agreement	FPA	{0, 1}	False	True
Platform Type	PT	{0, 1, …, 5}	0: merchant ship 1:patrol boat 2:frigate 3: destroyer 4:a/c carrier 5:RHIB	
Weapon Engagement Range	WER	{0, 1, 2}	0: short 1: medium 2:long	
Imminence (of attack)	I	{0, 1, 2}	0: low 1: medium 2:high	

4.1.2 Construct Evidential Network

The Evidential Network presented in Figure 4-1 shows nodes and belief masses in circles and diamonds, respectively. The orange (m_1 to m_7) and green diamonds (m_8 to m_{15}) are associated with intermediate and leaf nodes, respectively. The valuations for the leaf nodes are determined by available real-time input data whereas the valuations for the intermediate nodes are typically set according to *a priori* relationship information about these node variables.

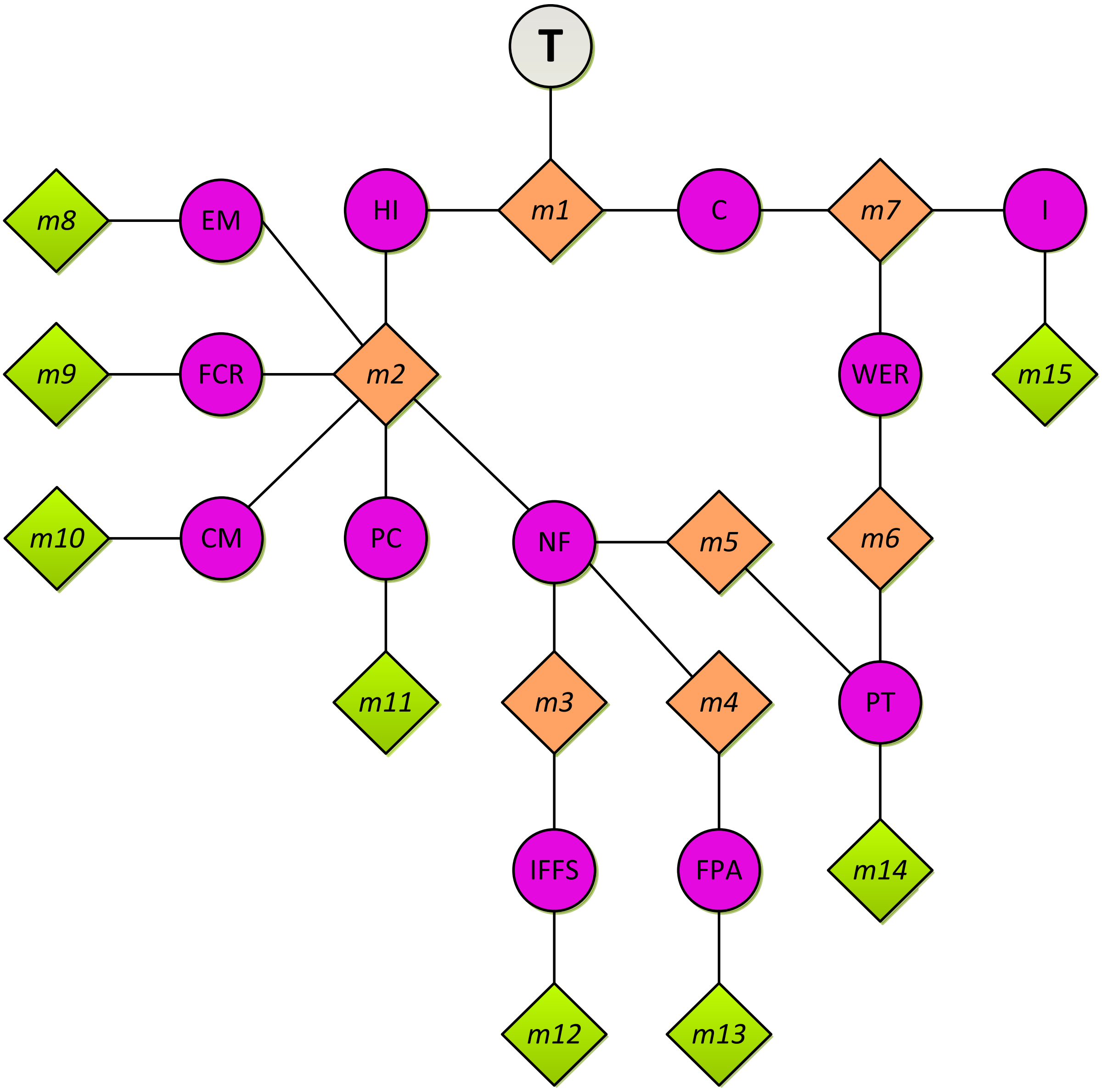


Figure 4-1 An Evidential Network showing variable nodes in purple circles, BBA's in diamonds, with leaf and intermediate BBA's shown in green and orange, respectively.

The Evidential Network shown in Figure 4-1 can be described as a:

5 tuple, Valuation Based System: {D, Θ_D, Φ_D, ⊕, ↓} with:

- Domain of Interest: $D^0 = \{T\}$ (i.e. the set of variables of interest for decision making).
- Θ_D: Set of frames of all variables of set D.
- Φ_D: Set of all valuations for the set of variables, D.
- ⊕: combination (mathematical operator)
- ↓: marginalisation (mathematical operator)
- Domain: D = {T, HI, C, EM, FCR, CM, PC, NF, IFFS, FPA, PT, WER, I}
- Power set: Set of all subsets of Φ_D

4.1.3 Calculate Basic Belief Assignments

The variables are represented by the nodes and BBA's depicted in Figure 4-1 (i.e. for the threat model Evidential Network). There are seven BBA's which are calculated according to their pre-defined rules. Some BBA's, such as m_1, have simple linear rules, whereas other BBA's have uncertain 'if-then' implication rules with degrees of confidence (e.g. m_3). The seven BBA's (m_1 to m_7) represent the generic knowledge of the Evidential Network, whereas the remaining eight BBA's (m_8 to m_{15}) represent the available evidence, or factual knowledge, about the Evidential Network. In the case of a threat model, m_1 to m_7 represent existing relationships between variables, such as between threat, hostile intent and capability, whereas m_8 to m_{15} represent organic information, such as available sensor data from radar, etc. and are more likely to be subject to change.

The rules for BBA's m_1 to m_7, which are outlined below, are the identical rules used in the original reference [1] . The detailed workings for these BBA's, not previously presented by the original authors, are listed in Appendix A.

BBA for m_1:
The Threat Level variable, T, is dependent on the Hostile Intent variable, HI, and the Threat Capability variable, C, according to the rule:

$$T = HI + C$$

Consequently, the BBA m_1 is defined according to this rule on the product space, *T x HI x C*. m_1 is described fully (along with the following BBA's) in Appendix A.

BBA for m_2:
The Hostile Intent variable, HI, is dependent on evidence that the target is behaving in a hostile manner. Such behaviour related parameters may include: evasive manoeuvres (EM); countermeasures (CM), fire-control radar (FCR) status, the broader political climate (PC)

and identification as whether or not the target is non-friendly (NF). HI has a relationship with {EM, FCR, CM, PC, NF} according to the rule:

HI = EM + 2.FCR + CM + PC + NF

The BBA m_2 is defined according to this rule on the product space, *HI x EM x FCR x CM x PC x NF.*

BBA for m_3:
The third BBA is based on the Identify Friend or Foe Squawking (IFFS) response and Non-Friendly (NF) variables and exists on the {IFFS, NF} domain. A different methodology is used here compared to the preceding BBA's since these rules are not deterministic; i.e. there is uncertainty in the implication rules. Here our *a priori* knowledge is that:

Rule 1: *We are 95 to 100% confident that if the IFF squawking response is true (i.e. IFFS=1), then the target is actually a friend. That is if IFFS=1 then NF=0 with at least 95% confidence.*

Rule 2: *Conversely, if there is no response to the IFF squawking (i.e. IFFS = 0) interrogation then we are only 10 to 30% confident that the target is non-friendly.*

The BBA m_3 is defined according to these rules on the product space, *IFFS x NF.*

BBA for m_4:
The fourth BBA is based on the Flight Plan Agreement (FPA) and Non-Friendly (NF) variables, respectively and exists on the {FPA, NF} domain. Our *a priori* knowledge is that:

> ***Rule 1:*** *We are 95 to 100% confident that if the target is flying in accordance with their flight plan, FPA = 1, then the target is friendly, NF=0.*
>
> ***Rule 2:*** *Conversely, if the target is not flying in accordance with its flight plan, FPA=0 then we are 10 to 30% confident that the target is non-friendly, NF=1.*

The BBA m_4 is defined on the product space, *FPA x NF.*

BBA m_5:
The fifth BBA relates the Platform Type (PT) variable to the target non-friendly (NF) variable. Based on *a priori* knowledge,

> *If the target is non-friendly (NF=1) then the target can be one of three platform types:*
> $PT \in \{3,4,5\}$ *with confidence between 50 and 100%.*

The BBA m_5 is defined on the product space, *PT x NF.*

BBA m_6:

The sixth BBA relates the Platform Type (PT) variable to the Weapon Engagement Range (WER) variable on the domain {PT, WER}. That is we have *a priori* information that permits us to estimate the WER based on the platform type identified, using the following rules:

Rule 1: We are 40 to 100% confident that if the target is either platform type 0 or 1, it has no WER (i.e. WER = 0).

Rule 2: We are 40 to 100% confident that if the target is either platform type 2 or 3, it has a WER of either 1 or 2.

Rule 3: We are 40 to 100% confident that if the target is either platform type 4 or 5, it has a WER of either 2 or 3.

The BBA m_6 is defined on the product space, *PT x WER.*

BBA m_7:

The seventh BBA relates the threat Capability (C) variable to the WER and Imminence of Attack (I) variables. BBA m_7 is defined by the following rule:

$$\mathrm{C} = \mathrm{WER} + \mathrm{I}$$

The BBA m_7 is defined on the product space, $C \times WER \times I$.

This is a simple rule that indicates if the WER of the target is large and the imminence of attack (I) is high, then the threat capability of the target is also high.

As mentioned above, the calculations for the BBA valuations for this Evidential Network are shown in Appendix A.

4.2 Part B: BJT Problem Solution

The formation of the Evidential Network and its associated BBA's is described above for this threat problem. The following five steps are used to solve this problem:

- Construct a Binary Join Tree (BJT), which is an efficient graphical representation of the Evidential Network, using a heuristic that will be used to eliminate variables until domain of interest is achieved.
- Initialise leaf BBA's (i.e. m_8 to m_{15}) of the BJT.
- Apply the inward propagation algorithm (IPA) using local computation methods including combination and marginalisation
- Marginalise the final belief of the root of the BJT to D^0.
- Apply pignistic transformation to put belief values into more practical probability values.

These five steps are covered in more detail below.

4.2.1 Binary Join Tree Construction

If there are several queries on different domains, it is much more efficient to make use of a 'join tree'. A join tree consists of a set of nodes, where each node is connected to one or more neighbour nodes and where the initial potentials are distributed on the nodes. A join tree must also satisfy the Markov Property. That is, a variable which appears in two nodes appears also in every node on the path between the two nodes. Marginals are then computed on the basis of a message passing scheme, where nodes receive and send messages to their neighbour nodes. Therefore, a join tree can be seen as a data structure which allows the efficient computation of marginals.

As mentioned in Section 3.5.2, a BJT is a join tree where each node has at most, three neighbours, i.e. one parent and two children. The reference Evidential Network can be reorganised into a BJT, making the elimination of variables and data fusion process computationally simpler. This is useful if, as described earlier, the Evidential Network is dynamic since BJTs also allow for the re-evaluation of a network by recalculating the affected branch of the network (i.e. without the need to recalculate the entire network) when new input information becomes available. Data fusion processes are generally used for analysing static networks whereas BJTs are a more efficient choice when analysing dynamic networks.

An Evidential Network algorithm used to generate BJTs, previously written and coded in MATLAB [1], was used for this purpose. This MATLAB Evidential Network code was originally intended for prioritising threats in air domain scenarios and has now been applied to the AWW domain. Various heuristics can be used to generate BJTs [28] which are discussed in the following section.

To construct a BJT, we must first define: D^0, Δ, Θ_V, where:

- D^0 is the set of variables of interest for decision making.
- Δ is the set of variables to be eliminated (i.e. to arrive at D^0)
- Θ_V is the set of BBA valuations; m_1, m_2, …, etc.

We then apply a heuristic algorithm chosen to generate the BJT.

4.2.2 BJT and the Variable Elimination Sequence

To obtain the most efficient elimination sequence, we first need to construct a BJT, more generally referred to in mathematical terms as a hypertree structure. The concept of a hypertree, hyperedges[5] and the subsequent choice of a variable elimination sequence concept are explained in detail in Lehmann's dissertation [28]. A fusion algorithm, which can be used to compute marginals for any subset of variables, is then used to remove a variable 'x_i' at each step 'i' of the elimination process from the current set of potentials, 'Θ_i'.

[5] A hypergraph is a hypertree if it is acyclic. A hypergraph is a graph in which an edge can connect any number of vertices [28]. The corresponding edges of a hypertree are called hyperedges (or edges).

In order to determine the optimum hyper tree, in this case a BJT, it is necessary to find the hypertree whose largest hyper edge is as small as possible. This is recognised as an NP-complete problem. There are many heuristic algorithms that attempt to find optimal[6] hypertrees [28]. Most of these heuristics begin by first eliminating leaf nodes. The approaches then differ by eliminating either (i) nodes for which the associated clique[7] is as small as possible, (ii) nodes for which the associated focal set is as small as possible, or (iii) nodes for which the fewest fill-ins[8] for the associated clique are required. The heuristics include the One Step Look Ahead – Smallest Clique, Fewest Focal Sets (OSLA – SCFF) and the OLSA – Fewest Fill-Ins (OSLA-FFI) heuristic. These may result in BJTs of varying efficiency (i.e. different solution time), but they will ultimately yield the same final belief.

The MATLAB Evidential Network code (refer Section 4.2.1) uses the "One-Step-Look-Ahead Smallest Clique, Fewest Focal Sets" (OSLA-SC FFS) heuristic [28], which takes into account the size of the focal set of each variable whereas other heuristics generally do not. The other heuristics mentioned do not consider the number of configurations of each clique (i.e. most simply take into account the size of the clique) as each additional focal set effectively represents a different configuration. The OSLA-SC FFS considers the number of different focal set configurations of each closure which more precisely measures the costs of storing an individual focal set of the potential obtained at each step 'i' of the elimination process. The OSLA-SC FFS pseudo-algorithm as originally quoted by Lehmann [28] is:

OSLA – SC FFS.

1. If there is a leaf variable, eliminate it.
2. If there is no leaf variable, eliminate the variable 'x' for which the clique is as small as possible.
3. If there are several such variables, eliminate the variable 'x' for which the clique with the number of focal sets is as small as possible.
4. If there are several such variables, break ties arbitrarily.

The elimination sequence generated by the MATLAB Evidential Network code reportedly using the OSLA-SC FFS heuristic is:

IFFS, FPA, I, C, EM, FCR, CM, PC, PT, WER, HI, NF

{T} is not included in this sequence as it is not eliminated. The resulting BJT is illustrated in Figure 4-2. The sequence of the numbers annotated in the BJT diagram indicates the optimal message passing scheme between BBA's (not nodes). The nodes connected by the BBA's are shown inside the diamonds, with green BBA's being those associated with leaf nodes.

[6] Since heuristics are being used to identify efficient elimination sequences, it is prudent to refer to these schemes as near-optimal rather than optimal.

[7] In graph theory, a clique is a set of mutually adjacent nodes (i.e. a complete graph) in a graph. A clique is effectively a subset of vertices (i.e. a subgraph) of an undirected graph (i.e. a graph with edges with no orientation).

[8] Fill-ins are the number of pairs which are not connected. In other words, it is the number of connections that would need to be 'filled in' (i.e. added) if we were to eliminate a node from a graph.

Once a BJT is constructed, the next step is to initialise the valuations of the leaves (i.e. m_8 to m_{15}) of the BJT. This is essentially the first step of the message passing scheme; i.e. the inward propagation of information toward the root of the tree. The initialised leaf values are then propagated through the tree to the root node. The propagation process is performed using an inward propagation algorithm (IPA).

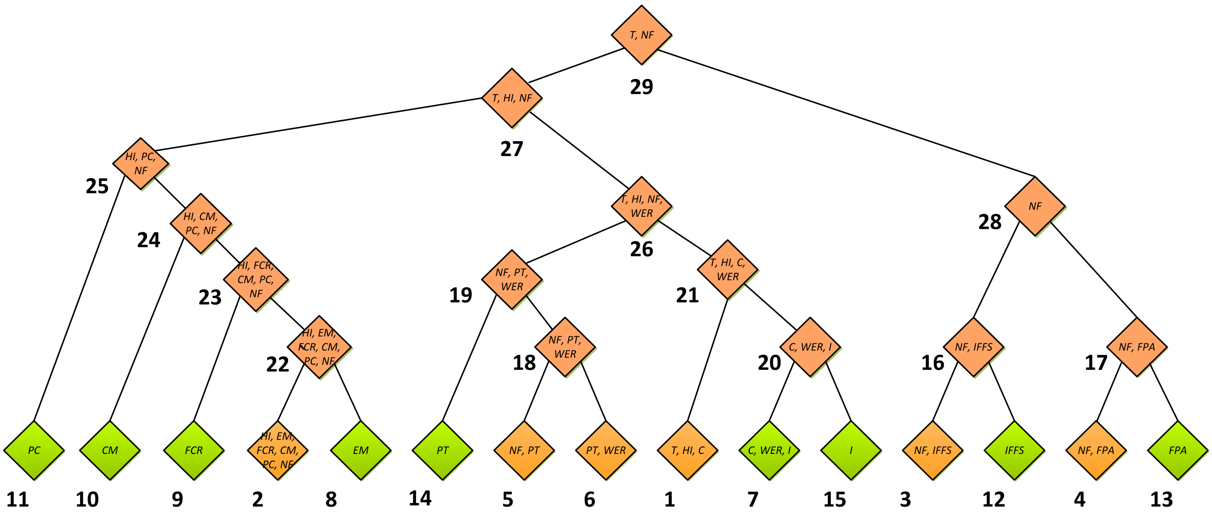


Figure 4-2 The reference threat model BJT using the OSLA-SC FFS heuristic. Numbers show sequence of application of the IPA (i.e. using combination/marginalisation) to marginalise to node T.

For example, consider variables: IFFS and FPA:

- IFFS and FPA are included in the domains of BBA's 3, 4, 12 and 13.
- These BBA's will be combined.
- Subtree of BBA's {3, 4, 12, 13, 16, 17, 28} shown in Figure 4-3 is used in interim steps of combination process.
- BBA 16 represents combination of BBA's 3 and 12.
- BBA 17 represents combination of BBA's 4 and 13.
- BBA 28 represents combination of BBA's 16 and 17.

Combine BBA's 3 and 12 to domain {NF, IFFS} as illustrated in Figure 4-3.

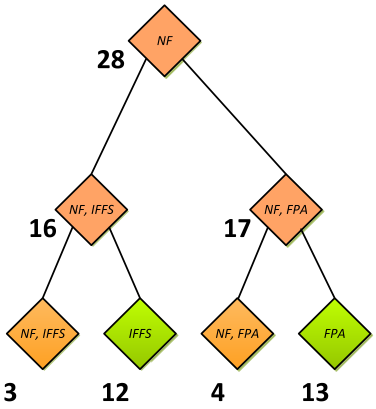


Figure 4-3 Subset of BJT covering domain {NF, IFFS}.

Extend m16 to common frame {NF, IFFS}:

$$d(m_3) = \{NF, IFFS\} \qquad d(m_{12}) = \{IFFS\}$$

$$m_{16} = m_{12} \oplus m_3^{\{IFFS\}\uparrow\{NF,IFFS\}} \qquad d(m_{16}) = \{NF, IFFS\}$$

Combine BBA's 4 and 13 to BBA 17, domain {NF, FPA} and extend m17 to common frame {NF, FPA}:

$$d(m_4) = \{NF, FPA\} \qquad d(m_{13}) = \{FPA\}$$

$$m_{17} = m_4 \oplus m_{13}^{\{FPA\}\uparrow\{NF,FPA\}} \qquad d(m_{17}) = \{NF, FPA\}$$

Combine BBA's 16 and 17 to BBA 28 using a vacuous extension to common frame {NF, IFFS, FPA}:

$$m_{28} = m_{16}^{\{NF,IFFS\}\uparrow\{NF,IFFS,FPA\}} \oplus m_{17}^{\{NF,FPA\}\uparrow\{NF,IFFS,FPA\}} \qquad d(m_{28}) = \{NF, IFFS, FPA\}$$

then marginalise to frame {NF}, thereby eliminating IFFS and FPA:

$$m_{28} = \left(m_{16}^{\{NF,IFFS\}\uparrow\{NF,IFFS,FPA\}} \oplus m_{17}^{\{NF,FPA\}\uparrow\{NF,IFFS,FPA\}}\right)^{\downarrow\{NF\}} \qquad d(m_{28}) = \{NF\}$$

new elimination sequence: ~~*IFFS, FPA*~~*, I, C, EM, FCR, CM, PC, PT, WER, HI, NF*

Next, consider variables: NF, PT & WER as shown in Figure 4-4.

