Bayesian Networks for Interpretable and Extensible Multi-Sensor Fusion

Leete T. Skinner[a] and Marc A. Johnson[a]

[a]Johns Hopkins University, Baltimore, MD, USA

ABSTRACT

In response to the broad range of threats experienced across the battlespace, modern defense systems have trended toward high levels of interconnectedness on the assumption that information from systems spanning numerous domains will be fused at the speed of relevance. One regime emblematic of these types of challenges is that of modern air defense, in which threats are increasing in sophistication and numerosity. To ensure the success of next generation defense systems, we need solutions where legacy and next generation sensors coexist and cohesively integrate information across domains and sources. Neural network-based approaches have demonstrated significant capabilities in dealing with complex data processing and fusion systems, however, in the context of safety critical defense systems there are various limitations that hinder their deployment. In particular, the lack of explainable outputs, the need for large amounts of data, which is typically lacking or severely limited in defense settings, and their high computational costs make NN-based solutions unsuitable. Often overlooked are more traditional and intuitive machine learning techniques such as Bayesian networks.

The attributes of Bayesian networks such flexibility, ease of use, lightweight computational needs, and innate explainability and reasoning capabilities has already led to their successful application in air defense for target tracking, identification, and intent classification. These same attributes also make Bayesian networks suitable for use in high level multi-sensor fusion. In this work we showcase the feasibility of using Bayesian networks as an extensible and dynamic multi-sensor fusion system to perform reasoning over any number of disparate black-box approaches, as well as their utility in producing more reliable, trustable, and interpretable results than any individual sensor system operating independently. We also demonstrate the ability of Bayesian networks to produce compelling results without incurring the computational overhead and difficulties associated with interpreting the results of large neural network-based approaches.

Keywords: Multi-source data fusion, object recognition, intent classification, behavior analysis, Bayesian networks, explainable AI

1. INTRODUCTION

In recent years, we have seen modern defense systems continue their trend towards higher levels of interconnectedness for a variety of reasons 1. At the same time, we have also seen advancements in computing technology and machine learning techniques and recognized their potential to address a broad range of defense use cases. While there are many defense systems and applications that stand to be positively impacted by machine learning, a standout regime is data fusion across sensors for modern air defense. New threats such as hypersonic missiles, advanced AI-piloted craft, and improvements in technology meant to evade or confuse standard air defense systems (like stealth technology), continues to make air defense a critical and challenging regime. Following the overarching paradigm of increased interconnectedness, many air defense systems currently and will continue to rely on and integrate a variety of sensors spanning numerous domains, combining readings from both legacy and next-generation systems. While data fusion in this domain is not a new concept, high performance compute, novel algorithms, and scale of data available across high cardinality systems are, and have created opportunities to develop next generation highly intelligent, interoperable, and extensible data fusion systems.

Although many newer machine learning techniques appear to be promising tools to address such needs, there remain serious concerns about neural network based approaches, especially for defense applications 2. Namely,

Further author information: (Send correspondence to L.T.S.)
L.T.S.: E-mail: leete.t.skinner@lmco.com
M.A.J.: E-mail: mjohn351@jh.edu

the lack of explainability and inability to generalize [3] have led to widespread concerns over use of AI on the battlefield. Termed “Second Wave AI” or “Narrow AI” by DARPA, the current generation neural network based techniques are characterized by their ability to meet or exceed human level performance for specific tasks, but are unable to generalize to unseen domains or problem frames [4]. Narrow AI systems have limited or non-existent means of reasoning or generalization, creating high potential for them to be fooled into delivering incorrect results [5], potentially leading to catastrophic system failures that are unacceptable in safety critical defense systems. The next state of evolution is known as “Third Wave AI”, which promises the fusion of human-level performant algorithms with the ability to reason over data and application contexts to produce trustworthy, explainable, and superhuman results. However, reaching the Third Wave state remains entirely theoretical and many experts argue we are years away from achieving it despite the impressive behavior that recent techniques, such as LLMs, have demonstrated.