- NF, PT & WER are included in the domains of BBA's 5, 6, 14, 18 & 19.
- These BBA's will be combined.
- Subtree of BBA's {5, 6, 14, 18, 19} shown in Figure 4-4 is used in interim steps of combination process.
- BBA 18 represents combination of BBA's 5 and 6

- BBA 19 represents combination of BBA's 14 and 18

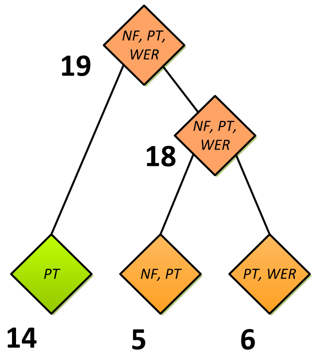


Figure 4-4 Subset of BJT covering domain {NF, PT, WER}.

$$d(m_5) = \{NF, PT\}$$
$$d(m_6) = \{PT, WER\}$$
$$m_{18} = m_5^{\{NF,PT\}\uparrow\{NF,PT,WER\}} \oplus m_6^{\{PT,WER\}\uparrow\{NF,PT,WER\}} \qquad d(m_{18}) = \{NF, PT, WER\}$$

Combine BBA's 14 and 18 to BBA 19, domain {NF, PT, WER}:

$$d(m_{14}) = \{PT\}$$
$$d(m_{18}) = \{NF, PT, WER\}$$
$$m_{19} = m_{18}^{\{NF,PT,WER\}} \oplus m_{14}^{\{PT\}\uparrow\{NF,PT,WER\}} \qquad d(m_{19}) = \{NF, PT, WER\}$$

Next, consider variables: T, HI, C, WER, I as shown in Figure 4-5:

- C, WER and I are included in the domains of BBA's 7, 15 and 20.
- These BBA's will be combined.
- Subtree of BBA's {1, 7, 15, 20, 21} shown in Figure 4-5 is used in interim steps of combination process.
- BBA 20 represents combination of BBA's 7 and 15
- BBA 21 represents combination of BBA's 1 and 20

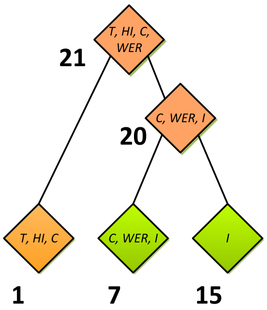


Figure 4-5 Subset of BJT covering domain {T, HI, C, WER, I}.

Combine BBA's 7 and 15 to BBA 20, domain {C, WER, I}:

$$\mathrm{d}(\mathrm{m}_7) = \{\mathrm{C}, \mathrm{WER}, \mathrm{I}\}$$
$$\mathrm{d}(\mathrm{m}_{15}) = \{\mathrm{I}\}$$
$$\mathrm{m}_{20} = \mathrm{m}_7^{\{\mathrm{C,WER,I}\}} \oplus \mathrm{m}_{15}^{\{\mathrm{I}\}\uparrow\{\mathrm{C,WER,I}\}} \qquad \mathrm{d}(\mathrm{m}_{20}) = \{\mathrm{C}, \mathrm{WER}, \mathrm{I}\}$$

Combine BBA's 20 and 1 to BBA 21, domain {T, HI, C, WER}:

$$\mathrm{d}(\mathrm{m}_1) = \{\mathrm{T}, \mathrm{HI}, \mathrm{C}\}$$
$$\mathrm{d}(\mathrm{m}_{20}) = \{\mathrm{C}, \mathrm{WER}, \mathrm{I}\}$$
$$\mathrm{m}_{21} = \mathrm{m}_{20}^{\{\mathrm{C,WER}\}\uparrow\{\mathrm{T,HI,C,WER,I}\}} \oplus \mathrm{m}_1^{\{\mathrm{T,HI,C}\}\uparrow\{\mathrm{T,HI,C,WER,I}\}} \qquad \mathrm{d}(\mathrm{m}_{21}) = \{\mathrm{T}, \mathrm{HI}, \mathrm{C}, \mathrm{WER}, \mathrm{I}\}$$

Marginalise BBA 21 to {T, HI, C, WER}:

$$m'_{21} = \left\{\mathrm{m}_{20}^{\{\mathrm{C,WER}\}\uparrow\{\mathrm{T,HI,C,WER,I}\}} \oplus \mathrm{m}_1^{\{\mathrm{T,HI,C}\}\uparrow\{\mathrm{T,HI,C,WER,I}\}}\right\}^{\downarrow\{\mathrm{T,HI,C,WER}\}}$$
$$\mathrm{d}(m'_{21}) = \{\mathrm{T}, \mathrm{HI}, \mathrm{C}, \mathrm{WER}\}$$

new elimination sequence: *~~IFFS, FPA, I,~~ C, EM, FCR, CM, PC, PT, WER, HI, NF*

Marginalise BBA 21 to {T, HI, WER}:

$$m'_{21} = \left\{\mathrm{m}_{21}^{\{\mathrm{T,HI,C,WER}\}}\right\}^{\downarrow\{\mathrm{T,HI,WER}\}} \qquad \mathrm{d}(m'_{21}) = \{\mathrm{T}, \mathrm{HI}, \mathrm{WER}\}$$

new elimination sequence: *~~IFFS, FPA, I, C~~, EM, FCR, CM, PC, PT, WER, HI, NF*

Next, consider variables: HI, EM, FCR, CM, PC, NF as shown in Figure 4-6.

- HI, EM, FCR, CM, PC and NF are included in the domains of BBA's 2 and 8.
- These BBA's will be combined.
- Subtree of BBA's 2, 8, 9, 10, 11, 22, 23, 24, 25} shown in Figure 4-6 is used in interim steps of combination process.
- BBA 22 represents combination of BBA's 2 and 8
- Marginalise BBA 22 to domain of BBA 23
- BBA 23 represents combination of BBA's 9 and 22
- Marginalise BBA 23 to domain of BBA 24
- BBA 24 represents combination of BBA's 10 and 23
- Marginalise BBA 22 to domain of BBA 25

- BBA 25 represents combination of BBA's 11 and 24

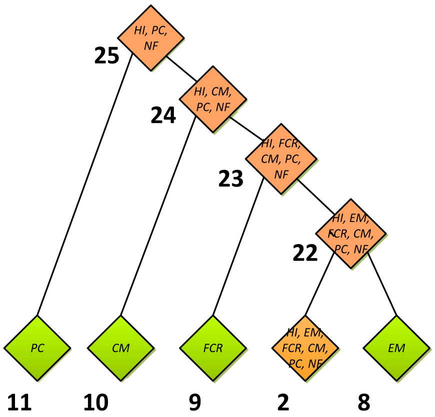


Figure 4-6 Subset of BJT covering domain { HI, EM, FCR, CM, PC, NF}.

Combine BBA's 2 and 8 to BBA 22, domain {HI, EM, FCR, CM, PC, NF }:

$$\mathrm{d}(\mathrm{m}_8) = \{\mathrm{EM}\}$$
$$\mathrm{d}(\mathrm{m}_2) = \{\mathrm{HI, EM, FCR, CM, PC, NF}\}$$
$$\mathrm{m}_{22} = \mathrm{m}_2^{\{\mathrm{HI,EM,FCR,CM,PC,NF}\}} \oplus \mathrm{m}_8^{\{\mathrm{EM}\}\uparrow\{\mathrm{HI,EM,FCR,CM,PC,NF}\}}$$
$$\mathrm{d}(\mathrm{m}_{22}) = \{\mathrm{HI, EM, FCR, CM, PC, NF}\}$$

Combine BBA's 9 and 22 to BBA 23, domain {HI, EM, FCR, CM, PC, NF }:

$$\mathrm{d}(\mathrm{m}_9) = \{\mathrm{FCR}\}$$
$$\mathrm{d}(\mathrm{m}_{22}) = \{\mathrm{HI, EM, FCR, CM, PC, NF}\}$$
$$\mathrm{m}_{23} = \mathrm{m}_{22}^{\{\mathrm{HI,EM,FCR,CM,PC,NF}\}} \oplus \mathrm{m}_9^{\{\mathrm{FCR}\}\uparrow\{\mathrm{HI,EM,FCR,CM,PC,NF}\}}$$
$$\mathrm{d}(\mathrm{m}_{23}) = \{\mathrm{HI, EM, FCR, CM, PC, NF}\}$$

Marginalise BBA 23 to { HI, FCR, CM, PC, NF }:

$$m_{23}' = \left\{\mathrm{m}_{22}^{\{\mathrm{HI,EM,FCR,CM,PC,NF}\}} \oplus \mathrm{m}_9^{\{\mathrm{FCR}\}\uparrow\{\mathrm{HI,EM,FCR,CM,PC,NF}\}}\right\}^{\downarrow\{\mathrm{HI,FCR,CM,PC,NF}\ \}}$$
$$\mathrm{d}(m_{23}') = \{\mathrm{HI, FCR, CM, PC, NF}\ \}$$

new elimination sequence: *~~IFFS, FPA, I, C, EM~~, FCR, CM, PC, PT, WER, HI, NF*

Combine BBA's 10 and 23 to BBA 24, domain {HI, FCR, CM, PC, NF }:

$$\mathrm{d}(\mathrm{m}_{10}) = \{\mathrm{CM}\}$$
$$\mathrm{d}(\mathrm{m}_{23}) = \{\mathrm{HI, FCR, CM, PC, NF}\}$$
$$\mathrm{m}_{24} = \mathrm{m}_{10}^{\{\mathrm{HI,FCR,CM,PC,NF}\}} \oplus \mathrm{m}_{23}^{\{\mathrm{CM}\}\uparrow\{\mathrm{HI,FCR,CM,PC,NF}\}} \qquad \mathrm{d}(\mathrm{m}_{24}) = \{\mathrm{HI, FCR, CM, PC, NF}\}$$

Marginalise BBA 24 to { HI, CM, PC, NF }:

$$m'_{24} = \left\{ \mathrm{m}_{10}^{\{\mathrm{HI,FCR,CM,PC,NF}\}} \oplus \mathrm{m}_{23}^{\{\mathrm{CM}\}\uparrow\{\mathrm{HI,FCR,CM,PC,NF}\}} \right\}^{\downarrow\{\mathrm{HI,CM,PC,NF}\}}$$
$$\mathrm{d}(m'_{24}) = \{\mathrm{HI, CM, PC, NF}\}$$

new elimination sequence: *~~IFFS, FPA, I, C, EM, FCR~~, CM, PC, PT, WER, HI, NF*

Combine BBA's 11 and 24 to BBA 25, domain {HI, CM, PC, NF}:

$$\mathrm{d}(\mathrm{m}_{11}) = \{\mathrm{PC}\}$$
$$\mathrm{d}(\mathrm{m}_{24}) = \{\mathrm{HI, CM, PC, NF}\}$$
$$\mathrm{m}_{25} = \mathrm{m}_{11}^{\{\mathrm{PC}\}\uparrow\{\mathrm{HI,CM,PC,NF}\}} \oplus \mathrm{m}_{24}^{\{\mathrm{HI,CM,PC,NF}\}} \qquad \mathrm{d}(\mathrm{m}_{25}) = \{\mathrm{HI, CM, PC, NF}\}$$

Marginalise BBA 25 to { HI, PC, NF }:

$$m'_{25} = \left\{ \mathrm{m}_{11}^{\{\mathrm{PC}\}\uparrow\{\mathrm{HI,CM,PC,NF}\}} \oplus \mathrm{m}_{24}^{\{\mathrm{HI,CM,PC,NF}\}} \right\}^{\downarrow\{\mathrm{HI,PC,NF}\}} \qquad \mathrm{d}(m'_{25}) = \{\mathrm{HI, PC, NF}\}$$

new elimination sequence: *~~IFFS, FPA, I, C, EM, FCR, CM~~, PC, PT, WER, HI, NF*

Marginalise BBA 25 to { HI, NF }:

$$m'_{25} = \left\{ \mathrm{m}_{25}^{\{\mathrm{HI,PC,NF}\}} \right\}^{\downarrow\{\mathrm{HI,NF}\}} \qquad \mathrm{d}(m'_{25}) = \{\mathrm{HI, NF}\}$$

new elimination sequence: *~~IFFS, FPA, I, C, EM, FCR, CM, PC~~, PT, WER, HI, NF*

Combine BBA's 19 and 21 to domain {T, HI, NF, PT, WER} as shown in Figure 4-7.

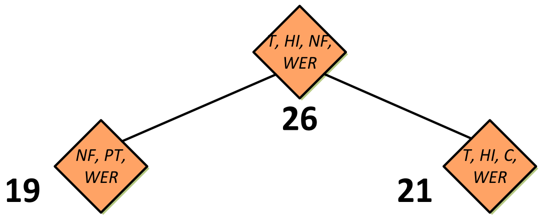


Figure 4-7 Subset of BJT covering domain { T, HI, NF, PT, WER}.

$$\mathrm{d}(\mathrm{m}_{19}) = \{\mathrm{NF, PT, WER}\}$$
$$\mathrm{d}(\mathrm{m}_{21}) = \{\mathrm{T, HI, WER}\}$$
$$\mathrm{m}_{26} = \mathrm{m}_{19}^{\{\mathrm{NF,WER}\}\uparrow\{\mathrm{T,HI,NF,PT,WER}\}} \oplus \mathrm{m}_{21}^{\{\mathrm{T,HI,WER}\}\uparrow\{\mathrm{T,HI,NF,PT,WER}\}}$$
$$\mathrm{d}(\mathrm{m}_{26}) = \{\mathrm{T, HI, NF, PT, WER}\}$$

Marginalise BBA 26 to {T, HI, NF, WER}:

new elimination sequence: *~~IFFS, FPA, I, C, EM, FCR, CM, PC, PT~~, WER, HI, NF*

$$m'_{26} = \left\{ \mathrm{m}_{19}^{\{\mathrm{NF,WER}\}\uparrow\{\mathrm{T,HI,NF,PT,WER}\}} \oplus \mathrm{m}_{21}^{\{\mathrm{T,HI,WER}\}\uparrow\{\mathrm{T,HI,NF,PT,WER}\}} \right\}^{\downarrow\{\mathrm{T,HI,NF,WER}\}}$$
$$\mathrm{d}(m'_{26}) = \{\mathrm{T, HI, NF, WER}\}$$

Combine BBA's 25 and 26 to BBA 27, domain {T, HI, NF,WER } as shown in Figure 4-8:

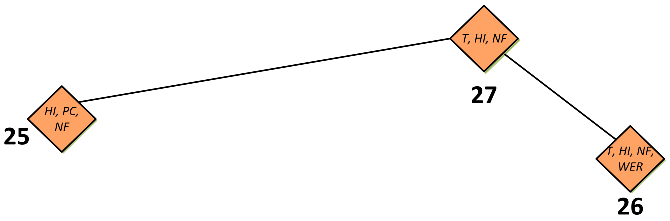


Figure 4-8 Subset of BJT covering domain {T, HI, NF, PT, WER}.

$$\mathrm{d}(\mathrm{m}_{25}) = \{\mathrm{HI, NF}\}$$
$$\mathrm{d}(\mathrm{m}_{26}) = \{\mathrm{T, HI, NF, WER}\}$$
$$\mathrm{m}_{27} = \mathrm{m}_{25}^{\{\mathrm{HI,NF}\}\uparrow\{\mathrm{T,HI,NF,WER}\}} \oplus \mathrm{m}_{26}^{\{\mathrm{T,HI,NF,WER}\}\uparrow\{\mathrm{T,HI,NF,WER}\}} \qquad \mathrm{d}(\mathrm{m}_{27}) = \{\mathrm{T, HI, NF, WER}\}$$

Marginalise BBA 27 to { T, HI, NF } as shown in Figure 4-9.

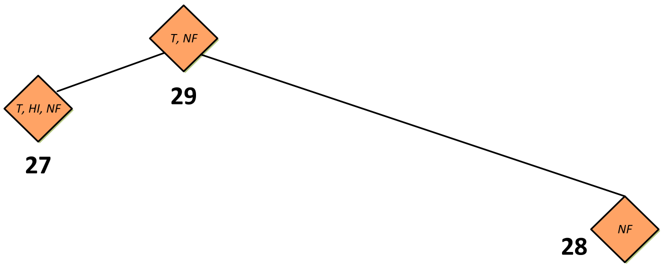


Figure 4-9 Subset of BJT covering domain {T, HI, NF}.

$$m'_{27} = \left\{ \mathrm{m}_{25}^{\{\mathrm{HI,NF}\}\uparrow\{\mathrm{T,HI,NF,WER}\}} \oplus \mathrm{m}_{26}^{\{\mathrm{T,HI,NF,WER}\}\uparrow\{\mathrm{T,HI,NF,WER}\}} \right\}^{\downarrow\{\mathrm{T,HI,NF}\}}$$
$$\mathrm{d}(m'_{27}) = \{\mathrm{T, HI, NF}\}$$

new elimination sequence: *~~IFFS, FPA, I, C, EM, FCR, CM, PC, PT, WER~~, HI, NF*

Combine BBA's 27 and 28 to BBA 29, domain {T, HI, NF}:

$$\mathrm{d}(\mathrm{m}_{27}) = \{\mathrm{T, HI, NF}\}$$
$$\mathrm{d}(\mathrm{m}_{28}) = \{\mathrm{NF}\}$$
$$\mathrm{m}_{29} = \mathrm{m}_{27}^{\{\mathrm{T,HI,NF}\}} \oplus \mathrm{m}_{28}^{\{\mathrm{NF}\}\uparrow\{\mathrm{T,HI,NF}\}} \qquad \mathrm{d}(\mathrm{m}_{29}) = \{\mathrm{T, HI, NF}\}$$

Marginalise BBA 29 to { T, NF }:

$m'_{29} = \left\{ \mathrm{m}_{27}^{\{\mathrm{T,HI,NF}\}} \oplus \mathrm{m}_{28}^{\{\mathrm{NF}\}\uparrow\{\mathrm{T,HI,NF}\}} \right\}^{\downarrow\{\mathrm{T,NF}\}}$ $\mathrm{d}(m'_{29}) = \{\mathrm{T,NF}\}$

new elimination sequence: ~~*IFFS, FPA, I, C, EM, FCR, CM, PC, PT, WER, HI*~~*, NF*

The output of the IPA thus far is the BBA 29, defined on the domain {T, NF}. The final step is to marginalise BBA 29 of the *root* of the BJT to the domain, D^0:

i.e. Marginalise BBA 29′ to { T}:

$m'_{29} = \left\{ \mathrm{m}_{29}^{\{\mathrm{T,NF}\}} \right\}^{\downarrow\{\mathrm{T}\}}$ $D^0 = \mathrm{d}(m'_{29}) = \{\mathrm{T}\}$

Completed elimination sequence: ~~*IFFS, FPA, I, C, EM, FCR, CM, PC, PT, WER, HI, NF*~~

All BBA's are finally projected on to D^0, the marginalised domain {T}.

4.2.3 Apply Pignistic Transformation

The final BBA, once marginalised to domain {T}, is transformed to the pignistic probability, which is a more usable parameter for purposes of threat prioritisation. A pignistic transformation is the probability measure that we use for decision making on the domain of interest within Evidential Networks. The pignistic transform of m^D is defined for every element of the frame $\theta \in \Theta_D$ as:

$$\mathrm{BetP}(\theta) = \sum_{\theta \in A \subseteq \theta_D} \frac{1}{|A|} \frac{m^D(A)}{1 - m^D(\emptyset)}$$

on the domain of interest $D_0 \subseteq V$.

4.3 Valuations for Intermediate Nodes

In order to apply the inward propagation algorithm (IPA), it is necessary to assign valuations to the intermediate BBA's; i.e. we need to assign values for the BBA's 1 to 7. These are often referred to as input valuations or prior valuations, since they are fixed values (at least in the time frames considered), whereas the leaf nodes have the potential to be dynamic. We use the values for BBA's m_1 to m_7 given previously in Section 4.1.3:

for m_1\{T, HI, C\}

$$m_1\left(\left\{\begin{matrix}(0,0,0),(1,0,1),\dots,(4,0,4),\\ \dots\\ (t,hi,c)\\ \dots\\ (6,6,0),(7,6,1),\dots,(10,6,4)\end{matrix}\right\}\right)=1$$

for m₂{HI, EM, FCR, CM, PC, NF}:

$$m_2\left(\left\{\begin{matrix}(0,0,0,0,0,0),(1,0,0,0,0,1),(1,0,0,0,1,0),\dots,(1,1,0,0,1,0)\\ (2,0,0,0,1,1),(2,0,0,1,1,0),(2,0,0,1,0,1),\dots,(2,1,0,1,0,0)\\ \dots\\ (hi,em,fcr,cm,pc,nf)\\ \dots\\ (5,0,1,1,1,1),(5,1,1,1,1,0),(5,1,1,1,0,1),\dots,(6,1,1,1,1,1)\end{matrix}\right\}\right)=1$$

for m₃{NF, IFFS} See table in Appendix A

for m₄{FPA, NF} See table in Appendix A

for m₅{NF, PT}

$$m_5\big((1,3),(1,4),(1,5),(0,0),(0,1),(0,2),(0,3),(0,4),(0,5)\big)=\ 0.50$$

$$m_5\big((1,0),(1,1),(1,2),(1,3),(1,4),(1,5),(0,0),(0,1),(0,2),(0,3),(0,4),(0,5)\big)=0.50$$

for m₆{PT, WER}

Rule 1: *PT* $\in\{0,1\}$ *WER = 0 with at least 40% confidence (a = 0.40).*

$$m_6^{D_1\cup D_2}\begin{pmatrix}(0,0),(1,0),(3,0),(3,1),(3,2),(3,3),\\ (4,0),(4,1),(4,2),(4,3),\\ (5,0),(5,1),(5,2),(5,3)\end{pmatrix}=0.40$$

$$m_6^{D_1\cup D_2}\begin{pmatrix}(0,0),(0,1),(0,2),(0,3),\\ (1,0),(1,1),(1,2),(1,3),\\ (2,0),(2,1),(3,2),(3,3)\\ (3,0),(3,1),(3,2),(3,3)\\ (4,0),(4,1),(4,2),(4,3)\\ (5,0),(5,1),(5,2),(5,3)\end{pmatrix}=0.60$$

Rule 2*: PT* $\in\{2,3\}$ *then WER* $\in\{1,2\}$ *with at least 40% confidence (a = 0.40).*

$$m_6^{D_1 \cup D_2}\begin{pmatrix} (2,1),(2,2),(3,1),(3,2), \\ (0,0),(0,1),(0,2),(0,3), \\ (1,0),(1,1),(1,2),(1,3), \\ (4,0),(4,1),(4,2),(4,3), \\ (5,0),(5,1),(5,2),(5,3) \end{pmatrix} = 0.40$$

$$m_6^{D_1 \cup D_2}\begin{pmatrix} (0,0),(0,1),(0,2),(0,3), \\ (1,0),(1,1),(1,2),(1,3), \\ (2,0),(2,1),(3,2),(3,3) \\ (3,0),(3,1),(3,2),(3,3) \\ (4,0),(4,1),(4,2),(4,3) \\ (5,0),(5,1),(5,2),(5,3) \end{pmatrix} = 0.60$$

Rule 3: $PT\ \in\ \{4,5\}$ *then* $WER\ \in\ \{2,3\}$ *with at least 40% confidence (a = 0.40).*

$$m_6^{D_1 \cup D_2}\begin{pmatrix} (4,2),(4,3),(5,2),(5,3), \\ (0,0),(0,1),(0,2),(0,3), \\ (1,0),(1,1),(1,2),(1,3), \\ (2,0),(2,1),(2,2),(2,3), \\ (3,0),(3,1),(3,2),(3,3) \end{pmatrix} = 0.40$$

$$m_6^{D_1 \cup D_2}\begin{pmatrix} (0,0),(0,1),(0,2),(0,3), \\ (1,0),(1,1),(1,2),(1,3), \\ (2,0),(2,1),(3,2),(3,3) \\ (3,0),(3,1),(3,2),(3,3) \\ (4,0),(4,1),(4,2),(4,3) \\ (5,0),(5,1),(5,2),(5,3) \end{pmatrix} = 0.60$$

for m$_7${C, WER, I}

$$m_7(\{(0,0,0),(1,0,1),(2,0,2),(1,1,0),(2,1,1),(3,1,2),(2,2,0),(3,2,1),(4,2,2),\}) = 1$$

Input valuations of BBA's 8 to 15 are assigned where information is known.

4.4 Valuations for Three Extreme Threat Cases

By way of example, input valuations at leaf nodes (BBA's 8 to 15) can be chosen for three extreme cases as demonstrated by Benavoli et al. [23]:

1. Total ignorance
2. High degree of threat
3. Low degree of threat

as listed in Table 4-2 (reproduced from [23]).

Table 4-2 Input valuations of leaf nodes are given by BBA's 8 to 15 with minimum and maximum degrees of threat focal set values.

Input Valuations:		Total ignorance		High degree of threat		Low degree of threat	
BBA	Domain	Focal set	Mass	Focal set	Mass	Focal set	Mass
m_8	EM	{0, 1}	1	{1}	1	{0}	1
m_9	FCR	{0, 1}	1	{1}	1	{0}	1
m_{10}	CM	{0, 1}	1	{1}	1	{0}	1
m_{11}	PC	{0, 1}	1	{1}	1	{0}	1
m_{12}	IFFS	{0, 1}	1	{0}	1	{1}	1
m_{13}	FPA	{0, 1}	1	{0}	1	{1}	1
m_{14}	PT	{0, 1, 2, 3, 4, 5}	1	{5}	1	{0}	1
m_{15}	I	{0, 1, 2}	1	{2}	1	{0}	1

NOTE:

1. For total ignorance (i.e. no information): all input valuations are represented by vacuous BBA's:

$$m_8\{0, 1\} = m_9\{0, 1\} = m_{10}\{0, 1\} = m_{11}\{0, 1\} = m_{12}\{0, 1\} =$$
$$m_{13}\{0, 1\} = m_{14}\{0, 1, 2, 3, 4, 5\} = m_{15}\{0, 1, 2\} = 1$$

2. For a high degree of threat: all BBA's are singletons taking on high threat values:

$$m_8\{1\} = m_9\{1\} = m_{10}\{1\} = m_{11}\{1\} = m_{12}\{0\} = m_{13}\{0\} = m_{14}\{5\} = m_{15}\{2\} = 1$$

3. For a low degree of threat: all BBA's are singletons taking on low threat values:

$$m_8\{0\} = m_9\{0\} = m_{10}\{0\} = m_{11}\{0\} = m_{12}\{1\} = m_{13}\{1\} = m_{14}\{0\} = m_{15}\{0\} = 1$$

In order to apply the inward propagation algorithm (IPA), it is necessary to assign valuations to the intermediate BBA's 1 to 7. These are often referred to as input valuations or prior valuations, since they are fixed values (at least in the time frames considered), whereas the leaf nodes have the potential to be dynamic. In this example, we use the values for BBA's m_1 to m_7 given previously in Section 4.1.3.

4.4.1 Results for Three Extreme Cases

The above BBA's were used as input to the MATLAB code and generated the results shown in Table 4-3. Results are given as pignistic probabilities as described in Sections 3.6 and 4.2.3.

As expected, total ignorance BBA's yield an even spread across all threat levels, BBA's with minimum threat indicators yield probabilities concentrated toward the lower overall threat level and BBA's with maximum threat indicators yield probabilities concentrated toward the higher overall threat level, respectively.

Table 4-3 Comparison of resultant pignistic probabilities at discrete threat levels produced using the three extreme case data provided in Table 4-2.

Threat	BetP (Pignistic Probability)		
Level	ignorance	min	max
0.0	0.0909	0.5562	0.0000
0.1	0.0909	0.2288	0.0000
0.2	0.0909	0.1988	0.0000
0.3	0.0909	0.0162	0.0000
0.4	0.0909	0.0000	0.0000
0.5	0.0909	0.0000	0.0000
0.6	0.0909	0.0000	0.0000
0.7	0.0909	0.0000	0.1215
0.8	0.0909	0.0000	0.1595
0.9	0.0909	0.0000	0.3215
1.0	0.0909	0.0000	0.3975

4.5 Comparison to Bayesian Network Approach

4.5.1 Node Edges

The conditional dependencies between variables in a Bayesian Network are represented by directed edges between the nodes. The concept used in Evidential Networks is similar to Bayesian Networks in that dependencies between nodes are also represented by links or edges. However, BBA's or masses are used to represent dependencies instead of probabilities where masses represent the degree of belief in a proposition, rather than a probability. BBA's are used to propagate evidence and uncertainty information through the Evidential Network. This is often referred to as a message passing scheme.

Furthermore, the links between nodes in an Evidential Network represent *joint valuations on the product space of the variables*. Conversely, the information associated with the edges between neighbouring nodes in a Bayesian Network represent simple conditional dependencies based on at least one common variable between parent and child node using the Bayes' Theorem; i.e. the concept of product spaces, and consequently disjoint product spaces, do not arise in Bayesian Networks.

4.5.2 Equation Descriptors

Equations, such as those used to describe the relationship of the Threat variable to the Hostile Intent and Capability variables are inherently deterministic; i.e. T = HI + C. Similarly for the HI intent variable, there is a simple linear relationship between HI and all of its parent nodes:

HI = EM + 2*FCR + CM + PC + NF

In such limited cases, the relationship between variables in Bayesian Networks and Evidential Networks can be described as being the same. Of course, the parent node inputs may differ due to the ways they are described, such as in the use of uncertain implication rules, it should be noted that such rules aren't formally part of Bayesian Networks.

4.5.3 Deterministic and Stochastic IF-THEN Rules

Where there is no uncertainty in relationships between nodes in IF-THEN relationships, then these relationships are equivalent to deterministic rules in both Bayesian Networks and Evidential Networks. However, in the case of the models presented in this paper, there exists uncertainty in some of the rules.

For example, as previously stated in Section 4, there are a number of stochastic 'if A then *probably* B' relationships (as opposed to a deterministic 'if A then B') which are described in Evidential Networks using uncertain implication rules developed using DST. For example, for the IFFS, NF relationship, the following two rules were presented in Section 4.1.3 and detailed in Appendix A.

Rule 1: *We are 95 to 100% confident that if there is a correct response to IFFS squawking (IFFS=1), then the target is actually a friend (NF=0). That is if IFFS=1* $(iffs)$ *then NF=0* (nf) *with at least 95% confidence.*

$$m_3^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ 1-\alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

α = 0.95

$$m_3^{D_1 \cup D_2}(C) = 0.95 \quad C = (iffs \times nf) \cup \left(\overline{iffs} \times \left(nf, \overline{nf}\,\right)\right)$$
$$m_3^{D_1 \cup D_2}\left((iffs, nf), \left(\overline{iffs}, nf\right), \left(\overline{iffs}, \overline{nf}\right)\right) = 0.95$$

Rule 2: *Conversely, if there is no response to the IFFS interrogation then we are only 10 to 30% confident that the target is non-friendly.*

$$m_3^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ 1-\beta & C = (A \times \bar{B}) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ \beta-\alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$$m_3^{D_1 \cup D_2}(C) = \begin{cases} 0.1 & C = \left(\overline{iffs} \times nf\right) \cup \left(iffs \times \left(nf, \overline{nf}\right)\right) \\ 1 - 0.3 & C = \left(\overline{iffs} \times \overline{nf}\right) \cup \left(iffs \times \left(nf, \overline{nf}\right)\right) \\ 0.3 - 0.1 & C = \left(iffs, \overline{iffs}\right) \times \left(nf, \overline{nf}\right) \end{cases}$$

$$m_3^{D_1 \cup D_2}\left(\left(\overline{iffs}, nf\right), \left(iffs, nf\right), \left(iffs, \overline{nf}\right)\right) = 0.1$$
$$m_3^{D_1 \cup D_2}\left(\left(\overline{iffs}, \overline{nf}\right), \left(iffs, nf\right), \left(iffs, \overline{nf}\right)\right) = 0.7$$
$$m_3^{D_1 \cup D_2}\left(\left(iffs, \overline{nf}\right), \left(iffs, nf\right), \left(\overline{iffs}, \overline{nf}\right), \left(\overline{iffs}, nf\right)\right) = 0.2$$

It should be noted that in contrast with a Bayesian Network approach, we are only able to define the basic if-then relationships. The closest approximation to Rule 1 in a Bayesian Network is:

$$p(NF \mid IFFS = 1) = 0.95$$

And to Rule 2, the following is a very approximate Bayesian Network version of the Evidential Network rule:

$$p(NF \mid IFFS = 0) = 0.20$$

Although there may be more accurate Bayesian Network versions of the Evidential Network rule, the Bayesian rule approximation was used for demonstration purposes. As shown in Appendix A, the BBA notation for the *IFFS, NF* relationship is far more complex mathematically than its Bayesian Network equivalent, which is an obvious deterrent to using the Evidential Network approach.

5. New Threat Model

5.1 Introduction

The Evidential Network solution from Chapter 4 is aimed at solving the threat evaluation problem in the air domain, and has been adapted by the author to address a generic threat evaluation in the AWW domain. The solution adaptation in this section is presented as a first iteration of a potentially useful and practical approach to threat evaluation in the AWW domain. It is not the author's intention to evaluate the solution in this report, but merely to present it for consideration. The Evidential Network methodology used for the threat evaluation was covered in detail in Chapter 4, so only the specific information describing the new threat model will be presented in the following sections.

5.2 Threat model parameters

The threat model parameters listed in Table 5-1 represent the node variables in the new threat model shown in Figure 5-1. Although there are similarities between these parameters and those in the reference threat model, there is a significant difference in the approach to assessing threats.

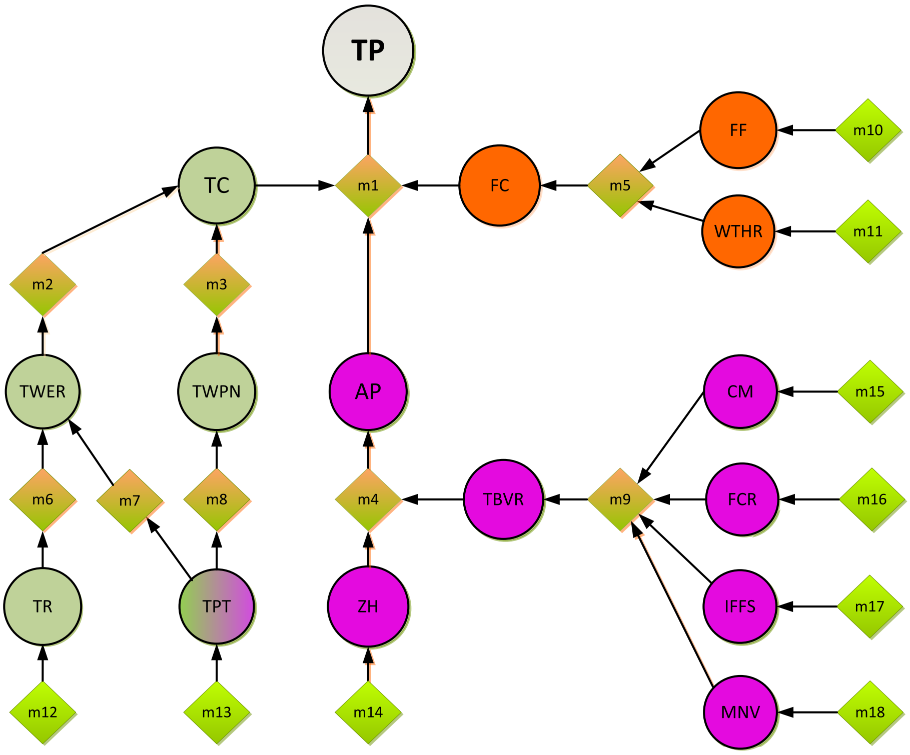


Figure 5-1 New threat model Evidential Network showing variable nodes in purple circles, BBA's in diamonds, with leaf and intermediate BBA's shown in green and green/orange, respectively.

Whereas Benavoli began with the premise that Threat had a linear relationship with Hostile Intent (HI) and Capability (C), the model presented here relates Threat Priority (TP) to Attack Possibility (AP), Threat Capability (TC) and Firing Constraints (FC). TC is defined in a similar manner to C in the reference threat model, with relationships to the target's weapon engagement range (TWER) and actual weaponry (TWPN). Although there is a strong relationship between the threat's potential weaponry (TWPN) and weapon engagement range (TWER), these two parameters have been included in this model, although they could easily be refined to a single parameter if needed.

Table 5-1 Parameters used to generate the Evidential Network for the new threat model.

Parameter	Symbol	Frame	Frame Min	Frame Max
Threat Priority	TP	{0, 1,…10}	lowest threat	highest threat
Attack Possibility	AP	{0, 1, … 7}	benign	maximum hostility
Threat Capability	TC	{0, 1… 4}	no capability	highest capability
Firing Constraints	FC	{0, 1, 2, 3}	No firing constraints	Highest firing constraints
Threat: Weapon Engagement Range	TWER	Short, medium, long-range	Short range	Long range
Threat: Weaponry	TWPN	NONE, MOD, FULL	No weapons	Highly weaponised
Threat Behaviour	TBVR	{0, 1, … 5}	Non-hostile behaviour	Hostile behaviour
Zone Hostility	ZH	PCE, HOS, WAR	Peace	War
Friendly Fire	FF	T/F	Possibility of friendly fire	No possibility of friendly fire
Weather	WTHR	CALM, MOD, EXTM	Extreme weather conditions	Ideal weather conditions
Target Range	TR	{0, 1, 2, 3}	Target at close range	Target at long range
Target Platform	TPT	{0, 1, 2, 3}	Non-military platform	Military, highly weaponised, high-value unit
Countermeasures	CM	T/F	Countermeasures not used	Countermeasures used
Fire Control Radar status	FCR	ON/OFF	FCR is off	FCR is on
Identify Friend or Foe Squawk	IFFS	T/F	Correct IFFS response	Incorrect IFFS response
Suspect Manoeuvre	MNV	T/F	No suspect manoeuvres observed	Suspect manoeuvres observed

In this model, AP is used in preference to HI. HI was previously defined according to: HI = EM + 2*FCR + CM + PC + NF, where NF is related to IFFS and FCR by means of two separate BBA's. In this case, AP, which is defined below in Table 5-1 as AP = ZH + TBVR, where TBVR is related to CM, FCR, IFFS and MNV by four BBA's. EM and MNV are equivalent parameters, as are PC and ZH, and WER and TR, in their respective models. The choice of the term AP over HI is subtle; from the author's perspective, AP implies circumstantial knowledge of the enemy's intentions whereas the term HI implies actual knowledge. This statement in itself is a matter of personal interpretation.

An additional parameter, Firing Constraints (FC), has also been added. The FC parameter represents factors that hinder the assignment of a relatively higher priority to particular threats through environmental constraints, such as the poor weather conditions, or the risk of friendly fire causing destruction of nearby assets. In effect, the FC parameter serves to reduce threat level rather than increase it (i.e. in contrast other listed parameters).

For example, in the case of two otherwise equivalent threats, where one is isolated in a blue water scenario and the other is in a littoral environment with other friendly assets nearby, the former would be prioritised ahead of the latter. FC is related to FF and WTHR by means of two separate BBA's. Although weather conditions (WTHR) may be perceived to be equivalent for all threats, there may for example, be precipitation or similar local weather in the direction of particular targets.

Otherwise, there are some minor notational differences in the description of parameters. Frame minima and maxima are listed in Table 5-1 relating typically to minimum and maximum threat levels. The discrete numerical threat values shown in the Frame column are arbitrary and can be tailored to suit the analyst's needs.

5.3 Basic Belief Assignments

The Evidential Network presented in Figure 5-1 shows nodes and belief masses (i.e. BBA's) in circles and diamonds, respectively. The green diamonds (m_{10} to m_{18}) are associated with leaf nodes and can be varied according to available input data. The Evidential Network shown in Figure 5-1 is in a similar manner to the reference threat model which has a 5 tuple, VBS: $\{D, \Theta_D, \Phi_D, \oplus, \downarrow\}$, however with a domain: D = {TP, TC, AP, FC, TWER, TWPN, TBVR, TPT, TR, ZH, CM, FCR, IFFS, MNV, WTHR, FF}

The 18 BBA's are calculated according to their rules described below. Some BBA's, such as m_1, have simple linear rules, whereas other BBA's have uncertain 'if-then' implication rules with degrees of confidence (e.g. m_2, m_3, etc.). The first nine BBA's (m_1 to m_9) represent the generic knowledge of the Evidential Network, whereas the remaining nine BBA's (m_{10} to m_{18}) represent the available evidence, typically through observations about the Evidential Network. Put in another way, in the case of this particular threat model, m_1 to m_9 represent knowledge about existing relationships between variables, whereas m_{10} to m_{18} represent organic information, such as real-time sensor data.

The rules provided are not necessarily representative of the most accurate threat relationships for these parameters.

5.3.1 Intermediate Nodes

The rules for intermediate BBA's m_1 to m_9 for the new threat model are outlined below.

BBA for m_1:
In this model, the Threat Prioritisation level variable, TP, is dependent on the Attack Possibility variable, AP, the Threat Capability variable, TC, and to a lesser extent, the Collateral Damage Risk, CDR, according to the simple linear rule:

TP = 2*TC + AP + FC

$$\Theta_{D_1} = \{0,1,2,\ldots,10\} \quad \Theta_{D_2} = \{0,1,2,3,4\}$$
$$\Theta_{D_3} = \{0,1,2,\ldots,7\} \quad \Theta_{D_4} = \{0,1,2,3\}$$

$$m_1^{D_1 \cup D_2 \cup D_3 \cup D_4}(tp, tc, ap, fc) = 1.00$$

where: *tp = 2*tc + ap + fc (2*4 + 7 + 3 = 18 so will need to be normalised to 10)*

$$m_1^{D_1 \cup D_2 \cup D_3 \cup D_4}\begin{pmatrix}(0,0,0,0),(1,0,0,1),(1,0,1,0),(1,0,1,1),\\(2,1,0,0),(3,1,0,1),(3,1,1,0),(4,1,1,1)\end{pmatrix} = 1.00$$

Here, TC is given a coefficient of '2', indicating a higher weighting in relation to the AP and FC parameters. Consequently, the BBA m_1 is defined according to this rule on the product space, *TP x TC x AP x FC.*

BBA for m_2:
The second BBA relates to the Threat Weapons' Engagement Range (TWER) and Target Capability (TC) variables and consequently exists on the {TWER, TC} domain. The 'uncertain implication rule' formulation is used here: Here the *a priori* knowledge is that:

> ***Rule 1:*** *We are 95 to 100% confident that if the Target's WER is poor (i.e. TWER=1), then the resultant Target Capability (TC) is low (i.e.* $TC \in \{0,1\}$*). That is if TWER=1 then TC= 0 or 1 with at least 95% confidence.*
>
> ***Rule 2:*** *We are 95 to 100% confident that if the TWER is moderate (i.e. TWER=2), then the resultant TC is medium (i.e.* $TC \in \{1,2\}$*). That is if TWER=2 then TC= 1 or 2 with at least 95% confidence.*
>
> ***Rule 3:*** *We are 95 to 100% confident that if the TWER is optimum (i.e. TWER=3), then the resultant TC is maximum (i.e.* $TC \in \{3,4\}$*). That is if TWER=3 then TC= 3 or 4 with at least 95% confidence.*

The BBA m2 is defined according to this rule on the product space, *TWER x TC*.

m2: is defined on the domain {TWER, TC}. There is different methodology used here as there is uncertainty in the implication rules: For example, *a priori* knowledge that:

Rule 1: *If TWER = {1} then TC = {0, 1} with at least 95% confidence.*

$$m_2^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup (\bar{A} \times \Theta_{D_2}) \\ 1-\alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$\Theta_{D_1} = \{POOR, MOD, OPT\}$ $\Theta_{D_2} = \{0,1,2,3,4\}$

Or: $\Theta_{D_1} = \{1,2,3\}$ $\Theta_{D_2} = \{0,1,2,3,4\}$

$\Theta_{D_1} = \{twer, \overline{twer}\}$ $\Theta_{D_2} = \{tc, \overline{tc}\}$

In this case: *twer* = {1} $\overline{twer}$= {2, 3}

And: *tc* = {0, 1} $\overline{tc}$= {2, 3, 4}

$$m_2^{D_1 \cup D_2}(C) = \alpha \quad C = (twer \times tc) \cup (\overline{twer} \times \Theta_{D_2})$$
$$m_2^{D_1 \cup D_2}(C) = 0.95 \quad C = (twer \times tc) \cup (\overline{twer} \times (tc, \overline{tc}\,))$$
$$m_2^{D_1 \cup D_2}((twer, tc), (\overline{twer}, tc), (\overline{twer}, \overline{tc})) = 0.95$$

So:

$(twer, tc)$ = {(1, 0), (1, 1)}
$(\overline{twer}, tc)$ = {(2, 0), (2, 1), (3, 0), (3, 1)}
$(twer, \overline{tc})$ = {(1, 2), (1, 3), (1, 4)}
$(\overline{twer}, \overline{tc})$ = {(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)}

$$m_2^{D_1 \cup D_2}\begin{pmatrix}(1,0),(1,1),(2,0),(2,1),(3,0),(3,1), \\ (2,2),(2,3),(2,4),(3,2),(3,3),(3,4)\end{pmatrix} = 0.95$$