In light of this, to serve the need of developing more intelligent systems, traditional machine learning approaches such as Bayesian Networks have re-emerged as relevant techniques. Highlighted by attributes such as their innate reasoning capabilities, making them explainable and interpretable, as well as their comparatively lower compute cost to neural networks, making them edge compliant for real-time processing needs [6], Bayesian Networks bring to bear all the requisite attributes to facilitate and solve next generation data fusion problems. This paper will review several relevant reasoning techniques, focusing specifically on Bayesian Networks, and their application to data fusion problems primarily in the air defense regime. Next, a prototype Bayesian Network-driven data fusion framework performing target identification and intent classification will be presented. Here, we examine several use cases showcasing the performance of Bayesian Networks in domain context and their ability to overcome data fusion challenges that neural network based approaches falter on.

2. BACKGROUND AND RELATED WORK

2.1 Historical Context

Despite advances in machine learning techniques, there remain numerous concerns about the use of AI on the battlefield, largely driven by the lack of explainability [3]. The lack of explainability is typically attributed to neural network driven approaches, with their size and complexity making the rationale behind outputs challenging to summarize, interpret, and explain [7]. There are several classes of interpretable Explanators that continue to be researched to improve the explainability of neural networks, encompassing the breadth of approaches including Local Interpretable Model Explanation (LIME), Layer-wise Relevance BackPropogation (LRP), and SHapely Additive ExPlanation (SHAP). Many of these approaches are computationally expensive and lack guarantees that optimal solutions or explanations are produced [8]. Another approach to improve the explainability, interpretability, and performance of neural network-based systems has been to directly couple symbolic reasoning or logical engines with neural networks themselves. This intersection is termed “neuro symbolic” reasoning and exists as a highly active area of research [7]. Example techniques such as DeepProbLog [9], Logical Tensor Networks (LTN) [10], or NeurASP [11] continue to mature but have yet to see widespread adoption. Very recently, LLMs have captivated many researchers exploring their ability to reason. A consensus has yet to be reached on LLMs ability to formally reason [12], yet, despite improvements to training procedures and prompting routines focusing on chain-of-thought to elicit reasoning-like behavior, the sheer size of LLMs and their neural foundations eliminate any form empirically validatable outputs, no matter how human-like or logical their outputs appear.

Before the proliferation of neural networks, there existed machine learning techniques grouped under the reasoning umbrella (also known as first-wave, rule-based, or symbolic reasoning [13]), which by nature are assumed to be explainable by virtue of their deterministic, repeatable, and interpretable logical sequences used to produce outputs. This class of reasoning has seen useful application through direct coupling to ontological systems, in many cases evolving into fully fledged knowledge graphs [14]. Some examples of deductive reasoning engines and their associated knowledge graphs include: grakn/TypeDB [15,16], GraphDB [17], and Stardog [18]. Many of these tools are built upon RDF [19] and OWL Semantic Web Standards [20].

In parallel, the class of probabilistic logical systems has remained a steadfast suite of approaches to perform reasoning, and the field continues to see mathematically grounded improvements. Despite producing outputs that may be perceived as functionally equivalent to deductive logic systems, probabilistic logic systems differ greatly in the use of prior information. Where purely deductive systems disregard prior information in the face of information presently available [21], probabilistic systems combine historical or prior data with current information to produce their outputs. Furthermore, at the human-machine interface level, probabilistic values are typically preferred by humans [22] despite our biological inability to truly comprehend what a probabilistic measure actually means [23]. Examples of relevant probabilistic logic systems include approaches grounded in the Dempster-Shafer theory, extending to Probabilistic Argumentation Systems, as well as Probabilistic Graphical Models as the parent class that Bayesian Networks fall under.