And:

$$m_2^{D_1 \cup D_2}(C) = 1-\alpha \quad C = \Theta_{D_1 \cup D_2}$$
$$m_2^{D_1 \cup D_2}(C) = 0.05 \quad C = (twer, \overline{twer}) \times (tc, \overline{tc})$$

$$m_2^{D_1 \cup D_2}((twer, tc), (\overline{twer}, tc), (twer, \overline{tc}), (\overline{twer}, \overline{tc})) = 0.05$$

$$m_2^{D_1 \cup D_2}\begin{pmatrix}(1,0),(1,1),(2,0),(2,1),(3,0), \\ (3,1),(1,2),(1,3),(1,4),(2,2), \\ (2,3),(2,4),(3,2),(3,3),(3,4)\end{pmatrix} = 0.05$$

Rule 2: *If TWER= 2 then* $TC = \{2,3\}$ *with at least 95% confidence.*

$$m_2^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup (\bar{A} \times \Theta_{D_2}) \\ 1-\alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$\Theta_{D_1} = \{POOR, MOD, OPT\}$ $\Theta_{D_2} = \{0,1,2,3,4\}$

Or: $\Theta_{D_1} = \{1,2,3\}$ $\Theta_{D_2} = \{0,1,2,3,4\}$

$\Theta_{D_1} = \{twer, \overline{twer}\}$ $\Theta_{D_2} = \{tc, \overline{tc}\}$

In this case: $twer = \{2\}$ $\overline{twer} = \{1, 3\}$

And: $tc = \{2, 3\},$ $\overline{tc} = \{0, 1, 4\}$

$$m_2^{D_1 \cup D_2}(C) = \alpha \qquad C = (twer \times tc) \cup \left(\overline{twer} \times \Theta_{D_2}\right)$$
$$m_2^{D_1 \cup D_2}(C) = 0.95 \qquad C = (twer \times tc) \cup \left(\overline{twer} \times (tc, \overline{tc}\,)\right)$$
$$m_2^{D_1 \cup D_2}\left((twer, tc), (\overline{twer}, tc), (\overline{twer}, \overline{tc})\right) = 0.95$$

So:

$(twer, tc) = \{(2, 2), (2, 3)\}$
$(\overline{twer}, tc) = \{(1, 2), (1, 3), (3, 2), (3, 3)\}$
$(twer, \overline{tc}) = \{(2, 0), (2, 1), (2, 4)\}$
$(\overline{twer}, \overline{tc}) = \{(1, 0), (1, 1), (1, 4), (3, 0), (3, 1), (3, 4)\}$

$$m_2^{D_1 \cup D_2}\begin{pmatrix}(2,2),(2,3),(1,2),(1,3),(3,2),(3,3),\\(1,0),(1,1),(1,4),(3,0),(3,1),(3,4)\end{pmatrix} = 0.95$$

And:

$$m_2^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$$
$$m_2^{D_1 \cup D_2}(C) = 0.05 \quad C = (twer, \overline{twer}) \times (tc, \overline{tc})$$

$$m_2^{D_1 \cup D_2}\left((twer, tc), (\overline{twer}, tc), (twer, \overline{tc}), (\overline{twer}, \overline{tc})\right) = 1 - \alpha$$

$$m_2^{D_1 \cup D_2}\begin{pmatrix}(2,2),(2,3),(1,2),(1,2),(3,3),\\(3,3),(2,0),(2,1),(2,4),(1,0),\\(1,1),(1,4),(3,0),(3,1),(3,4)\end{pmatrix} = 0.05$$

Rule 3: *If TWER=3 then TC= 3 or 4 with at least 95% confidence.*

$\Theta_{D_1} = \{POOR, MOD, OPT\}$ $\Theta_{D_2} = \{0, 1, 2, 3, 4\}$

Or: $\Theta_{D_1} = \{1, 2, 3\}$ $\Theta_{D_2} = \{0, 1, 2, 3, 4\}$

$\Theta_{D_1} = \{twer, \overline{twer}\}$ $\Theta_{D_2} = \{tc, \overline{tc}\}$

In this case: twer = {3} $\overline{twer}$= {1, 2}

And: tc = {3, 4} $\overline{tc}$= {0, 1, 2}

$$m_2^{D_1 \cup D_2}(C) = \alpha \qquad C = (twer \times tc) \cup \left(\overline{twer} \times \Theta_{D_2}\right)$$
$$m_2^{D_1 \cup D_2}(C) = 0.95 \qquad C = (twer \times tc) \cup \left(\overline{twer} \times (tc, \overline{tc}\,)\right)$$
$$m_2^{D_1 \cup D_2}\left((twer, tc), (\overline{twer}, tc), (\overline{twer}, \overline{tc})\right) = 0.95$$

So:

$(twer, tc) = \{(3, 3), (3, 4)\}$
$(\overline{twer}, tc) = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$
$(twer, \overline{tc}) = \{(3, 0), (3, 1), (3, 2)\}$

$(\overline{twer}, \overline{tc})$ = {(1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (2, 2)}

$$m_2^{D_1 \cup D_2}\begin{pmatrix}(3,3),(3,4),(1,3),(1,4),(2,3),(2,4),\\(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\end{pmatrix} = 0.95$$

And: $m_2^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$

$m_2^{D_1 \cup D_2}(C) = 0.05 \quad C = (twer, \overline{twer}) \times (tc, \overline{tc})$

$$m_2^{D_1 \cup D_2}\big((twer, tc), (\overline{twer}, tc), (twer, \overline{tc}), (\overline{twer}, \overline{tc})\big) = 0.05$$

$$m_2^{D_1 \cup D_2}\begin{pmatrix}(3,3),(3,4),(1,3),(1,4),(2,3),(2,4),\\(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\end{pmatrix} = 0.05\ (1 - \alpha)$$

BBA for m$_3$:

The third BBA is based on the Threat Weaponry (TWPN) and Target Capability (TC) variables, respectively and exists on the {TWPN, TC} domain. Uncertainty in the implication rules methodology is used here: Here the *a priori* knowledge is that:

> ***Rule 1:*** *We are 90 to 100% confident that if there are no effective weapons (i.e. TWPN=0), then the resultant Target Capability will be zero (i.e. TC = 0). That is if TWPN=0 then TC=0 with at least 95% confidence.*
>
> ***Rule 2:*** *We are 90 to 100% confident that if the only type I weapons are available (i.e.* $TWPN \in \{1\}$*), then the resultant Target Capability is low to medium (i.e. TC = 1, 2). That is if TWPN=1, then* $TC \in \{1, 2\}$*with at least 95% confidence.*
>
> ***Rule 3:*** *We are 90 to 100% confident that if the only type II weapons are available (i.e.* $TWPN \in \{2\}$*), then the resultant Target Capability is high to max (i.e. TC = 3, 4). That is if TWPN=2, then* $TC \in \{3, 4\}$ *with at least 95% confidence.*

The BBA m$_3$ is defined according to this rule on the product space, *TWPN x TC*.

m$_2$: is defined on the domain {TWPN, TC}. There is different methodology used here as there is uncertainty in the implication rules: For example, *a priori* knowledge that:

Rule 1: *If twpn = {0} then tc = {0} with at least 95% confidence.*

$$m_3^{D_1 \cup D_2}(C) = \begin{cases}\alpha & C = (A \times B) \cup (\bar{A} \times \Theta_{D_2})\\ 1 - \alpha & C = \Theta_{D_1 \cup D_2}\end{cases}$$

$\Theta_{D_1} = \{NONE, MOD, FULL\}$ $\Theta_{D_2} = \{0, 1, 2, 3, 4\}$

Or: $\Theta_{D_1} = \{0, 1, 2\}$ $\Theta_{D_2} = \{0, 1, 2, 3, 4\}$

$\Theta_{D_1} = \{twpn, \overline{twpn}\}$ $\Theta_{D_2} = \{tc, \overline{tc}\}$

In this case: *twpn* = {0} $\overline{twpn}$= {1, 2}

And: *tc* = {0} $\overline{tc}$= {1, 2, 3, 4}

$$m_3^{D_1 \cup D_2}(C) = \alpha \qquad C = (twpn \times tc) \cup \left(\overline{twpn} \times \Theta_{D_2}\right)$$
$$m_3^{D_1 \cup D_2}(C) = 0.90 \quad C = (twpn \times tc) \cup \left(\overline{twpn} \times (tc, \overline{tc})\right)$$
$$m_3^{D_1 \cup D_2}\left((twpn, tc), (\overline{twpn}, tc), (\overline{twpn}, \overline{tc})\right) = 0.90$$

So:

$(twpn, tc) = \{(0, 0)\}$
$(\overline{twpn}, tc) = \{(1, 0), (2, 0)\}$
$(twpn, \overline{tc}) = \{(0, 1), (0, 2), (0, 3), (0, 4)\}$
$(\overline{twpn}, \overline{tc}) = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (2, 4)\}$

$$m_3^{D_1 \cup D_2}\begin{pmatrix} (0,0),(1,0),(2,0),(1,1),(1,2), \\ (1,3),(1,4),(2,1),(2,2),(2,3),(2,4) \end{pmatrix} = 0.90$$

And:

$$m_3^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$$
$$m_3^{D_1 \cup D_2}(C) = 0.10 \quad C = (twpn, \overline{twpn}) \times (tc, \overline{tc})$$
$$m_3^{D_1 \cup D_2}\left((twpn, tc), (\overline{twpn}, tc), (twpn, \overline{tc}), (\overline{twpn}, \overline{tc})\right) = 0.10$$

$$m_3^{D_1 \cup D_2}\begin{pmatrix} (0,0),(1,0),(2,0),(0,1),(0,2), \\ (0,3),(0,4),(1,1),(1,2),(1,3), \\ (1,4),(2,1),(2,2),(2,3),(2,4) \end{pmatrix} = 0.10$$

Rule 2: *If TWPN=1, then TC = 1 or 2 with at least 95% confidence.*

$$m_3^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ 1 - \alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$\Theta_{D_1} = \{NONE, MOD, FULL\}$ $\quad \Theta_{D_2} = \{0, 1, 2, 3, 4\}$

Or: $\Theta_{D_1} = \{0, 1, 2\}$ $\quad \Theta_{D_2} = \{0, 1, 2, 3, 4\}$

$\Theta_{D_1} = \{twpn, \overline{twpn}\}$ $\quad \Theta_{D_2} = \{tc, \overline{tc}\}$

In this case: *twpn* = {1} $\quad \overline{twpn}$= {0, 2}

And: *tc* = {1, 2} $\quad \overline{tc}$= {0, 3, 4}

$$m_3^{D_1 \cup D_2}(C) = \alpha \qquad C = (twpn \times tc) \cup \left(\overline{twpn} \times \Theta_{D_2}\right)$$
$$m_3^{D_1 \cup D_2}(C) = 0.90 \quad C = (twpn \times tc) \cup \left(\overline{twpn} \times (tc, \overline{tc})\right)$$
$$m_3^{D_1 \cup D_2}\left((twpn, tc), (\overline{twpn}, tc), (\overline{twpn}, \overline{tc})\right) = 0.90$$

So:

$(twpn, tc) = \{(1, 1), (1, 2)\}$
$(\overline{twpn}, tc) = \{(0, 1), (0, 2), (2, 1), (2, 2)\}$
$(twpn, \overline{tc}) = \{(1, 0), (1, 3), (1, 4)\}$
$(\overline{twpn}, \overline{tc}) = \{(0, 0), (0, 3), (0, 4), (2, 0), (2, 3), (2, 4)\}$

$$m_3^{D_1 \cup D_2}\begin{pmatrix} (1,1),(1,2),(0,1),(0,2),(2,1),(2,2), \\ (0,0),(0,3),(0,4),(2,0),(2,3),(2,4) \end{pmatrix} = 0.90$$

And: $m_3^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$

$m_3^{D_1 \cup D_2}(C) = 0.10 \quad C = (twpn, \overline{twpn}) \times (tc, \overline{tc})$

$$m_3^{D_1 \cup D_2}\left((twpn, tc), (\overline{twpn}, tc), (twpn, \overline{tc}), (\overline{twpn}, \overline{tc})\right) = 0.10$$

$$m_3^{D_1 \cup D_2}\begin{pmatrix} (1,1), (1,2), (0,1), (0,2), (2,1), \\ (2,2), (1,0), (1,3), (1,4), (0,0), \\ (0,3), (0,4), (2,0), (2,3), (2,4) \end{pmatrix} = 0.10$$

Rule 3: *If TWPN=2, then TC = 3 or 4, with at least 95% confidence.*

$$m_3^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ 1 - \alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$\Theta_{D_1} = \{NONE, MOD, FULL\} \quad \Theta_{D_2} = \{0, 1, 2, 3, 4\}$

Or: $\Theta_{D_1} = \{1, 2, 3\} \qquad \Theta_{D_2} = \{0, 1, 2, 3, 4\}$

$\Theta_{D_1} = \{twpn, \overline{twpn}\} \qquad \Theta_{D_2} = \{tc, \overline{tc}\}$

In this case: $twpn = \{2\} \qquad \overline{twpn} = \{0, 1\}$

And: $tc = \{3, 4\} \qquad \overline{tc} = \{0, 1, 2\}$

$m_3^{D_1 \cup D_2}(C) = \alpha \quad C = (twpn \times tc) \cup \left(\overline{twpn} \times \Theta_{D_2}\right)$

$m_3^{D_1 \cup D_2}(C) = 0.90 \quad C = (twpn \times tc) \cup \left(\overline{twpn} \times (tc, \overline{tc})\right)$

$m_3^{D_1 \cup D_2}\left((twpn, tc), (\overline{twpn}, tc), (\overline{twpn}, \overline{tc})\right) = 0.90$

So:

$(twpn, tc) = \{(2, 3), (2, 4)\}$

$(\overline{twpn}, tc) = \{(0, 3), (0, 4), (1, 3), (1, 4)\}$

$(twpn, \overline{tc}) = \{(2, 0), (2, 1), (2, 2)\}$

$(\overline{twpn}, \overline{tc}) = \{(0, 0), (0, 1), (0, 2), (2, 0), (2, 1), (2, 2)\}$

$$m_3^{D_1 \cup D_2}\begin{pmatrix} (2,3), (2,4), (0,3), (0,4), (1,3), (1,4), \\ (0,0), (0,1), (0,2), (2,0), (2,1), (2,2) \end{pmatrix} = 0.90$$

And: $m_3^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$

$m_3^{D_1 \cup D_2}(C) = 0.10 \quad C = (twpn, \overline{twpn}) \times (tc, \overline{tc})$

$$m_3^{D_1 \cup D_2}\left((twpn, tc), (\overline{twpn}, tc), (twpn, \overline{tc}), (\overline{twpn}, \overline{tc})\right) = 0.10$$

$$m_3^{D_1 \cup D_2}\begin{pmatrix} (2,3), (2,4), (0,3), (0,4), (1,3), \\ (1,4), (2,0), (2,1), (2,2), (0,0), \\ (0,1), (0,2), (2,0), (2,1), (2,2) \end{pmatrix} = 0.10$$

BBA for m4:
The Attack Possibility variable, AP, is the accumulation of evidence that the target is likely to act in a hostile manner and in this model, has related parameters such as, Target Platform Type (TPT), Zone Hostility (ZH) and Target Behaviour (TBVR). AP has a simple, linear, nodal relationship with {TPT, ZH, TBVR} according to the rule:

AP = TBVR + ZH

$$\Theta_{D_1} = \{0,1,2,\ldots,7\} \quad \Theta_{D_3} = \{0,1,2,\ldots,5\} \quad \Theta_{D_2} = \{PCE, HOS, WAR\}$$

or: $$\Theta_{D_1} = \{0,1,2,\ldots,7\} \quad \Theta_{D_3} = \{0,1,2,\ldots,5\} \quad \Theta_{D_2} = \{0,1,2\}$$

$$m_2^{D_1 \cup D_2 \cup D_3}(ap, tbvr, zh) = 1.0$$

$$m_4^{D_1 \cup D_2 \cup D_3}\left(\begin{array}{c} (0,0,0),(1,0,1),(2,0,2),(3,0,3),(4,0,4),(5,0,5), \\ (1,1,0),(2,1,1),(3,1,2),(4,1,3),(5,1,4),(6,1,5), \\ \ldots \\ (ap, tbvr, zh) \\ \ldots \\ (7,7,0),(8,7,1),(9,7,2),(10,7,3),(11,7,4),(12,7,5) \end{array}\right) = 1.00$$

where: *ap = tbvr + zh*

The BBA m3 is defined according to this rule on the product space, *AP x TBVR x ZH*.

It could be reasonably argued that the AP BBA is also dependent on the target platform type (i.e. TPT). However, this variable is included as one of the variables used to describe the Threat Capability, so it is unnecessary to include it twice. Of more significance is the sensitivity of the model to the mass associated with the TPT's BBA.

BBA for m5:
The fifth BBA is the accumulation of evidence based on the relationship between the Friendly Fire (FF), adverse Weather conditions (WTHR) and Firing Constraints (FC) variables and exists on the {FF, WTHR, FC} domain. FC has a nodal relationship with FF and WTHR according to the simple implication rule:

FC = FF + WTHR

$$\Theta_{D_1} = \{0,1,2,3\} \quad \Theta_{D_2} = \{T, F\} \quad \Theta_{D_3} = \{EXTM, MOD, CALM\}$$

or: $$\Theta_{D_1} = \{0,1,2,3\} \quad \Theta_{D_2} = \{0,1\} \quad \Theta_{D_3} = \{1,2,3\}$$

$$m_2^{D_1 \cup D_2 \cup D_3}(fc, ff, wthr) = 1.0$$

$$m_5^{D_1 \cup D_2 \cup D_3}\begin{pmatrix} (0,0,0),(1,0,1),(1,1,0) \\ \dots \\ (fc,ff,wthr) \\ \dots \\ ((2,1,1),(3,1,2),(4,1,3) \end{pmatrix} = 1.00$$

where: $fc = ff + wthr$

The BBA m_5 is defined according to this rule on the product space, *FC x FF x WTHR*. This is a highly idealised rule which would be further improved by weighting the FF and WTHR to represent their relative influence on the FC parameter.

BBA for m_6:

The sixth BBA is based on the relationship between the Target (to defended asset) Range (TR) and TWER variables and exists on the {TR, TWER} domain. TWER has a nodal relationship with TR according to the definitions and rule:

Ranges used for TWER:

FAR:	Outside optimal engagement range: > x_1 km
MED:	Within optimal engagement range: < x_1 km
SHORT:	Short engagement range: < x_2 km (i.e. $x_2 < x_1$)

Rule 1: *We are 95% confident that if the target's range is > x_1 km of the defended asset (i.e. TR=0), then the target is in a sub-optimal weapon engagement range (i.e. TWER = 1). That is if TR=0 then TWER=1 with at least 95% confidence.*

Rule 2: *Conversely, we are 90% confident that if the target is within range (i.e. < x_2 km) of the defended asset (i.e. $TR \in \{1,2\}$), then the target is within the threat's WER (i.e. $TWER \in \{2,3\}$). That is, the target is in an optimal weapon engagement range. That is if TR= 1 or 2, TWER = 2 or 3 with at least 90% confidence.*

The BBA m_6 is defined according to these rules on the product space, *TR x TWER*.

Rule 1: *That is if TR=0 then TWER=1 with at least 95% confidence.*

$$m_6^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup (\bar{A} \times \Theta_{D_2}) \\ 1-\alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$$m_6^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (tr \times twer) \cup (\overline{tr} \times \Theta_{D_2}) \\ 1-\alpha & C = (tr, \overline{tr}) \times (twer, \overline{twer}) \end{cases}$$

$$\Theta_{D_1} = \{FAR, MED, SHRT\} \qquad \Theta_{D_2} = \{POOR, MOD, OPT\}$$

Or: $\Theta_{D_1} = \{0,1,2\}$ $\qquad \Theta_{D_2} = \{1,2,3\}$

$$\Theta_{D_1} = \{twer, \overline{twer}\} \qquad \Theta_{D_2} = \{tr, \overline{tr}\}$$

In this case: *tr* = {0} $\overline{tr}$ = {1, 2}

And: *twer* = {1} $\overline{twer}$= {2, 3}

$$m_6^{D_1 \cup D_2}(C) = \alpha \qquad C = (tr \times twer) \cup \left(\overline{tr} \times \Theta_{D_2}\right)$$
$$m_6^{D_1 \cup D_2}(C) = 0.95 \qquad C = (tr \times twer) \cup \left(\overline{tr} \times (twer, \overline{twer})\right)$$
$$m_6^{D_1 \cup D_2}\left((tr, twer), (\overline{tr}, twer), (\overline{tr}, \overline{twer})\right) = 0.95$$

So:

$(tr, twer)$ = {(0, 1)}
$(\overline{tr}, twer)$ = {(1, 1), (2, 1)}
$(tr, \overline{twer})$ = {(0, 2), (0, 3)}
$(\overline{tr}, \overline{twer})$ = {(1, 2), (1, 3), (2, 2), (2, 3)}

$$m_6^{D_1 \cup D_2}\left((0,1), (1,1), (2,1), (1,2), (1,3), (2,2), (2,3)\right) = 0.95$$

And:

$$m_6^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$$
$$m_6^{D_1 \cup D_2}(C) = 0.05 \quad C = (tr, \overline{tr}) \times (twer, \overline{twer})$$

$$m_6^{D_1 \cup D_2}\left((tr, twer), (\overline{tr}, twer), (tr, \overline{twer}), (\overline{tr}, \overline{twer})\right) = 0.05$$

$$m_6^{D_1 \cup D_2}\left((0,1), (1,1), (2,1), (0,2), (0,3), (1,2), (1,3), (2,2), (2,3)\right) = 0.05$$

Rule 2: *That is if TR= 1 or 2, TWER = 2 or 3 with at least 90% confidence.*

$\Theta_{D_1} = \{FAR, MED, SHRT\}$ $\Theta_{D_2} = \{POOR, MOD, OPT\}$

Or: $\Theta_{D_1} = \{0, 1, 2\}$ $\Theta_{D_2} = \{1, 2, 3\}$

$\Theta_{D_1} = \{twer, \overline{twer}\}$ $\Theta_{D_2} = \{tr, \overline{tr}\}$

In this case: *tr* = {1, 2} $\overline{tr}$ = {0}

And: *twer* = {2, 3} $\overline{twer}$= {1}

$$m_6^{D_1 \cup D_2}(C) = \alpha \qquad C = (tr \times twer) \cup \left(\overline{tr} \times \Theta_{D_2}\right)$$
$$m_6^{D_1 \cup D_2}(C) = 0.90 \qquad C = (tr \times twer) \cup \left(\overline{tr} \times (twer, \overline{twer})\right)$$
$$m_6^{D_1 \cup D_2}\left((tr, twer), (\overline{tr}, twer), (\overline{tr}, \overline{twer})\right) = 0.90$$

So:

$(tr, twer)$ = {(1, 2), (1, 3), (2, 2), (2, 3)}
$(\overline{tr}, twer)$ = {(0, 2), (0, 3)}
$(tr, \overline{twer})$ = {(1, 1), (2, 1)}
$(\overline{tr}, \overline{twer})$ = {(0, 1)}

$$m_6^{D_1 \cup D_2}\left((1,2), (1,3), (2,2), (2,3), (0,2), (0,3), (0,1)\right) = 0.90$$

And:

$$m_6^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$$
$$m_6^{D_1 \cup D_2}(C) = 0.10 \quad C = (tr, \overline{tr}) \times (twer, \overline{twer})$$

$$m_6^{D_1 \cup D_2}\big((tr, twer), (\overline{tr}, twer), (tr, \overline{twer}), (\overline{tr}, \overline{twer})\big) = 0.10$$

$$m_6^{D_1 \cup D_2}\big((1,2), (1,3), (2,2), (2,3), (0,2), (0,3), (1,1), (2,1), (0,1)\big) = 0.10$$

BBA for m7:

The seventh BBA is based on the Target Platform Type (TPT) and the target's Weapon Engagement Range (TWER) variables. Based on *a priori* knowledge, TWER has a nodal relationship to TPT according to the following rules:

> ***Rule 1:*** *If the target is a commercial vessel or similar (i.e. TPT = 0), then its WER is non-existent (i.e. TWER = 0) with confidence in each case between 50 and 100%.*
> ***Rule 2:*** *If the target is one of two platform types (i.e. TPT* $\in$ {1,2}*), then then its WER is medium (i.e. TWER = 1) with confidence in each case between 50 and 100%.*
> ***Rule 3:*** *If the target is one of the third platform type (i.e. TPT = 3) then then its WER is high (i.e. TWER = 2) with confidence in each case between 50 and 100%.*

The BBA m7 is defined on the product space, *TPT x TWER.*

> ***Rule 1:*** *If TPT = 0 then TWER = 0 with confidence > 50%.*

$$m_7^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ 1-\alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$$m_7^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (tpt \times twer) \cup \left(\overline{tpt} \times \Theta_{D_2}\right) \\ 1-\alpha & C = (tpt, \overline{tpt}) \times (twer, \overline{twer}) \end{cases}$$

$\Theta_{D_1} = \{0,1,2,3\}$ $\Theta_{D_2} = \{NONE, MOD, FULL\}$

Or: $\Theta_{D_1} = \{0,1,2,3\}$ $\Theta_{D_2} = \{0,1,2\}$

$\Theta_{D_1} = \{tpt, \overline{tpt}\}$ $\Theta_{D_2} = \{twer, \overline{twer}\}$

In this case: *tpt* = {0} $\overline{tpt}$ = {1, 2, 3}

And: *twer* = {0} $\overline{twer}$= {1, 2}

$$m_7^{D_1 \cup D_2}(C) = \alpha \quad C = (tpt \times twpn) \cup \left(\overline{tpt} \times \Theta_{D_2}\right)$$
$$m_7^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt \times twpn) \cup \left(\overline{tpt} \times (twpn, \overline{twpn}\,)\right)$$
$$m_7^{D_1 \cup D_2}\big((tpt, twer), (\overline{tpt}, twer), (\overline{tpt}, \overline{twer})\big) = 0.50$$

So:

$(tpt, twer)$ = {(0, 0)}
$(\overline{tpt}, twer)$ = {(1, 0), (2, 0), (3, 0)}
$(tpt, \overline{twer})$ = {(0, 1), (0, 2)}
$(\overline{tpt}, \overline{twer})$ = {(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2)}

$$m_7^{D_1 \cup D_2}\begin{pmatrix}(0,0), (1,0), (2,0), (3,0), (1,1), \\ (1,2), (2,1), (2,2), (3,1), (3,2)\end{pmatrix} = 0.50$$

And: $m_7^{D_1 \cup D_2}(C) = 1-\alpha \quad C = \Theta_{D_1 \cup D_2}$

$$m_7^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt, \overline{tpt}) \times (twpn, \overline{twpn})$$

$$m_7^{D_1 \cup D_2}\big((tpt, twpn), (\overline{tpt}, twpn), (tpt, \overline{twer}), (\overline{tpt}, \overline{twer})\big) = 0.50$$

$$m_7^{D_1 \cup D_2}\begin{pmatrix}(0,0),(1,0),(2,0),(3,0),(1,1),(0,1),\\(0,2),(1,2),(2,1),(2,2),(3,1),(3,2)\end{pmatrix} = 0.50$$

Rule 2: *If TPT = 1 or 2 then TWER = 1 with confidence > 50%.*

$$m_7^{D_1 \cup D_2}(C) = \begin{cases}\alpha & C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right)\\ 1-\alpha & C = \Theta_{D_1 \cup D_2}\end{cases}$$

$$m_7^{D_1 \cup D_2}(C) = \begin{cases}\alpha & C = (tpt \times twer) \cup \left(\overline{tpt} \times \Theta_{D_2}\right)\\ 1-\alpha & C = (tpt, \overline{tpt}) \times (twer, \overline{twer})\end{cases}$$

$\Theta_{D_1} = \{0, 1, 2, 3\}$ $\qquad$ $\Theta_{D_2} = \{NONE, MOD, FULL\}$

Or: $\Theta_{D_1} = \{0, 1, 2, 3\}$ $\qquad$ $\Theta_{D_2} = \{0, 1, 2\}$

$\Theta_{D_1} = \{tpt, \overline{tpt}\}$ $\qquad$ $\Theta_{D_2} = \{twer, \overline{twer}\}$

In this case: *tpt* = {1, 2} $\qquad$ $\overline{tpt}$ = {0, 3}

And: *twer* = {1} $\qquad$ $\overline{twer}$= {0, 2}

$$m_7^{D_1 \cup D_2}(C) = \alpha \quad C = (tpt \times twer) \cup \left(\overline{tpt} \times \Theta_{D_2}\right)$$
$$m_7^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt \times twer) \cup \left(\overline{tpt} \times (twer, \overline{twer}\ )\right)$$
$$m_7^{D_1 \cup D_2}\big((tpt, twer), (\overline{tpt}, twer), (\overline{tpt}, \overline{twer})\big) = 0.50$$

So:

$(tpt, twer)$ = {(1, 1), (2, 1)}

$(\overline{tpt}, twer)$ = {(0, 1), (3, 1)}

$(tpt, \overline{twer})$ = {(1, 0), (1, 2), (2, 0), (2, 2)}

$(\overline{tpt}, \overline{twer})$ = {(0, 0), (0, 2), (3, 0), (3, 2)}

$$m_7^{D_1 \cup D_2}\begin{pmatrix}(1,1),(2,1),(0,1),(3,1),\\(0,0),(0,2),(3,0),(3,2)\end{pmatrix} = 0.50$$

And:

$$m_7^{D_1 \cup D_2}(C) = 1-\alpha \quad C = \Theta_{D_1 \cup D_2}$$
$$m_7^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt, \overline{tpt}) \times (twer, \overline{twer})$$

$$m_7^{D_1 \cup D_2}\big((tpt, twer), (\overline{tpt}, twer), (tpt, \overline{twer}), (\overline{tpt}, \overline{twer})\big) = 0.50$$

$$m_7^{D_1 \cup D_2}\begin{pmatrix}(1,1),(2,1),(0,1),(3,1),\\(1,0),(1,2),(2,0),(2,2),\\(0,0),(0,2),(3,0),(3,2)\end{pmatrix} = 0.50$$

Rule 3: *If TPT = 3 then TWER = 2 with confidence > 50%.*

$$m_7^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ 1 - \alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$$m_7^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (tpt \times twer) \cup \left(\overline{tpt} \times \Theta_{D_2}\right) \\ 1 - \alpha & C = (tpt, \overline{tpt}) \times (twer, \overline{twer}) \end{cases}$$

$\Theta_{D_1} = \{0, 1, 2, 3\}$ $\Theta_{D_2} = \{NONE, MOD, FULL\}$

Or: $\Theta_{D_1} = \{0, 1, 2, 3\}$ $\Theta_{D_2} = \{0, 1, 2\}$

$\Theta_{D_1} = \{tpt, \overline{tpt}\}$ $\Theta_{D_2} = \{twer, \overline{twer}\}$

In this case: *tpt* = {3} $\overline{tpt}$ = {0, 1, 2}

And: *twer* = {2} $\overline{twer}$= {0, 1}

$$m_7^{D_1 \cup D_2}(C) = \alpha \quad C = (tpt \times twer) \cup \left(\overline{tpt} \times \Theta_{D_2}\right)$$

$$m_7^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt \times twer) \cup \left(\overline{tpt} \times (twer, \overline{twer}\ )\right)$$

$$m_7^{D_1 \cup D_2}\left((tpt, twer), (\overline{tpt}, twer), (\overline{tpt}, \overline{twer})\right) = 0.50$$

So:

$(tpt, twer)$ = {(3, 2)}

$(\overline{tpt}, twer)$ = {(0, 2), (1, 2), (2, 2)}

$(tpt, \overline{twer})$ = {(3, 0), (3, 1), (3, 2)}

$(\overline{tpt}, \overline{twer})$ = {(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1)}

$$m_7^{D_1 \cup D_2}\begin{pmatrix} (3,2), (0,2), (1,2), (2,2), (0,0), \\ (0,1), (1,0), (1,1), (2,0), (2,1) \end{pmatrix} = 0.50$$

And: $m_7^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$

$$m_7^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt, \overline{tpt}) \times (twer, \overline{twer})$$

$$m_7^{D_1 \cup D_2}\left((tpt, twer), (\overline{tpt}, twer), (tpt, \overline{twer}), (\overline{tpt}, \overline{twer})\right) = 0.50$$

$$m_7^{D_1 \cup D_2}\begin{pmatrix} 3,2), (0,2), (1,2), (2,2), (3,0), \\ (3,1), (3,2), (0,0), (0,1), (1,0), \\ (1,1), (2,0), (2,1) \end{pmatrix} = 0.50$$

BBA m8:

The eighth BBA is based on the Target Platform Type (TPT) and the target's Weaponry (TWPN) variables. Based on *a priori* knowledge, TWPN has a nodal relationship to TPT according to the following rules:

Rule 1: If the target is a commercial vessel or similar (i.e. TPT = 0), then its Weaponry is non-existent (i.e. TWPN = 0) with confidence in each case between 50 and 100%.

Rule 2: If the target is one of two platform types (i.e. TPT $\in$ {1,2}), then then its Weaponry is medium (i.e. TWPN = 1) with confidence in each case between 50 and 100%.

Rule 3: If the target is one of the third platform type (i.e. TPT = 3) then then its Weaponry is high (i.e. TWPN = 2) with confidence in each case between 50 and 100%.

The BBA m$_8$ is defined on the product space, *TPT x TWPN.*

Rule 1: *If TPT = 0 then TWPN = 0 with confidence > 50%.*

$$m_8^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup (\bar{A} \times \Theta_{D_2}) \\ 1-\alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$$m_8^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (tpt \times twpn) \cup (\overline{tpt} \times \Theta_{D_2}) \\ 1-\alpha & C = (tpt, \overline{tpt}) \times (twpn, \overline{twpn}) \end{cases}$$

$\Theta_{D_1} = \{0, 1, 2, 3\}$ $\Theta_{D_2} = \{NONE, MOD, FULL\}$

Or: $\Theta_{D_1} = \{0, 1, 2, 3\}$ $\Theta_{D_2} = \{0, 1, 2\}$

$\Theta_{D_1} = \{tpt, \overline{tpt}\}$ $\Theta_{D_2} = \{twpn, \overline{twpn}\}$

In this case:	*tpt* = {0}	$\overline{tpt}$ = {1, 2, 3}
And:	*twpn* = {0}	$\overline{twpn}$= {1, 2}

$$m_8^{D_1 \cup D_2}(C) = \alpha \quad C = (tpt \times twpn) \cup (\overline{tpt} \times \Theta_{D_2})$$

$$m_8^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt \times twpn) \cup (\overline{tpt} \times (twpn, \overline{twpn}\,))$$

$$m_8^{D_1 \cup D_2}((tpt, twpn), (\overline{tpt}, twpn), (\overline{tpt}, \overline{twpn})) = 0.50$$

So:

$(tpt, twpn)$ = {(0, 0)}
$(\overline{tpt}, twpn)$ = {(1, 0), (2, 0), (3, 0)}
$(tpt, \overline{twpn})$ = {(0, 1), (0, 2)}
$(\overline{tpt}, \overline{twpn})$ = {(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2)}

$$m_7^{D_1 \cup D_2}\begin{pmatrix}(0,0), (1,0), (2,0), (3,0), (1,1), \\ (1,2), (2,1), (2,2), (3,1), (3,2)\end{pmatrix} = 0.50$$

And:

$$m_8^{D_1 \cup D_2}(C) = 1-\alpha \quad C = \Theta_{D_1 \cup D_2}$$

$$m_8^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt, \overline{tpt}) \times (twpn, \overline{twpn})$$

$$m_8^{D_1 \cup D_2}((tpt, twpn), (\overline{tpt}, twpn), (tpt, \overline{twpn}), (\overline{tpt}, \overline{twpn})) = 0.50$$

$$m_8^{D_1 \cup D_2}\begin{pmatrix}(0,0), (1,0), (2,0), (3,0), (1,1), (0,1), \\ (0,2), (1,2), (2,1), (2,2), (3,1), (3,2)\end{pmatrix} = 0.50$$

Rule 2: *If TPT = 1 or 2 then TWPN = 1 with confidence > 50%.*

$$m_8^{D_1 \cup D_2}(C) = \begin{cases} \alpha \quad C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ \ 1 - \alpha \quad C = \Theta_{D_1 \cup D_2} \end{cases}$$

$$m_8^{D_1 \cup D_2}(C) = \begin{cases} \quad \alpha \quad C = (tpt \times twpn) \cup \left(\overline{tpt} \times \Theta_{D_2}\right) \\ 1 - \alpha \quad C = (tpt, \overline{tpt}) \times (twpn, \overline{twpn}) \end{cases}$$

$\Theta_{D_1} = \{0, 1, 2, 3\}$ $\Theta_{D_2} = \{NONE, MOD, FULL\}$

Or: $\Theta_{D_1} = \{0, 1, 2, 3\}$ $\Theta_{D_2} = \{0, 1, 2\}$

$\Theta_{D_1} = \{tpt, \overline{tpt}\}$ $\Theta_{D_2} = \{twpn, \overline{twpn}\}$

In this case: *tpt* = {1, 2} $\overline{tpt}$ = {0, 3}

And: *twpn* = {1} $\overline{twpn}$= {0, 2}

$$m_8^{D_1 \cup D_2}(C) = \alpha \quad C = (tpt \times twpn) \cup \left(\overline{tpt} \times \Theta_{D_2}\right)$$
$$m_8^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt \times twpn) \cup \left(\overline{tpt} \times (twpn, \overline{twpn}\,)\right)$$
$$m_8^{D_1 \cup D_2}\left((tpt, twpn), (\overline{tpt}, twpn), (\overline{tpt}, \overline{twpn})\right) = 0.50$$

So:

$(tpt, twpn)$ = {(1, 1), (2, 1)}
$(\overline{tpt}, twpn)$ = {(0, 1), (3, 1)}
$(tpt, \overline{twpn})$ = {(1, 0), (1, 2), (2, 0), (2, 2)}
$(\overline{tpt}, \overline{twpn})$ = {(0, 0), (0, 2), (3, 0), (3, 2)}

$$m_7^{D_1 \cup D_2}\begin{pmatrix}(1,1),(2,1),(0,1),(3,1),\\(0,0),(0,2),(3,0),(3,2)\end{pmatrix} = 0.50$$

And: $m_8^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$

$$m_8^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt, \overline{tpt}) \times (twpn, \overline{twpn})$$

$$m_8^{D_1 \cup D_2}\left((tpt, twpn), (\overline{tpt}, twpn), (tpt, \overline{twpn}), (\overline{tpt}, \overline{twpn})\right) = 0.50$$

$$m_8^{D_1 \cup D_2}\begin{pmatrix}(1,1),(2,1),(0,1),(3,1),\\(1,0),(1,2),(2,0),(2,2),\\(0,0),(0,2),(3,0),(3,2)\end{pmatrix} = 0.50$$

Rule 3: *If TPT = 3 then TWPN = 2 with confidence > 50%.*

$$m_8^{D_1 \cup D_2}(C) = \begin{cases} \alpha \quad C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ \ 1 - \alpha \quad C = \Theta_{D_1 \cup D_2} \end{cases}$$

$$m_8^{D_1 \cup D_2}(C) = \begin{cases} \quad \alpha \quad C = (tpt \times twpn) \cup \left(\overline{tpt} \times \Theta_{D_2}\right) \\ 1 - \alpha \quad C = (tpt, \overline{tpt}) \times (twpn, \overline{twpn}) \end{cases}$$

$\Theta_{D_1} = \{0, 1, 2, 3\}$ $\Theta_{D_2} = \{NONE, MOD, FULL\}$

Or: $\Theta_{D_1} = \{0, 1, 2, 3\}$ $\Theta_{D_2} = \{0, 1, 2\}$

	$\Theta_{D_1} = \{tpt, \overline{tpt}\}$	$\Theta_{D_2} = \{twpn, \overline{twpn}\}$
In this case:	*tpt* = {3}	$\overline{tpt}$ = {0, 1, 2}
And:	*twpn* = {2}	$\overline{twpn}$= {0, 1}

$$m_8^{D_1 \cup D_2}(C) = \alpha \qquad C = (tpt \times twpn) \cup \left(\overline{tpt} \times \Theta_{D_2}\right)$$
$$m_{87}^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt \times twpn) \cup \left(\overline{tpt} \times (twpn, \overline{twpn}\,)\right)$$
$$m_8^{D_1 \cup D_2}\left((tpt, twpn), (\overline{tpt}, twpn), (\overline{tpt}, \overline{twpn})\right) = 0.50$$

So:

$(tpt, twpn)$ = {(3, 2)}
$(\overline{tpt}, twpn)$ = {(0, 2), (1, 2), (2, 2)}
$(tpt, \overline{twpn})$ = {(3, 0), (3, 1), (3, 2)}
$(\overline{tpt}, \overline{twpn})$ = {(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1)}

$$m_8^{D_1 \cup D_2}\begin{pmatrix}(3,2),(0,2),(1,2),(2,2),(0,0),\\(0,1),(1,0),(1,1),(2,0),(2,1)\end{pmatrix} = 0.50$$

And: $m_8^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$

$$m_8^{D_1 \cup D_2}(C) = 0.50 \quad C = (tpt, \overline{tpt}) \times (twpn, \overline{twpn})$$

$$m_8^{D_1 \cup D_2}\left((tpt, twpn), (\overline{tpt}, twpn), (tpt, \overline{twpn}), (\overline{tpt}, \overline{twpn})\right) = 0.50$$

$$m_8^{D_1 \cup D_2}\left(\begin{matrix}3,2),(0,2),(1,2),(2,2),(3,0),\\(3,1),(3,2),(0,0),(0,1),(1,0),\\(1,1),(2,0),(2,1)\end{matrix}\right) = 0.50$$

BBA m9:

The ninth BBA relates the Target Behaviour (TBVR) to four parameters; those being whether the target is employing countermeasures (CM), whether the target has its FCR switched on (FCR), whether the target has responded correctly to an IFF squawk (IFFS) and whether the manoeuvring behaviour of the target (MNV) is suspect according to its known or predicted behaviour as a non-hostile vessel. TBVR has a linear, nodal relationship with {CM, FCR, IFFS, MNV} according to the rule:

TBVR = CM + 2*FCR + IFFS + MNV

$$\Theta_{D_1} = \{0,1,2,\ldots,5\} \quad \Theta_{D_2} = \{T,F\} \qquad \Theta_{D_3} = \{ON, OFF\}$$
$$\Theta_{D_1} = \{0,1,2,\ldots,5\} \quad \Theta_{D_2} = \{1,0\} \qquad \Theta_{D_3} = \{1,0\}$$

$$\Theta_{D_4} = \{T,F\} \qquad \Theta_{D_5} = \{T,F\}$$
$$\Theta_{D_4} = \{0,1\} \qquad \Theta_{D_5} = \{1,0\}$$

$$m_9^{D_1 \cup D_2 \cup D_3 \cup D_4 \cup D_5}(tbvr, cm, fcr, iffs, mnv) = 1.0$$

where: *tbvr = cm + 2*fcr + iffs + mnv*

$$m_9^{D_1 \cup D_2 \cup D_3 \cup D_4 \cup D_5}\begin{pmatrix}(0,0,0,0,0),(1,0,0,0,1),(1,0,0,1,0),(1,0,0,1,1),\\(2,0,1,0,0),(3,0,1,0,1),(3,0,1,1,0),(4,0,1,1,1),\\\dots\\(3,1,1,0,0),(4,1,1,0,1),(4,1,1,1,0),(5,1,1,1,1),\end{pmatrix} = 1.00$$

The BBA m_9 is defined on the product space, *TBVR x CM x FCR x IFFS x MNV*

5.3.2 Leaf Nodes

Whereas BBA's m_1 to m_9 represent the relationships between intermediate BBA's, BBA's m_{10} to m_{18} represent the most current organic input data available for the ZH, FF, WTHR, RAN, TPT, CM, FCR, IFFS and MNV leaf node variables. It cannot be assumed that there is specific data for each leaf node BBA. In such cases, these BBA's are set to indicate ignorance. Possible values for the BBA's associated with the leaf nodes (nodes 9 to 16) are listed in Table 5-2.

Table 5-2 Parameters, node types and frames, used to generate the new threat model Evidential Network.