Bayesian networks present themselves as a highly flexible, interpretable, lightweight, and operationally robust tool capable of performing reasoning, also suitable for use in fusing and integrating data from various levels of abstraction. Bayesian networks are probabilistic graphical models composed of nodes representing random variables, and edges denoting their relationships and conditional probabilities for corresponding nodes [6], of which there is extensive literature. These probabilities may be found empirically, populated manually, or intelligently determined by heuristics or other offline approaches. Differing themselves from deductive reasoning engines and knowledge graphs, these prior values implicitly ensure operational robustness and guarantee the ability to run inference in the absence of observables, should an observable producer (such as a sensor, or Automatic Target Recognition (ATR) system) become unavailable at inference time. Furthermore, through the hierarchical relationships of the network, Bayesian networks can be implemented in a hierarchy mimicking the abstraction levels of all the data available from the observables producers (subsystems) that we strive to integrate. Functionally, this means that very low level sensor readings from a radar system, for example, can be integrated *directly* with a high level object detection or automatic target recognition system, to produce any number of classifications or decisions. This capability alone should theoretically make Bayesian networks the pre-eminent technique to perform sensor, data, and information fusion across a variety of data levels as defense systems continue to increase in complexity and interconnectedness, their innate reasoning and explainability notwithstanding.

2.2 The Air Defense Regime and Previous Application of Bayesian Networks

Transitioning our focus now to examine the air defense regime specifically, data streams from multiple sensors are typically fused together [24, 25] at different levels to perform three core tasks: detection, tracking, and classification, which are then used to perform higher level tasks such as intent classification, situational awareness, and impact assessment [26]. In the past, these tasks were performed in the paradigm of X-then-Y (e.g., "track-then-classify") architecture, which was effective, but does a poor job leveraging all available information in the system. Specifically, there exist couplings between the capabilities and intents of different targets and the known kinematic and dynamics of targets, that if backpropagated to the tracking layer, would provide valuable information to improve the tracker.

Several Bayesian approaches have been proposed to perform threat evaluation of aerial targets, which typically focuses on the problem frames of identification and classification of targets with respect to defended assets in the area [27, 28]. Many of these approaches have been augmented by Dynamic Bayesian Networks (DBNs) as well [29], in which the temporally accommodating aspects of DBNs are better suited to the continuous time nature of air defense. Common across these approaches is using Bayesian Networks to process and fuse extracted stateful and discretized information about targets, such as distance, altitude, speed, and effective threat range [27–30]. The Joint Target Tracking, Classification, and Intent (JTCI) framework was a recently proposed approach, in which the tasks of tracking, classification, and intent (inference) are performed simultaneously [26]. The JTCI relies on two sources of sensor information, a radar and electronic support measure (ESM), which are then processed within a Bayesian Network and leverages several state-transition models to fuse information from task specific models.

While the JTCI is one of the first frameworks to perform multi-task inference simultaneously, it builds on a legacy of using Bayesian Networks to support air defense missions. At the lower sensor processing level, Bayesian filters have been used to perform single and multi-target detection and tracking. Here, Bayesian filters are capable of leveraging information extracted from radar, sonar, and optical sensors and are capable of modeling both linear and non-linear relationships [31]. The ability to handle non-linear relationships makes Bayesian approaches much more appealing than traditional Kalman filtering for cases where a Gaussian distribution of the system cannot be assumed [31, 32]. Because of this flexibility, Bayesian techniques have also been applied to numerous other domains requiring detection and tracking functionality, such as space situational awareness [33], air traffic control and runway operations 34,35, ground vehicle tracking 36,37, IoT device tracking 38, and personnel/figure tracking 39, among others.

3. PROPOSED BAYESIAN NETWORK

Taking inspiration from and building on the above techniques and approaches, we will now introduce and explain a prototype Bayesian Network-driven air defense object and intent classification system. The system consists of three main constructs: the available features (observable and derived), the Bayesian Network structure itself, and the determination of conditional probabilities for each node in the network. Each of these components will be discussed in depth below.

3.1 Features and Network Design

Beginning with the overall problem frame, and final output of the system, is the intent classification of a detected object in the hypothetical air defense area of operation. For our purposes, three possible discrete intent modes were identified: a travel/cruise mode, an attack mode, and an evasive/neutralized mode 26.