Parameter	Symbol	NODE TYPE	Frame	Frame
1	TP	Variable of interest (i.e. D_0^*)	{0, 1,…10}	{0, 1,…10}
2	AP	INTERMEDIATE	{0, 1, … 7}	{0, 1, … 7}
3	TC		{0, 1… 4}	{0, 1… 4}
4	FC		{0, 1, 2, 3}	{0, 1, 2, 3}
5	TWER		{SHRT, MED, LR}	{1, 2, 3}
6	TWPN		{NONE, MOD, FULL}	{0, 1, 2}
7	TBVR		{0, 1, … 5}	{0, 1, … 5}
8	ZH		{PCE, HOS, WAR}	{0, 1, 2}
9	FF		{T, F}	{1, 0}
10	WTHR	LEAF	{EXTM, MOD, CALM}	{1, 2, 3}
11	TR		{0, 1, 2, 3}	{0, 1, 2, 3}
12	TPT		{0, 1, 2, 3}	{0, 1, 2, 3}
13	CM		{T, F}	{1, 0}
14	FCR		{ON, OFF}	{1, 0}
15	IFFS		{T, F}	{0, 1}
16	MNV		{T, F}	{1, 0}

D_0^* is domain of interest: {TP}.

5.4 BJT

A BJT was calculated using the MATLAB Evidential Network software for the new threat model using the method described in Section 4.2 and is shown in Figure 5-2. This model uses the elimination sequence based on the OSLA-SC FFS heuristic (refer Section 4.2.1):

CM, FCR, IFFS, MNV, TR, TPT, FF, WTHR, ZH, TBVR, FC, TWER, TWPN, AP, TC

5.5 Analysis Using New Threat Evaluation Model

The new threat evaluation model has been presented in this report for appraisal purposes only. It is intended that detailed analyses of this model will be undertaken and presented at a later stage. Prior to further model analysis occurring, some rigorous testing and development of the MATLAB Evidential Network software is required to verify the code's output.

For the purposes of this report, an example input data file was manually created (i.e. as opposed to being entered via prompts into the MATLAB code) as a separate MATLAB routine for the new threat evaluation model. It was considered that this was a method less prone to possible bugs in the supplied MATLAB code. Furthermore, the code does not have a user friendly GUI for data entry purposes. The input data, including variable and frame definitions, BBA and focal set descriptions for each BBA was coded into a MATLAB routine (amounting to over 1000 lines of code).

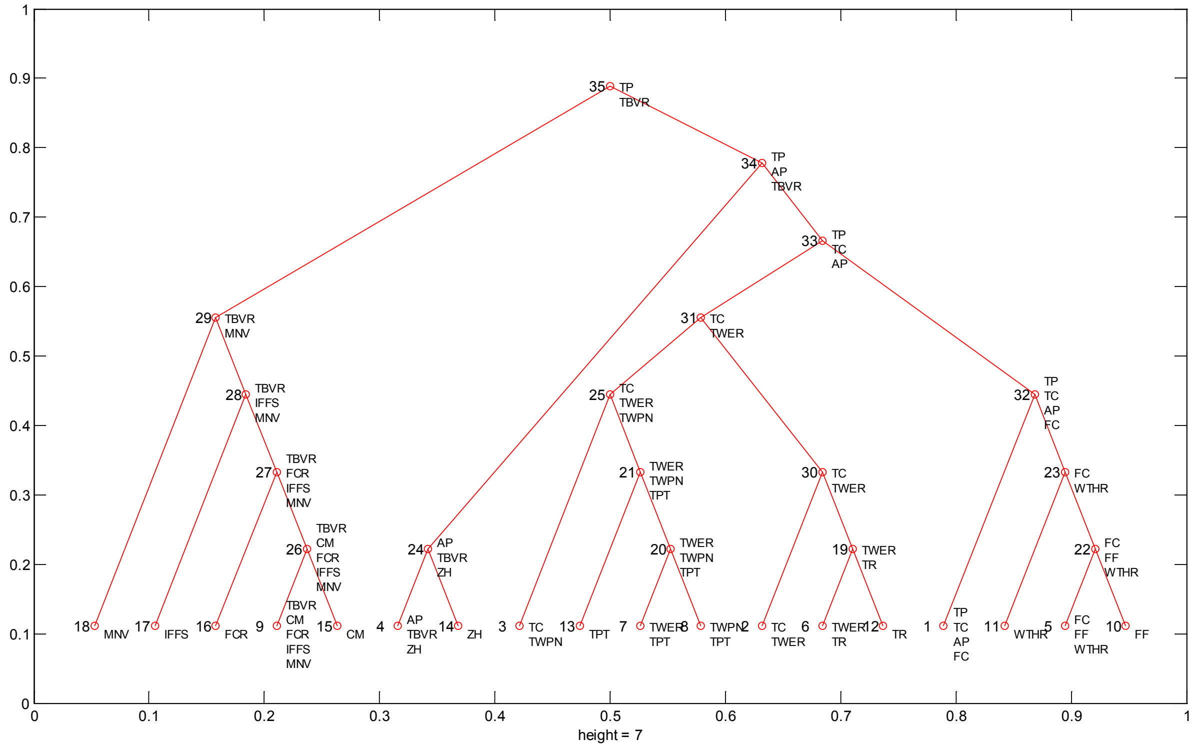


Figure 5-2 The BJT for the new threat evaluation model produced using the MATLAB Evidential Network software. The numbers at each BBA point on the BJT diagram can be cross-referenced with the BBA's shown in Figure 5-1.

Table 5-3 Leaf node values entered for the example analysis using new threat model.

BBA #	Related Node	BBA: Frame	BBA: Value
10	FF	{T, F}	{T}
11	WTHR	{XTRM, MOD, CALM}	{MOD}
12	TR	{0, 1, 2, 3}	{3, 4}
13	TPT	{0, 1, 2, 3}	{2, 3}
14	ZH	{PCE, HOS, WAR}	{PCE}
15	CM	{T, F}	{F}
16	FCR	{ON, OFF}	{ON}
17	IFFS	{T, F}	{F}
18	MNV	{T, F}	{F}

The output included the BJT shown in Figure 5-2 and the Probability v's Threat Level (TL) bar graph presented in Figure 5-3. The BBAs were converted to probabilities by the MATLAB programme using the pignistic transformation formula shown in Section 3.6, generating the resultant probability v's TL distribution shown in Figure 5-3. It should be noted that nothing in particular should be inferred from these results until code validation is performed. They are merely a demonstration of the type of data entry used and output generated.

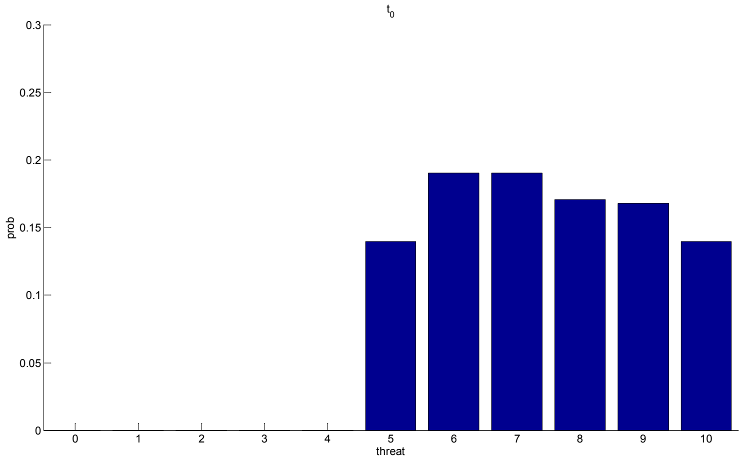


Figure 5-3 Pignistic probabilities for the new threat model produced using the MATLAB Evidential Network software. The data entered produces TL probabilities spread around TL 5 to 10, with more weighting towards TL 6 and 7.

6. Conclusion

6.1 Review

The significance of the choice of methodology for threat prioritisation cannot be underestimated. It is clearly of paramount significance in a combat situation where decision-making time is measured in seconds or less and sub-optimal choices can have dire consequences.

As stated in Section 1.3, the work presented in this report was done as part of the author's project area objective to develop an automated decision aid tool for Threat Evaluation. RBAs were briefly introduced followed by a comparison of the Bayesian Network and Evidential Network techniques, testing and evaluation of Evidential Network algorithms, as well as the development of an AWW threat model. The threat model would be used to prioritise targets in an optimal manner based on all relevant and available parameters so as to minimise the threat level to the defended asset, typically a maritime platform.

The principal difference between Bayesian Network and Evidential Network techniques is that BBA's or masses are used to represent beliefs in events as opposed to probabilities where the masses represent the degree of belief in a proposition. Masses can also be assigned to a subset of events, rather than just a single event. In other words, one's level of knowledge may be that a target has been identified and it is one of three aircraft types, but we do not have additional information to confirm which type. In this way, an Evidential Network is able to simulate levels of ignorance in one's situational awareness, whereas a Bayesian Network cannot.

Whereas in classical probability theory, probabilities between 0 and 1 are assigned to events, weighted masses are employed in DST. The masses are not probabilities, but weightings given to an event or subset of events.

Deterministic methods were compared to stochastic methods for 'if-then' implication rules used in Evidential Network Theory. Situational awareness, whether in combat scenarios, weather forecasting or any other rules of human or environmental behaviour are more closely reflected by stochastic rules that incorporate levels of uncertainty. The methodology presented for describing uncertainty in implication rules can be either a simplistic 'if-then' deterministic or a more realistic 'if- then *probably*' stochastic approach.

In short, Evidential Network methods provide a more accurate representation of knowledge, or beliefs associated with situational awareness, which can be used to prioritise threats. In comparison, Bayesian Networks are particularly limited in their ability to represent situational awareness with any fidelity.

The Evidential Network methodology developed by Benavoli et al, including Dempster-Shafer Theory, uncertainty in implication rules and the application of heuristics for dynamic threat assessment techniques, such as binary join trees, allow for rapid reassessment of threat prioritisation when input parameters change. Rather than recalculating the total joint valuation of an Evidential Network, local computations can be used to calculate branches of an Evidential Network that are affected by updated input parameters, such as sensor data.

Following the detailed analysis of the reference threat model for the air domain, a new threat model for AWW was produced by the author after some consultation with Navy SMEs. This model should be considered as a prototype for continued developed rather than a final offering. It is similar in many aspects to the air domain model, with some exceptions. The Hostile Intent nodal parameter is replaced in the AWW model by Attack Possibility for reasons discussed earlier. This model also proved useful in testing and debugging the provided MATLAB Evidential Network code which has not reportedly been tested beyond the original air domain modelling work.

6.2 Future Work

The new threat model presented in this report will require ongoing refinement, both of the model itself and the simple parameter relationships used. This threat model was designed primarily for AWW combat scenarios, whereas the reference threat model was primarily concerned with air combat.

The mathematical procedure used to develop the AWW Threat Model was drawn from the PhD thesis of Benavoli [6]. The MATLAB Evidential Network software was used in this report to reproduce analyses of the reference threat model and subsequently, to evaluate the AWW-specific threat model generated by the author. That said, some caution should be taken with respect to results generated since there no rigorous testing of the software has been undertaken by this author, although the original documents referenced in this report provide some confidence.

It is also apparent that the MATLAB Evidential Network software, which was gratefully received by the author from one of the co-authors of the original analysis [1], was most likely never intended for use by others. It is evident that the author is probably the first to utilise the software since the original work was undertaken. Regrettably, there are no user manuals or notes, or a user-friendly user-interface. It took the author considerable time to identify and in some cases modify, the various MATLAB Evidential Network routines provided. However, as there is no other known AWW threat evaluation software known to the author that uses Evidential Networks and Dempster-Shafer Theory, it is well worthwhile pursuing the development of this software, undertaking further testing and evaluation, and developing a user-friendly GUI.

The MATLAB Evidential Network software's features also require further systematic testing. For example, whereas the AWW threat evaluation model is essentially static, the software has functionality to conduct dynamic analyses, more closely simulating a real-time analysis for threat evaluation scenarios. That is, the analyst can vary input parameters with time over a series of time steps and the model's sensitivity to these changes can be then be assessed. Time restrictions did not permit dynamic analyses for the new AWW threat evaluation model. This would be a worthwhile pursuit in future work.

The presentation of Evidential Network results has generally been through the use of pignistic transformations, i.e. transformation of belief assignments to equivalent probabilities. The choice of method of result presentation also needs further consideration, since probability values may not be the most suitable format for warfighters. Alternatives may include, confidence intervals, or plausibility values (the plausibility value is the sum of all propositions that totally or partially agree with a proposition; i.e. all plausible propositions). The presentation of Evidential Network results would be a suitable area for a human factors discipline to review.

7. Acknowledgements

The author acknowledges the contributions of Dr. Martin Oxenham for reviewing the report, and to Manuel Salazar, who incorporated the reviewer's comments and finalised the report post the departure of the author.

8. References

[1] A. Benavoli, B. Ristic, A. Farina, M. Oxenham and L. Chisci, "An Application of Evidential Networks to Threat Assessment," *Aerospace and Electronic Systems, IEEE Transactions 45(2),* pp. 620-639, 2009.

[2] L. Hammond, "Application of a Dynamic Programming Algorithm for Weapon Target," DST Group, Fishermans Bend, 2016.

[3] F. Rheaume and A. Benaskeur, "Target Engageability Improvement through Adaptive Data Fusion and Sensor Management: An Approach Based on the Fire Control Radar Search to Lock-on time," Defence R&D Canada, Valcartier, 2008.

[4] V. McCabe, "How Missed Details Led to the USS Vincennes Incident," September 2014. [Online]. Available: http://www.utne.com/mind-and-body/uss-vincennes-incident-ze0z1409zcwil.aspx. [Accessed 6 April 2016].

[5] L. Swartz, "Overwhelmed by Technology: How did User Interface Failures on Board the USS Vincennes lead to 290 Dead?," 2001. [Online]. Available: http://xenon.stanford.edu/~lswartz/vincennes.pdf. [Accessed 4 April 2016].

[6] A. Benavoli, "Modelling and Efficient Fusion of Uncertain Information: Beyond the Classical Probability Approach," Universita Degli Studi Di Firenze, Florence, Italy, 2007.

[7] H. Naeem and A. Masood, "An Optimal Dynamic Threat Evaluation and Weapon Scheduling Technique," *Knowledge Based Systems,* pp. 337-342, 4 May 2010.

[8] C. Vandepeer, Rethinking Threat: Intelligence Analysis, Intentions, Capabilities, and the Challenge of Non-State Actors, Adelaide: University of Adelaide, South Aust., 2011.

[9] F. Johansson and G. Falkman, "A Bayesian Network Approach to Threat Evaluation with Application to an Air Defense Scenario," in *11th International Conference on Information Fusion*, Cologne, Germany, 2008.

[10] H. Irandoust, A. Benaskeur, P. Bellefeuille and F. Kabanza, "Distributed Threat Evaluation in Naval Tactical Battle Management," in *Collective C2 in Multinational Civil-Military Operations, 16th ICCRTS*, Quebec City, Quebec, 2011.

[11] A. Nicholson and K. Korb, Bayesian Artificial Intelligence, Melbourne, Australia: Chapman and Hall, 2004.

[12] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping," *The Annals of Mathematical Statistics 38 (2),* p. 325–339, 1967.

[13] G. Shafer, A Mathematical Theory of Evidence, Princeton, New Jersey, USA: Princeton University Press, 1976.

[14] A. Shenoy, "A Valuation-Based Language for Expert Systems," *International Journal of Approximate Reasoning,* vol. 3, no. 5, pp. 383-411, 1989.

[15] P. Shenoy, "Valuation-Based Systems: a Framework for Managing Uncertainty in Expert Systems," in *Fuzzy logic for the management of uncertainty*, New York, USA, John Wiley & Sons, Inc, 1992, pp. 83-104.

[16] P. Shenoy, "Using Dempster-Shafer's Belief_Function Theory in Expert Systems," in *Advances in Dempster-Shafer Theory of Evidence*, New York, USA, John Wiley & Sons,

1994, pp. 395-414.

[17] P. Shenoy, "Binary Join Trees," in *Twelfth Conference on Uncertainty in Artificial Intelligence*, Portland, Oregon, 1996.

[18] L. Meizhu, Q. Zhang and Y. Deng, 6 June 2004. [Online]. Available: arXiv:1406.1697v1 [cs.AI].

[19] S. McKeever, J. Ye, L. Coyle and S. Dobson, "Using Dempster Shafer Theory of Evidence for Situation Inference," in *EuroSSC 2009*, London, UK, 2009.

[20] K. Sentz and S. Ferson, "Combination of Evidence in Dempster-Shafer Theory," Sandia National Laboratories, Binghamton, NY 13902-6000, 2002.

[21] D. Koks and S. Challa, "An Introduction to Bayesian and Dempster-Shafer Data Fusion," Defence Science and Technology Organisation, Edinburgh, SA, 2005.

[22] P. Shenoy, *Binary Join Trees for Computing Marginals in the Shenoy-Shafter Architecture,* Uni of Kansas, Kansas: Ku School of Business , 1997.

[23] A. Benavoli, L. Chisci, B. Ristic and A. Farina, "Modelling Uncertain Implication Rules in Evidence Theory," in *Fusion '08, 11th Intl Conf.*, Cologne, Germany, 2008.

[24] B. Ristic and P. Smets, "Target Identification Using Belief Functions and Implication Rules," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 41, no. 3, pp. 1097-1103, 2005.

[25] H. Xu and P. Smets, "Reasoning in Evidential Networks With Conditional Belief Functions," *International Journal of Approximate Reasoning,* vol. 14, pp. 155-185, 1996.

[26] P. Smets, "Data Fusion in the Transferable Belief Model," in *Information Fusion*, Piscataway, NJ, USA, 2000.

[27] P. Smets and R. Kenes, "The Transferable Belief Model," *Artificial Intelligence,* vol. 66, pp. 191-234, 1994.

[28] N. Lehmann, "Argumentation Systems and Belief Functions," Department of Informatics, University of Fribourg, Fribourg, 2001.

[29] "Expert System," 20 June 2016. [Online]. Available: https://en.wikipedia.org/wiki/Expert_system. [Accessed 6 July 2016].

This page is intentionally blank.

Appendix A BBA Calculations for Reference Threat Model

BBA for m_1:

T is dependent on HI and C through the BBA (valuation) m_1
Relationship between parameters:
Define Rule: T = HI + C
Where variables' frames of reference are:
$t \in \{0, 1, \dots, 10\}$
$hi \in \{0, 1, \dots, 6\}$
$c \in \{0, 1, \dots, 4\}$
Can represent rule: T = HI + C by BBA
$m_1(\{T\}) = 1$

$$m_1\left(\left\{\begin{matrix}(0,0,0),(1,0,1),\dots,(4,0,4),\\ \dots\\ (t,hi,c)\\ \dots\\ (6,6,0),(7,6,1),\dots,(10,6,4)\end{matrix}\right\}\right)=1$$

i.e, 35 (t, hi, c) tuples.

BBA for m_2:

Hostile Intent (HI) is dependent on evidence that the target is behaving in a hostile manner. These include: evasive manoeuvres (EM); countermeasures (CM), fire-control radar (FCR) operation, the broader political climate (PC) and identification as whether or not the target is a friend (NF).
So HI has a relationship with {EM, FCR, CM, PC, NF}
e.g. can use: HI = EM + 2.FCR + CM + PC + NF
Note: weighted FCR higher than the other parameters.
This relationship can be represented by the second BBA: m_2 defined on a 6 dimensional product space: HI X EM X FCR X CM X PC X NF as follows:

$$m_2\left(\left\{\begin{matrix}(0,0,0,0,0,0),(1,0,0,0,0,1),(1,0,0,0,1,0),\dots,(1,1,0,0,1,0)\\ (2,0,0,0,1,1),(2,0,0,1,1,0),(2,0,0,1,0,1),\dots,(2,1,0,1,0,0)\\ \dots\\ (hi,em,fcr,cm,pc,nf)\\ \dots\\ (5,0,1,1,1,1),(5,1,1,1,1,0),(5,1,1,1,0,1),\dots,(6,1,1,1,1,1)\end{matrix}\right\}\right)=1$$

So there are 32 six-tuples for BBA m_2.

BBA for m3:

m3: is defined on the domain {IFFS, NF}. There is different methodology used here as there is uncertainty in the implication rules: For example, *a priori* knowledge that:

Rule 1: *We are 95 to 100% confident that if the IFF squawking (IFF=1) is true, then the target is actually a friend (NF=0). That is if IFFS=1 ($iffs$) then NF=0 (nf) with at least 95% confidence.*

$$m_3^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ 1-\alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$$\alpha = 0.95$$

$$\Theta_{D_1} = \{1, 0\} \qquad \Theta_{D_2} = \{0, 1\}$$

Or: $\Theta_{D_1} = \{iffs, \overline{iffs}\}$ $\qquad$ $\Theta_{D_2} = \{nf, \overline{nf}\}$

$$m_3^{D_1 \cup D_2}(C) = 0.95 \quad C = (iffs \times nf) \cup \left(\overline{iffs} \times \Theta_{D_2}\right)$$
$$m_3^{D_1 \cup D_2}(C) = 0.95 \quad C = (iffs \times nf) \cup \left(\overline{iffs} \times \left(nf, \overline{nf}\,\right)\right)$$
$$m_3^{D_1 \cup D_2}\left((iffs, nf), (\overline{iffs}, nf), (\overline{iffs}, \overline{nf})\right) = 0.95$$

And:
$$m_3^{D_1 \cup D_2}(C) = 1-\alpha \quad C = \Theta_{D_1 \cup D_2}$$
$$m_3^{D_1 \cup D_2}(C) = 0.05 \quad C = \left(iffs, \overline{iffs}\right) \times \left(nf, \overline{nf}\right)$$
$$m_3^{D_1 \cup D_2}\left((iffs, nf), (\overline{iffs}, nf), (iffs, \overline{nf}), (\overline{iffs}, \overline{nf})\right) = 0.05$$

Rule 2: *Conversely, if there is no response to the IFF interrogation (IFFS= 0) then we are only 10 to 30% confident that the target is non-friendly (NF=1). That is if $\overline{iffs}$ then $\overline{nf}$ with $\alpha = 0.1$ and $\beta = 0.3$.*

$$m_3^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ 1-\beta & C = (A \times \bar{B}) \cup \left(\bar{A} \times \Theta_{D_2}\right) \\ \beta-\alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$$m_3^{D_1 \cup D_2}(C) = \begin{cases} 0.1 & C = \left(\overline{iffs} \times nf\right) \cup \left(iffs \times \left(nf, \overline{nf}\right)\right) \\ 1-0.3 & C = \left(\overline{iffs} \times \overline{nf}\right) \cup \left(iffs \times \left(nf, \overline{nf}\right)\right) \\ 0.3-0.1 & C = \left(iffs, \overline{iffs}\right) \times \left(nf, \overline{nf}\right) \end{cases}$$

$$m_3^{D_1 \cup D_2}\left((\overline{iffs}, nf), (iffs, nf), (iffs, \overline{nf})\right) = 0.1$$
$$m_3^{D_1 \cup D_2}\left((\overline{iffs}, \overline{nf}), (iffs, nf), (iffs, \overline{nf})\right) = 0.7$$
$$m_3^{D_1 \cup D_2}\left((iffs, \overline{nf}), (iffs, nf), (\overline{iffs}, \overline{nf}), (\overline{iffs}, nf)\right) = 0.2$$

Combining the results of both rules:

	$m_3\{(Rule\ 1) \cap (Rule\ 2)\}$	$m_{3-Rule\ 1} \oplus m_{3-Rule\ 2}$
$\alpha_1(1-\beta_2)$ = 0.95 x 0.70 = 0.665	$m_3\left\{\left((iffs,nf),(\overline{iffs},nf),(\overline{iffs},\overline{nf})\right)\right.$ $\left.\cap\left((\overline{iffs},\overline{nf}),(iffs,nf),(iffs,\overline{nf})\right)\right\}$	$m_3\{(\overline{iffs},nf),(\overline{iffs},\overline{nf})\}$
$\alpha_1(\beta_2-\alpha_2)$ = 0.95 x 0.20 = 0.190	$m_3\left\{\left((iffs,nf),(\overline{iffs},nf),(\overline{iffs},\overline{nf})\right)\right.$ $\cap\left((iffs,\overline{nf}),(iffs,nf),(\overline{iffs},\overline{nf}),(\overline{iffs},nf\right.$	$m_3\{(\overline{iffs},nf),(\overline{iffs},\overline{nf}),(iffs,nf)\}$
$\alpha_1\alpha_2$ =0.95 x 0.10 =0.095	$m_3\left\{\left((iffs,nf),(\overline{iffs},nf),(\overline{iffs},\overline{nf})\right)\right.$ $\left.\cap\left((\overline{iffs},nf),(iffs,nf),(iffs,\overline{nf})\right)\right\}$	$m_3\{(\overline{iffs},\overline{nf}),(iffs,nf)\}$
$(1-\alpha_1)(1-\beta_2)$ 0.05 x 0.70 = 0.035	$m_3\left\{\left((iffs,nf),(\overline{iffs},nf),(iffs,\overline{nf}),(\overline{iffs},\right.\right.$ $\left.\cap\left((\overline{iffs},\overline{nf}),(iffs,nf),(iffs,\overline{nf})\right)\right\}$	$m_3\{(\overline{iffs},\overline{nf}),(iffs,nf),(iffs,\overline{nf})\}$
$(1-\alpha_1)\alpha_2$ = 0.05 x 0.20 = 0.010	$m_3\left\{\left((iffs,nf),(\overline{iffs},nf),(iffs,\overline{nf}),(\overline{iffs},\right.\right.$ $\cap\left((iffs,\overline{nf}),(iffs,nf),(\overline{iffs},\overline{nf}),(\overline{iffs},nf\right.$	$m_3\{(\overline{iffs},nf),(\overline{iffs},\overline{nf}),(iffs,nf),(iffs,\overline{nf}$
$(1-\alpha_1)(\beta_2-\alpha_2)$ = 0.05 x 0.10 = 0.005	$m_3\left\{\left((iffs,nf),(\overline{iffs},nf),(iffs,\overline{nf}),(\overline{iffs},\right.\right.$ $\left.\cap\left((\overline{iffs},nf),(iffs,nf),(iffs,\overline{nf})\right)\right\}$	$m_3\{(\overline{iffs},nf),(iffs,nf),(iffs,\overline{nf})\}$

BBA for m4: *(same approach as m3)*

m4: is defined on the domain {FPA, NF}. Our *a priori* knowledge is that:

Rule 1: *We are 95 to 100% confident that if the target is flying in accordance with their flight plan, FPA = 1, (fpa) then the target is friendly, NF=0 is true (nf). That is if fpa then nf with a = 0.95*

$$m_4^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup (\bar{A} \times \Theta_{D_2}) \\ 1-\alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$$\Theta_{D_1} = \{1, 0\} \qquad \Theta_{D_2} = \{0, 1\}$$

Or: $\Theta_{D_1} = \{fpa, \overline{fpa}\} \qquad \Theta_{D_2} = \{nf, \overline{nf}\}$

$m_4^{D_1 \cup D_2}(C) = 0.95 \quad C = (fpa \times nf) \cup (fpa \times \Theta_{D_2})$

$$m_4^{D_1 \cup D_2}(C) = 0.95 \quad C = (fpa \times nf) \cup \left(\overline{fpa} \times (nf, \overline{nf}\ )\right)$$

$$m_4^{D_1 \cup D_2}\left((fpa,nf),(\overline{fpa},nf),(fpa,\overline{nf})\right) = 0.95$$

And: $m_4^{D_1 \cup D_2}(C) = 1-\alpha \quad C = \Theta_{D_1 \cup D_2}$

$$m_4^{D_1 \cup D_2}(C) = 0.95 \quad C = (fpa, \overline{fpa}) \times (nf, \overline{nf})$$

$$m_4^{D_1 \cup D_2}\left((fpa,nf),(\overline{fpa},nf),(fpa,\overline{nf}),(\overline{fpa},\overline{nf})\right) = 0.05$$

Rule 2: *Conversely, if the target is not flying in accordance with its flight plan, FPA=0 then we are 10 to 30% confident that the target is non-friendly, NF=1. That is if* $\overline{fpa}$ *then nf with a = 0.10, β = 0.30.*

$$m_4^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup (\bar{A} \times \Theta_{D_2}) \\ 1-\beta & C = (A \times \bar{B}) \cup (\bar{A} \times \Theta_{D_2}) \\ \beta - \alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

$$m_4^{D_1 \cup D_2}(C) = \begin{cases} 0.1 & C = (\overline{fpa} \times \overline{nf}) \cup \left(fpa \times (nf, \overline{nf})\right) \\ 1 - 0.3 & C = (\overline{fpa} \times nf) \cup \left(fpa \times (nf, \overline{nf})\right) \\ 0.3 - 0.1 & C = (fpa, \overline{fpa}) \times (nf, \overline{nf}) \end{cases}$$

$$m_4^{D_1 \cup D_2}\left((\overline{fpa}, \overline{nf}), (fpa, nf), (fpa, \overline{nf})\right) = 0.10$$

$$m_4^{D_1 \cup D_2}\left((\overline{fpa}, nf), (fpa, nf), (fpa, \overline{nf})\right) = 0.70$$

$$m_4^{D_1 \cup D_2}\left((fpa, \overline{nf}), (fpa, nf), (\overline{fpa}, \overline{nf}), (\overline{fpa}, nf)\right) = 0.20$$

Combining rules:	$m_4\{(Rule\ 1) \cap (Rule\ 2)\}$	$m_{4-Rule\ 1} \oplus m_{4-Rule\ 2}$
$\alpha_1(1 - \beta_2)$ = 0.95 x 0.70 = 0.665	$m_4\left\{\left((fpa, nf), (\overline{fpa}, nf), (\overline{fpa}, \overline{nf})\right)\right.$ $\left.\cap \left((\overline{fpa}, nf), (fpa, nf), (fpa, \overline{nf})\right)\right\}$	$m_4\{(\overline{fpa}, nf), (fpa, nf)\}$
$\alpha_1(\beta_2 - \alpha_2)$ = 0.95 x 0.20 = 0.190	$m_4\left\{\left((fpa, nf), (\overline{fpa}, nf), (\overline{fpa}, \overline{nf})\right)\right.$ $\left.\cap \left((fpa, \overline{nf}), (fpa, nf), (\overline{fpa}, \overline{nf}), (\overline{fpa}, nf)\right)\right\}$	$m_4\{(\overline{fpa}, nf), (\overline{fpa}, \overline{nf}), (fpa, nf)\}$
$\alpha_1\alpha_2$ =0.95 x 0.10 =0.095	$m_4\left\{\left((fpa, nf), (\overline{fpa}, nf), (\overline{fpa}, \overline{nf})\right)\right.$ $\left.\cap \left((\overline{fpa}, \overline{nf}), (fpa, nf), (fpa, \overline{nf})\right)\right\}$	$m_4\{(\overline{fpa}, \overline{nf}), (fpa, nf)\}$
$(1 - \alpha_1)(1 - \beta_2)$ 0.05 x 0.70 = 0.035	$m_4\left\{\left((fpa, nf), (\overline{fpa}, nf), (fpa, \overline{nf}), (\overline{fpa}, \overline{nf})\right)\right.$ $\left.\cap \left((\overline{fpa}, nf), (fpa, nf), (fpa, \overline{nf})\right)\right\}$	$m_4\{(\overline{fpa}, nf), (fpa, nf), (fpa, \overline{nf})\}$
$(1 - \alpha_1)\alpha_2$ = 0.05 x 0.20 = 0.010	$m_4\left\{\left((fpa, nf), (\overline{fpa}, nf), (fpa, \overline{nf}), (\overline{fpa}, \overline{nf})\right)\right.$ $\left.\cap \left((fpa, \overline{nf}), (fpa, nf), (\overline{fpa}, \overline{nf}), (\overline{fpa}, nf)\right)\right\}$	$m_4\{(\overline{fpa}, nf), (\overline{fpa}, \overline{nf}), (fpa, nf), (fpa, \overline{nf}$
$(1 - \alpha_1)(\beta_2 - \alpha_2)$ = 0.05 x 0.10 = 0.005	$m_4\left\{\left((fpa, nf), (\overline{fpa}, nf), (fpa, \overline{nf}), (\overline{fpa}, \overline{nf})\right)\right.$ $\left.\cap \left((\overline{fpa}, \overline{nf}), (fpa, nf), (fpa, \overline{nf})\right)\right\}$	$m_4\{(\overline{fpa}, \overline{nf}), (fpa, nf), (fpa, \overline{nf})\}$

Extend BBA m₃ from domain { IFFS, NF } to common frame $\Theta_V = \{IFFS, FPA, NF\}$

$m'_3 = \mathrm{m}_3^{\{\mathrm{IFFS,NF}\}\uparrow\{\mathrm{IFFS,FPA,NF}\}}$ d$(m_3) = \{\mathrm{IFFS, NF}\}$ d$(m'_3) = \{IFFS, FPA, NF\}$

$m'_3\left\{\left((\overline{iffs}, fpa, nf), (iffs, fpa, nf), (\overline{iffs}, \overline{fpa}, nf), (iffs, \overline{fpa}, nf)\right)\right\}$ = 0.665
$m'_3\left\{\left((\overline{iffs}, fpa, nf), (\overline{iffs}, fpa, \overline{nf}), (iffs, fpa, nf), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf}), (iffs, \overline{fpa}, nf)\right)\right\} = 0.190$
$m'_3\left\{\left((\overline{iffs}, fpa, \overline{nf}), (iffs, fpa, nf)\right), \left((\overline{iffs}, \overline{fpa}, \overline{nf}), (iffs, \overline{fpa}, nf)\right)\right\}$= 0.095
$m'_3\left\{\left((\overline{iffs}, fpa, nf), (iffs, fpa, nf), (iffs, fpa, \overline{nf})\right), \left((\overline{iffs}, \overline{fpa}, nf), (iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf})\right)\right\}$ = 0.035
$m'_3\left\{\begin{matrix}\left((\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, \overline{nf}), (iffs, fpa, nf), (iffs, fpa, \overline{nf})\right), \\ \left((\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf}), (iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf})\right)\end{matrix}\right\} = 0.005$
$m'_3\left\{\left((\overline{iffs}, fpa, nf), (iffs, fpa, nf), (iffs, fpa, \overline{nf})\right), \left((\overline{iffs}, \overline{fpa}, nf), (iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf})\right)\right\}$ = 0.010

Extend BBA m₄ from domain { FPA, NF } to domain $\{IFFS, FPA, NF\}$:

$m'_4 = \mathrm{m}_4^{\{\mathrm{FPA,NF}\}\uparrow\{\mathrm{IFFS,FPA,NF}\}}$ d$(m_4) = \{\mathrm{FPA, NF}\}$ d$(m'_4) = \{IFFS, FPA, NF\}$

$m_4\left\{\begin{matrix}(iffs, \overline{fpa}, nf), (iffs, fpa, nf), \\ (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, fpa, nf)\end{matrix}\right\} = 0.665$

$m_4\left\{\begin{matrix}(iffs,\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf}),(iffs,fpa,nf),\\(\overline{iffs},\overline{fpa},nf),(\overline{iffs},\overline{fpa},\overline{nf}),(\overline{iffs},fpa,nf)\end{matrix}\right\}=0.190$
$m_4\left\{\begin{matrix}\left((iffs,\overline{fpa},\overline{nf}),(iffs,fpa,nf)\right),\\\left((\overline{iffs},\overline{fpa},\overline{nf}),(\overline{iffs},fpa,nf)\right)\end{matrix}\right\}=0.095$
$m_4\left\{\begin{matrix}(iffs,\overline{fpa},nf),(iffs,fpa,nf),(iffs,fpa,\overline{nf}),\\(\overline{iffs},\overline{fpa},nf),(\overline{iffs},fpa,nf),(\overline{iffs},fpa,\overline{nf})\end{matrix}\right\}=0.035$
$m_4\left\{\begin{matrix}(iffs,\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf}),(iffs,fpa,nf),(iffs,fpa,\overline{nf}),\\(\overline{iffs},\overline{fpa},nf),(\overline{iffs},\overline{fpa},\overline{nf}),(\overline{iffs},fpa,nf),(\overline{iffs},fpa,\overline{nf})\end{matrix}\right\}=0.005$
$m_4\left\{\begin{matrix}(iffs,\overline{fpa},\overline{nf}),(iffs,fpa,nf),(iffs,fpa,,\overline{nf}),\\(\overline{iffs},\overline{fpa},\overline{nf}),(\overline{iffs},fpa,nf),(\overline{iffs},fpa,\overline{nf})\end{matrix}\right\}=0.010$

We can now calculate $m_3 \oplus m_4$:

Mass	m₃ ⊕ m₄	$(iffs, fpa, n$	$(iffs, fpa, \overline{nf}$	$(iffs, \overline{fpa}, nf$	$(iffs, \overline{fpa}, \overline{nf}$	$(\overline{iffs}, fpa, nf$	$(\overline{iffs}, fpa, \overline{nf}$	$(\overline{iffs}, \overline{fpa}, nf$	$(\overline{iffs}, \overline{fpa}, \overline{nf})$
m_3 = 0.665	0.442	×		×		×		×	
m_4 = 0.665				×	×			×	×
m_3 = 0.665	0.126					×	×	×	×
m_4 = 0.190		×		×	×	×		×	×
m_3 = 0.665	0.063	×		×		×		×	
m_4 = 0.095		×		×		×			×
m_3 = 0.665	0.023	×		×		×		×	
m_4 = 0.035			×	×	×		×	×	×
m_3 = 0.665	0.003	×		×		×		×	
m_4 = 0.005		×	×	×	×	×	×	×	×
m_3 = 0.665	0.066	×		×		×		×	
m_4 = 0.010		×	×	×		×	×	×	
m_3 = 0.190	0.126	×		×		×	×	×	×
m_4 = 0.665				×	×			×	×
m_3 = 0.190	0.036	×		×		×	×	×	×
m_4 = 0.190		×		×	×	×		×	×
m_3 = 0.190	0.018	×		×		×	×	×	×
m_4 = 0.095		×		×		×			×
m_3 = 0.190	0.007	×		×		×	×	×	×
m_4 = 0.035			×	×	×		×	×	×
m_3 = 0.190	0.001	×		×		×	×	×	×
m_4 = 0.005		×	×	×	×	×	×	×	×
m_3 = 0.190	0.002	×		×		×	×	×	×
m_4 = 0.010		×	×	×		×	×	×	
m_3 = 0.095	0.063	×		×			×		×
m_4 = 0.665				×	×			×	×
m_3 = 0.095	0.018	×		×			×		×
m_4 = 0.190		×		×	×	×		×	×
m_3 = 0.095	0.009	×		×			×		×
m_4 = 0.095		×		×		×			×
m_3 = 0.095	0.003	×		×			×		×
m_4 = 0.035			×	×	×		×	×	×
m_3 = 0.095	0.0005	×		×			×		×
m_4 = 0.005		×	×	×	×	×	×	×	×
m_3 = 0.095	0.001	×		×			×		×
m_4 = 0.010		×	×	×		×	×	×	
m_3 = 0.035	0.023	×	×	×	×	×		×	
m_4 = 0.665				×	×			×	×
m_3 = 0.035	0.007		×	×	×	×		×	×
m_4 = 0.190		×		×	×	×		×	×

Mass	$m_3 \oplus m_4$	$(\,iffs,fpa,r$	$(iffs,fpa,\overline{n}$	$(iffs,\overline{fpa},n$	$(iffs,\overline{fpa},\overline{n}$	$(\overline{iffs},fpa,n$	$(\overline{iffs},fpa,\overline{n}$	$(\overline{iffs},\overline{fpa},n$	$(\overline{iffs},\overline{fpa},\overline{n}$
$m_3 = 0.035$	0.003	×	×	×	×	×		×	
$m_4 = 0.095$		×		×		×			×
$m_3 = 0.035$	0.001	×	×	×	×	×		×	
$m_4 = 0.035$			×	×	×		×	×	×
$m_3 = 0.035$	0.0002	×	×	×	×	×		×	
$m_4 = 0.005$		×	×	×	×	×	×	×	×
$m_3 = 0.035$	0.0003	×	×	×	×	×		×	
$m_4 = 0.010$		×	×	×		×	×	×	
$m_3 = 0.005$	0.003	×	×	×	×	×	×	×	×
$m_4 = 0.665$				×	×			×	×
$m_3 = 0.005$	0.001	×	×	×	×	×	×	×	×
$m_4 = 0.190$		×		×	×	×		×	×
$m_3 = 0.005$	0.0005	×	×	×	×	×	×	×	×
$m_4 = 0.095$		×		×		×			×
$m_3 = 0.005$	0.0002	×	×	×	×	×	×	×	×
$m_4 = 0.035$			×	×	×		×	×	×
$m_3 = 0.005$	0.00002	×	×	×	×	×	×	×	×
$m_4 = 0.005$		×	×	×	×	×	×	×	×
$m_3 = 0.005$	0.00005	×	×	×	×	×	×	×	×
$m_4 = 0.010$		×	×	×		×	×	×	
$m_3 = 0.010$	0.0067	×	×	×	×	×		×	
$m_4 = 0.665$				×	×			×	×
$m_3 = 0.010$	0.0019	×	×	×	×	×		×	
$m_4 = 0.190$		×		×	×	×		×	×
$m_3 = 0.010$	0.001	×	×	×	×	×		×	
$m_4 = 0.095$		×		×		×			×
$m_3 = 0.010$	0.0003	×	×	×	×	×		×	
$m_4 = 0.035$			×	×	×		×	×	×
$m_3 = 0.010$	0.00005	×	×	×	×	×		×	
$m_4 = 0.005$		×	×	×	×	×	×	×	×
$m_3 = 0.010$	0.00001	×	×	×	×	×		×	
$m_4 = 0.010$		×	×	×		×	×	×	

Which yields through $m_3 \oplus m_4$ combination:

Mass	$m_3 \oplus m_4$	$m_3 \oplus m_4$
$m_3 = 0.665$	0.442	$(iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, nf)$
$m_4 = 0.665$		
$m_3 = 0.665$	0.126	$(\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$
$m_4 = 0.190$		
$m_3 = 0.665$	0.063	$(iffs, \overline{fpa}, nf), (iffs, fpa, nf), (\overline{iffs}, fpa, nf)$
$m_4 = 0.095$		
$m_3 = 0.665$	0.023	$(iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, nf)$
$m_4 = 0.035$		
$m_3 = 0.665$	0.003	$(\overline{iffs}, fpa, nf), (iffs, fpa, nf), (\overline{iffs}, \overline{fpa}, nf), (iffs, \overline{fpa}, nf)$
$m_4 = 0.005$		
$m_3 = 0.665$	0.066	$(\overline{iffs}, fpa, nf), (iffs, fpa, nf), (iffs, \overline{fpa}, nf)$
$m_4 = 0.010$		
$m_3 = 0.190$	0.126	$(iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$
$m_4 = 0.665$		
$m_3 = 0.190$	0.036	$(iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$
$m_4 = 0.190$		
$m_3 = 0.190$	0.018	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$
$m_4 = 0.095$		
$m_3 = 0.190$	0.007	$(iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$
$m_4 = 0.035$		
$m_3 = 0.190$	0.001	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf),$ $(\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$
$m_4 = 0.005$		
$m_3 = 0.190$	0.002	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf),$ $(\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, \overline{fpa}, nf)$
$m_4 = 0.010$		
$m_3 = 0.095$	0.063	$(iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$
$m_4 = 0.665$		
$m_3 = 0.095$	0.018	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$
$m_4 = 0.190$		
$m_3 = 0.095$	0.009	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$
$m_4 = 0.095$		
$m_3 = 0.095$	0.003	$(iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, \overline{fpa}, \overline{nf})$
$m_4 = 0.035$		
$m_3 = 0.095$	0.0005	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, \overline{fpa}, \overline{nf})$
$m_4 = 0.005$		
$m_3 = 0.095$	0.001	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, \overline{nf})$
$m_4 = 0.010$		

$m_3 = 0.035$	0.023	$(iffs,\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf}),(\overline{iffs},\overline{fpa},nf)$
$m_4 = 0.665$		
$m_3 = 0.035$	0.007	$(iffs,\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf}),(\overline{iffs},fpa,nf),$ $(\overline{iffs},\overline{fpa},nf),(\overline{iffs},\overline{fpa},\overline{nf})$
$m_4 = 0.190$		