- The travel/cruise mode is characterized by objects that do not presently pose a threat and are moving into position to execute their mission.
- The attack mode indicates the object is about to cause or presently causing harm to the defended area.
- The evasive/neutralized mode means the object is either currently under engagement or has been successfully engaged and is not likely to become a threat soon.

To make this intent classification, there are several useful features we can define to condition the likelihood of each class on. First and foremost is the object/platform type, which is the secondary problem frame addressed here (and its determination will be discussed in the next section). In the hypothetical scenario this system addresses, it is expected that four platform types will be operating in the area: missiles, fighter jets, bombers, and UAVs. Given that each of these platforms poses a different kind of threat, and will position themselves differently for their preferred attack method, this is vital information for ultimately determining the object's intent.

However, knowing that a fighter or a bomber is in the area is not enough information alone, so three other features are used in conjunction with it, as shown in Figure 1. The first two are considered low-fidelity general readings: the range and altitude of the detected object. Range and altitude are useful features here because further away and higher altitude objects are less threatening, and each of the possible platforms operating in the area will tend to be observed at different altitudes and ranges depending on their intent. Range values have been discretized to "far", "medium", or "near", and altitude similarly was discretized to "high", "medium", or "low". In addition to these two, the speed of the object can also be determined. This is considered a high-fidelity measurement which is informed by two sensors in the system. The determination of speed will be discussed below, but for the purposes of intent classification each platform will operate at an expected speed depending on its intent mode and mission.

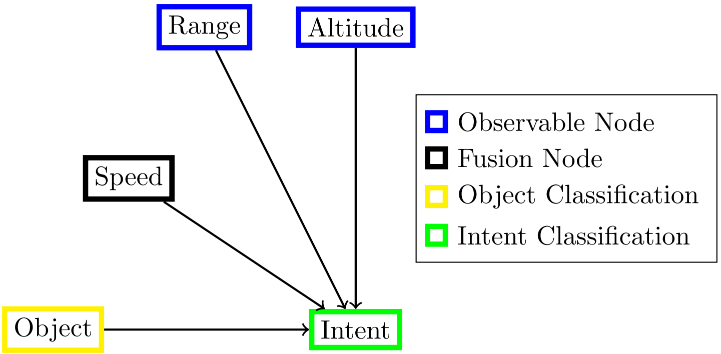

Figure 1. Intent input nodes and states.

Returning to the object/platform type determination, like the intent determination, this is conditioned on multiple input variables as shown in Figure 2. In this case three parameters are used: an altitude observation, a speed measurement, and a size measurement. Like the speed measurement, the size measurement is another high-fidelity measurement also informed by two sensors in the system. Size was discretized to “large”, “medium”, and “small”, and speed was discretized to “fast”, “medium”, and “slow”.

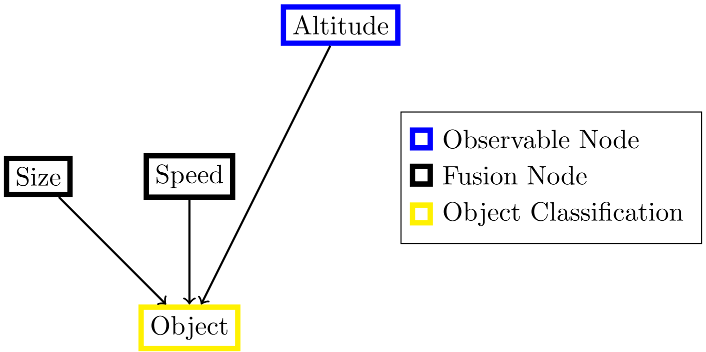

Figure 2. Object Classification input nodes and states.