Mass	$m_3 \oplus m_4$	$m_3 \oplus m_4$
$m_3 = 0.035$	0.003	$(iffs,\overline{fpa},nf),(\overline{iffs},fpa,nf),(iffs,fpa,nf)$
$m_4 = 0.095$		
$m_3 = 0.035$	0.001	$(iffs,fpa,\overline{nf}),(iffs,\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf}),(\overline{iffs},\overline{fpa},nf)$
$m_4 = 0.035$		
$m_3 = 0.035$	0.0002	$(iffs,fpa,\overline{nf}),(iffs,\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf}),$ $(\overline{iffs},fpa,nf),(\overline{iffs},fpa,\overline{nf}),(iffs,fpa,nf)$
$m_4 = 0.005$		
$m_3 = 0.035$	0.0003	$(iffs,fpa,\overline{nf}),(iffs,\overline{fpa},nf),(\overline{iffs},fpa,nf),(\overline{iffs},\overline{fpa},nf)$
$m_4 = 0.010$		$,(iffs,fpa,nf)$
$m_3 = 0.005$	0.003	$(iffs,\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf}),(\overline{iffs},\overline{fpa},nf),(\overline{iffs},\overline{fpa},\overline{nf})$
$m_4 = 0.665$		
$m_3 = 0.005$	0.001	$(iffs,fpa,nf),(iffs,\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf}),$ $(\overline{iffs},fpa,nf),(\overline{iffs},\overline{fpa},nf),(\overline{iffs},\overline{fpa},\overline{nf})$
$m_4 = 0.190$		
$m_3 = 0.005$	0.0005	$(iffs,fpa,nf),(iffs,\overline{fpa},nf),(\overline{iffs},fpa,nf),(\overline{iffs},\overline{fpa},\overline{nf})$
$m_4 = 0.095$		
$m_3 = 0.005$	0.0002	$(iffs,fpa,\overline{nf}),(iffs,\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf}),$ $(\overline{iffs},fpa,\overline{nf}),(\overline{iffs},\overline{fpa},nf),(\overline{iffs},\overline{fpa},\overline{nf})$
$m_4 = 0.035$		
$m_3 = 0.005$	0.00002	$(iffs,fpa,nf),(iffs,fpa,\overline{nf}),(iffs,\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf}),$ $(\overline{iffs},fpa,\overline{nf}),(\overline{iffs},fpa,nf),(\overline{iffs},\overline{fpa},nf),(\overline{iffs},\overline{fpa},\overline{nf})$
$m_4 = 0.005$		
$m_3 = 0.005$	0.00005	$(iffs,fpa,nf),(iffs,fpa,\overline{nf}),(iffs,\overline{fpa},nf),$ $(\overline{iffs},fpa,\overline{nf}),(\overline{iffs},fpa,nf),(\overline{iffs},\overline{fpa},nf)$
$m_4 = 0.010$		
$m_3 = 0.010$	0.0067	$(iffs,\overline{fpa},nf),(\overline{iffs},\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf})$
$m_4 = 0.665$		
$m_3 = 0.010$	0.0019	$(iffs,fpa,nf),(iffs,\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf}),$ $(\overline{iffs},fpa,nf),(\overline{iffs},\overline{fpa},nf)$
$m_4 = 0.190$		
$m_3 = 0.010$	0.001	$(iffs,fpa,nf),(iffs,\overline{fpa},nf),(\overline{iffs},fpa,nf)$
$m_4 = 0.095$		
$m_3 = 0.010$	0.0003	$(iffs,fpa,\overline{nf}),(iffs,\overline{fpa},nf),(\overline{iffs},\overline{fpa},nf),(iffs,\overline{fpa},\overline{nf})$
$m_4 = 0.035$		

$m_3 = 0.010$	0.00005	$(iffs, fpa, nf), (iffs, fpa, \overline{nf}), (iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf}),$ $(\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, nf)$
$m_4 = 0.005$		
$m_3 = 0.010$	0.00001	$(iffs, fpa, nf), (iffs, fpa, \overline{nf}), (iffs, \overline{fpa}, nf),$ $(\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, nf)$
$m_4 = 0.010$		

To find out chance of target not friendly, need to marginalise {IFFS, FPA, NF} to frame $\Theta_V = \{\mathrm{nf}, \overline{\mathrm{nf}}\}$.

$m_3 \oplus m_4$	$m_3 \oplus m_4$	marginalise
0.442	$(iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, nf)$	{nf}
0.126	$(\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.063	$(iffs, \overline{fpa}, nf), (iffs, fpa, nf), (\overline{iffs}, fpa, nf)$	{nf}
0.023	$(iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, nf)$	{nf}
0.003	$(\overline{iffs}, fpa, nf), (iffs, fpa, nf), (\overline{iffs}, \overline{fpa}, nf), (iffs, \overline{fpa}, nf)$	{nf}
0.066	$(\overline{iffs}, fpa, nf), (iffs, fpa, nf), (iffs, \overline{fpa}, nf)$	{nf}
0.126	$(iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.036	$(iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.018	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.007	$(iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.001	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf), (\overline{iffs}, fpa, \overline{nf}),$ $(\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.002	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf), (\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, \overline{fpa}, nf)$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.063	$(iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.018	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.009	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.003	$(iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.0005	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.001	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.023	$(iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf}), (\overline{iffs}, \overline{fpa}, nf)$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.007	$(iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf}), (\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.003	$(iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf), (iffs, fpa, nf)$	{nf}
0.001	$(iffs, fpa, \overline{nf}), (iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf}), (\overline{iffs}, \overline{fpa}, nf)$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.0002	$(iffs, fpa, \overline{nf}), (iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf}), (\overline{iffs}, fpa, nf),$ $(\overline{iffs}, fpa, \overline{nf}), (iffs, fpa, nf)$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.0003	$(iffs, fpa, \overline{nf}), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, nf)$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.003	$(iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf}), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.001	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf}), (\overline{iffs}, fpa, nf),$ $(\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.0005	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	{nf}
0.0002	$(iffs, fpa, \overline{nf}), (iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf}),$ $(\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.00002	$(iffs, fpa, nf), (iffs, fpa, \overline{nf}), (iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf}),$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$

	$(\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, \overline{nf})$	
0.00005	$(iffs, fpa, nf), (iffs, fpa, \overline{nf}), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, \overline{nf}), (\overline{iffs}, fpa, nf),$ $(\overline{iffs}, \overline{fpa}, nf)$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.0067	$(iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.0019	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf}), (\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, nf)$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.001	$(iffs, fpa, nf), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf)$	$\{\mathrm{nf}\}$
0.0003	$(iffs, fpa, \overline{nf}), (iffs, \overline{fpa}, nf), (\overline{iffs}, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf})$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.00005	$(iffs, fpa, nf), (iffs, fpa, \overline{nf}), (iffs, \overline{fpa}, nf), (iffs, \overline{fpa}, \overline{nf}), (\overline{iffs}, fpa, nf),$ $(\overline{iffs}, \overline{fpa}, nf)$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$
0.00001	$(iffs, fpa, nf), (iffs, fpa, \overline{nf}), (iffs, \overline{fpa}, nf), (\overline{iffs}, fpa, nf), (\overline{iffs}, \overline{fpa}, nf)$	$\{\mathrm{nf}, \overline{\mathrm{nf}}\}$

$\mathrm{m}\{\mathrm{nf}\} = 0.442+0.063+0.023+0.003+0.066+0.003+0.0005+0.001=0.60$ $\mathrm{m}\{\mathrm{nf}, \overline{\mathrm{nf}}\} = 0.40$

i.e. 60% confident target is non-friendly.

BBA m₅:

Relates the Platform Type (PT) variable to the NF variable using the following rule:

Based on *a priori* knowledge, if the target is non-friendly (NF=1) then the target can be one of three platform types:

$$PT \in \{3, 4, 5\} \text{ with confidence between 50 and 100\%}$$

m_5: is defined on the domain {NF, PT}. Our *a priori* knowledge is that:

Rule: We are 50 to 100% confident that if the target is non-friendly (NF=1) in the battlespace then the air platform is likely to be of type 3, 4 or 5. That is if NF = 1 then $PT \in \{3, 4, 5\}$ with at least 50% confidence.

$$\alpha = 0.50 \text{ and } \beta = 1.0$$

Rule can be expressed as:

$$A \subseteq \Theta_{D_1} \Rightarrow B \subseteq \Theta_{D_2}\ with\ confidence\ p \in [\alpha, \beta]$$

$$m_5^{D_1 \cup D_2}(C) = \begin{cases} \alpha & C = (A \times B) \cup (\bar{A} \times \Theta_{D_2}) \\ 1 - \alpha & C = \Theta_{D_1 \cup D_2} \end{cases}$$

So when: $$m_5^{D_1 \cup D_2}(C) = \alpha \quad C = (A \times B) \cup (\bar{A} \times \Theta_{D_2})$$

$$\alpha = 0.50$$
$$D_1 = \{NF\} \qquad D_2 = \{PT\}$$

And frames are: $$\Theta_{D_1} = \{NF, \overline{NF}\} \qquad \Theta_{D_2} = \{PT, \overline{PT}\}$$
$$\Theta_{D_1} = \{1, 0\} \qquad \Theta_{D_2} = \{0, 1, 2, 3, 4, 5\}$$

$$m_5^{D_1 \cup D_2}(C) = 0.50 \quad C = (NF \times PT) \cup \left(\overline{NF} \times \Theta_{D_2}\right)$$
$$m_5^{D_1 \cup D_2}(C) = 0.50 \quad C = (NF \times PT) \cup \left(NF \times (PT, \overline{PT})\right)$$
$$m_5^{D_1 \cup D_2}(C) = 0.50 \quad C = (1 \times (3,4,5)) \cup \left(0 \times (0,1,2,3,4,5)\right)$$
$$m_5^{D_1 \cup D_2}\left((1,3),(1,4),(1,5),(0,0),(0,1),(0,2),(0,3),(0,4),(0,5)\right) = 0.50$$

(α)

And:

$$m_5^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$$
$$m_5^{D_1 \cup D_2}(C) = 0.50 \quad C = (NF, \overline{NF}) \times (PT, \overline{PT})$$
$$m_5^{D_1 \cup D_2}(C) = 0.50 \quad C = (1,0) \times (0,1,2,3,4,5)$$

$$m_5^{D_1 \cup D_2}\begin{pmatrix}(1,0),(1,1),(1,2),(1,3),(1,4),(1,5),\\(0,0),(0,1),(0,2),(0,3),(0,4),(0,5)\end{pmatrix} = 0.50\ (1 - \alpha)$$

BBA m_6:

Relates the Platform Type (PT) variable to the Weapon Engagement Range (WER) variable. That is we have *a priori* information that permits us to estimate the WER based on the platform type identified, using the following rules:
m_6: is defined on the domain {PT, WER}. Our *a priori* knowledge is that:

Rule 1: *We are 40 to 100% confident that if the target is either platform type 0 or 1, it has no WER.* $PT \in \{0,1\} \Rightarrow WER = 0 \text{ with confidence } p \in [0.4, 1.0]$

Rule 2*: We are 40 to 100% confident that if the target is either platform type 2 or 3, it has an WER of either 1 or 2.* $PT \in \{2,3\} \Rightarrow WER \in \{1,2\} \text{ with confidence } p \in [0.4, 1.0]$

Rule 3: *We are 40 to 100% confident that if the target is either platform type 4 or 5, it has an WER of either 2 or 3.* $PT \in \{4,5\} \Rightarrow WER = 2 \text{ with confidence } p \in [0.4, 1.0]$

$$D_1 = \{PT\} \qquad D_2 = \{WER\}$$

RULE 1: $PT \in \{0,1\} \Rightarrow WER = 0$

$$\Theta_{D_1} = \{0,1,2,3,4,5\} \quad \Theta_{D_2} = \{0,1,2,3\}$$
$$m_6^{D_1 \cup D_2}(C) = 0.40 \quad C = (pt \times wer) \cup \left(\overline{pt} \times \Theta_{D_2}\right)$$
$$m_6^{D_1 \cup D_2}(C) = 0.40 \quad C = (pt \times wer) \cup \left(\overline{pt} \times (wer, \overline{wer})\right)$$

In this case: pt = {0, 1}, $\overline{pt}$= {2, 3, 4, 5}
And: wer = {0}, $\overline{wer}$ = {1, 2, 3}

(pt, wer) = {(0, 0), (1, 0)}
$(\overline{pt}, wer)$ = {(2, 0), (3, 0), (4, 0), (5, 0)}
$(pt, \overline{wer})$ = {(0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3)}

$(\overline{pt}, \overline{wer})$ = {(2, 1), (3, 1), (4, 1), (5, 1), (2, 2), (3, 2), (4, 2), (5, 2), (2, 3), (3, 3), (4, 3), (5, 3)}

$m_6^{D_1 \cup D_2}\big((pt, wer), (\overline{pt}, wer), (pt, \overline{wer})\big) = \ 0.40$

$$m_6^{D_1 \cup D_2}\begin{pmatrix}(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),\\(0,1),(0,2),(0,3),(1,1),(1,2),(1,3)\end{pmatrix} = 0.40$$

And: $m_6^{D_1 \cup D_2}(C) = \ 1 - \alpha \quad C = \ \Theta_{D_1 \cup D_2}$

$m_6^{D_1 \cup D_2}(C) = \ 0.60 \quad C = \ \Theta_{D_1} \times \Theta_{D_2}$

$m_6^{D_1 \cup D_2}(C) = \ 0.60 \quad C = \ (pt, \overline{pt}) \times (wer, \overline{wer})$

$m_6^{D_1 \cup D_2}\big((pt, wer), (\overline{pt}, wer), (pt, \overline{wer}), (\overline{pt}, \overline{wer})\big) = \ 0.40$

$$m_6^{D_1 \cup D_2}\begin{pmatrix}(0,0),(1,0),(3,0),(4,0),(5,0),\\(0,1),(0,2),(0,3),(1,1),(1,2),\\(1,3),(3,1),(4,1),(5,1),(3,2),\\(4,2),(5,2),(3,3),(4,3),(5,3)\end{pmatrix} = 0.40$$

RULE 2: $PT \ \in \ \{2, 3\}\, WER \ \in \ \{1, 2\}$

$\Theta_{D_1} \ = \ \{0, 1, 2, 3, 4, 5\} \quad \Theta_{D_2} \ = \ \{0,1, 2, 3\}$

$m_6^{D_1 \cup D_2}(C) = \ 0.40 \quad C = (pt \times wer) \ \cup \left(\overline{pt} \times \Theta_{D_2}\right)$

$m_6^{D_1 \cup D_2}(C) = \ 0.40 \quad C = (pt \times wer) \ \cup \left(\overline{pt} \times (wer, \overline{wer}\ )\right)$

In this case: pt = {2, 3}, $\overline{pt}$= {0, 1, 4, 5}

And: wer = {1, 2}, $\overline{wer}$= {0, 3}

(pt, wer) = {(2, 1), (2, 2), (3, 1), (3, 2)}

$(\overline{pt}, wer)$ = {(0, 1), (0, 2), (1, 1), (1, 2)} (4, 1), (4, 2), (5, 1), (5, 2)}

$(pt, \overline{wer})$ = {(2, 0), (2, 3), (3, 0), (3, 3)}

$(\overline{pt}, \overline{wer})$ = {(0, 0), (0, 3), (1, 0), (1, 3)} (4, 0), (4, 3), (5, 0), (5, 3)}

$m_6^{D_1 \cup D_2}\big((pt, wer), (\overline{pt}, wer), (\overline{pt}, \overline{wer})\big) = \ 0.40 \ \ (\alpha)$

$$m_6^{D_1 \cup D_2}\begin{pmatrix}(2,1),(2,2),(3,1),(3,2),(0,1),(0,2),\\(1,1),(1,2),(4,1),(4,2),(5,1),(5,2),\\(2,0),(2,3),(3,0),(3,3),(0,0),(0,3),\\(1,0),(1,3),(4,0),(4,3),(5,0),(5,3)\end{pmatrix} = \ 0.40 \ \ (\alpha)$$

And: $m_6^{D_1 \cup D_2}(C) = \ 1 - \alpha \quad C = \ \Theta_{D_1 \cup D_2}$

$m_6^{D_1 \cup D_2}(C) = \ 0.60 \quad C = \ (pt, \overline{pt}) \times (wer, \overline{wer})$

$$m_6^{D_1 \cup D_2}\big((pt, wer), (\overline{pt}, wer), (pt, \overline{wer}), (\overline{pt}, \overline{wer})\big) = 0.60\ (1 - \alpha)$$

$$m_6^{D_1 \cup D_2}\begin{pmatrix} (2,1),(2,2),(3,1),(3,2),(0,1), \\ (0,2),(1,1),(1,2)\}\ (4,1),(4,2), \\ (5,1),(5,2),(0,0),(0,3),(1,0), \\ (1,3),(4,0),(4,3),(5,0),(5,3), \end{pmatrix} = 0.60\ (1 - \alpha)$$

RULE 3: $PT\ \in \{4, 5\} \Rightarrow WER\ \in \{2, 3\}$

$\Theta_{D_1} = \{0, 1, 2, 3, 4, 5\}\quad \Theta_{D_2} = \{0,1, 2, 3\}$
$m_6^{D_1 \cup D_2}(C) = 0.40 \quad C = (pt \times wer)\ \cup \big(\overline{pt} \times \Theta_{D_2}\big)$
$m_6^{D_1 \cup D_2}(C) = 0.40 \quad C = (pt \times wer)\ \cup \big(\overline{pt} \times (wer, \overline{wer}\ )\big)$

In this case: pt = {4, 5}, $\overline{pt}$= {0, 1, 2, 3}
And: wer = {2, 3}, $\overline{wer}$= {0, 1}

(pt, wer) = {(2, 1), (2, 2), (3, 1), (3, 2)}
$(\overline{pt}, wer)$ = {(0, 1), (0, 2), (1, 1), (1, 2)} (4, 1), (4, 2), (5, 1), (5, 2)}
$(pt, \overline{wer})$ = {(2, 0), (2, 3), (3, 0), (3, 3)}
$(\overline{pt}, \overline{wer})$ = {(0, 0), (0, 3), (1, 0), (1, 3)} (4, 0), (4, 3), (5, 0), (5, 3)}

$$m_6^{D_1 \cup D_2}\big((pt, wer), (\overline{pt}, wer), (\overline{pt}, \overline{wer})\big) = 0.40\ (\alpha)$$

$$m_6^{D_1 \cup D_2}\begin{pmatrix} (2,1),(2,2),(3,1),(3,2),(0,1),(0,2), \\ (1,1),(1,2),(4,1),(4,2),(5,1),(5,2), \\ (2,0),(2,3),(3,0),(3,3),(0,0),(0,3), \\ (1,0),(1,3),(4,0),(4,3),(5,0),(5,3) \end{pmatrix} = 0.40\ (\alpha)$$

And: $m_6^{D_1 \cup D_2}(C) = 1 - \alpha \quad C = \Theta_{D_1 \cup D_2}$

$m_6^{D_1 \cup D_2}(C) = 0.60 \quad C = (pt, \overline{pt}) \times (wer, \overline{wer})$
$m_6^{D_1 \cup D_2}\big((pt, wer), (\overline{pt}, wer), (pt, \overline{wer}), (\overline{pt}, \overline{wer})\big) = 0.60\ (1 - \alpha)$

$$m_6^{D_1 \cup D_2}\begin{pmatrix} (2,1),(2,2),(3,1),(3,2),(0,1), \\ (0,2),(1,1),(1,2)\}\ (4,1),(4,2), \\ (5,1),(5,2),(0,0),(0,3),(1,0), \\ (1,3),(4,0),(4,3),(5,0),(5,3), \end{pmatrix} = 0.60\ (1 - \alpha)$$

BBA m7:

relates the threat Capability (C) variable to the Weapon Engagement Range (WER) and Imminence of Attack (I) variables. BBA m_7 is defined by the following rule on the product space, $C \times WER \times I$:

$$C = WER + I$$

This is a simple rule that indicates if the WER of the target is large and the imminence of attack (I) is high, then the threat capability of the target is also high.

$$\begin{aligned} &\Theta_{\mathrm{WER}} = \{0, 1, 2\} \\ &\Theta_{\mathrm{I}} = \{0, 1, 2\} \\ \Rightarrow\ &\Theta_{\mathrm{C}} = \{0, 1, 2, 3, 4\} \end{aligned}$$

Using the rule above there are 9 x (*c, wer, i*) tuplets possible:

$$m_7(\{(0,0,0),(1,0,1),(2,0,2),(1,1,0),(2,1,1),(3,1,2),(2,2,0),(3,2,1),(4,2,2),\}) = 1$$

**DEFENCE SCIENCE AND TECHNOLOGY GROUP
DOCUMENT CONTROL DATA**

1. DLM/CAVEAT (OF DOCUMENT)

2. TITLE

An Evidential Network Approach Applied to Threat Evaluation in Above Water Warfare

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED LIMITED RELEASE USE (U/L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Lloyd Hammond

5. CORPORATE AUTHOR

Defence Science and Technology Group
PO Box 1500
Edinburgh, South Australia, 5111

6a. DST GROUP NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DST-Group-TR-3349	AR-017-079	Technical Report	November 2017

8. OBJECTIVE ID	9.TASK NUMBER	10.TASK SPONSOR
	NAV 07/395	COMWAR

11. MSTC	12. STC
Tactical Systems Integration	Human and Autonomous Decision Superiority

13. DOWNGRADING/DELIMITING INSTRUCTIONS	14. RELEASE AUTHORITY
	Chief, Weapons and Combat Systems Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No limitations

17. CITATION IN OTHER DOCUMENTS

Yes

18. RESEARCH LIBRARY THESAURUS

evidential networks, above water warfare, naval combat, detect-to-engage, real-time tactical decision aids, maritime, combat, algorithm, weapon-target assignment, optimisation, dynamic programming

19. ABSTRACT

Threat prioritisation is a critical step in the detect-to-engage sequence during naval combat. As the warfighter's task requires the analysis of ever more complex scenarios, the ability to analyse all situational awareness information in a limited timeframe becomes more difficult, and the requirement for real-time tactical decision aids gains more prominence. The Evidential Network Technique is reviewed in this report with example analyses. In addition, a prototype threat evaluation model is presented for specific use in the above water warfare domain.