To properly explain the speed and size measurements, we will now review the input side of the network and discuss the available sensor systems. Here, hypothetical readings from three different sensor systems will be used:

- An optical camera
- An infrared (IR) sensor
- A radar system

These sensor systems were selected because of the variety of ranges, altitudes, and weather conditions they are most effective (or ineffective) in, and to help compensate for the shortcomings of the other sensors. Here, the camera is capable of observing object size, the IR sensor can observe the object speed, and the radar system can observe both size and speed. However, given the deceptive nature of warfare, we cannot always trust the observations of a sensor system. Taking stealth fighters for instance, the radar profile of an advanced stealth fighter may lead to an incorrect radar observation of a very small or undetectable object, but that same stealth fighter is fully visible to an optical camera system. Because of this, the raw observations from all sensors are combined with the observation from another sensor to make a final measurement. This is done for both size and speed, as seen in Figure 3.

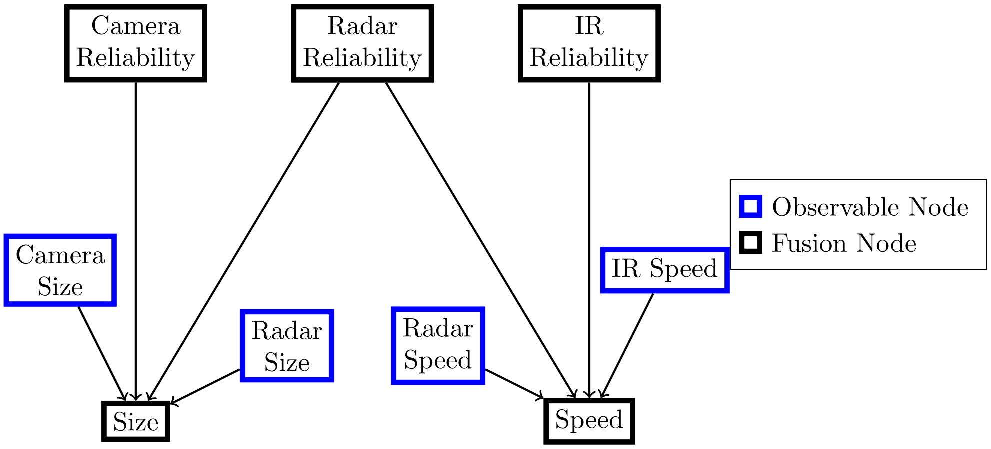

Figure 3. Size and Speed input nodes and states.

Additionally, each of these sensors will perform differently at different ranges and altitudes, and inclement weather in the area will also degrade the performance of each sensor differently. So in addition to combining the observations of each sensor, the reliability or trustworthiness of each sensor is also used to condition the final measurement for size and speed, as seen in Figure 4. For this scenario, the camera can be most trusted at near and medium ranges and altitudes. The IR sensor can be most trusted at high altitudes (where there is less atmosphere, so temperature differentials are greater). And the radar system is highly reliable for all ranges and altitudes, with slight degradation at far range. Under inclement weather conditions however, the camera is severely handicapped to short range and low altitudes only. The IR sensor gains improvement at medium altitudes and the radar system receives a blanket degradation at all ranges and altitudes.

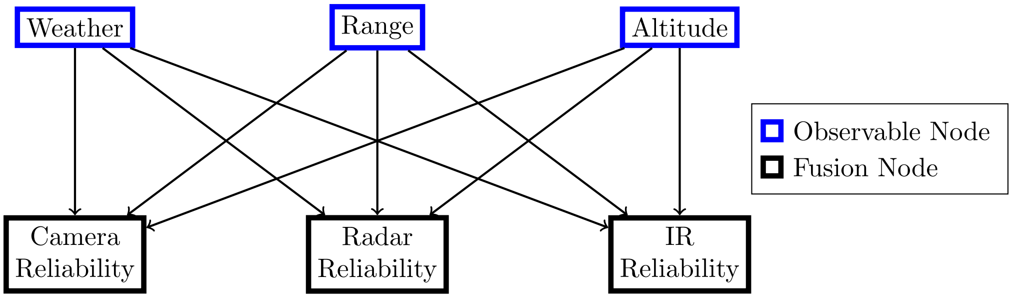

Figure 4. Sensor Reliability input nodes and states.

With each of the functional components of the Bayesian Network defined, as well as the edges connecting each network node/feature, Figure 5 below shows the full network structure.

3.2 Conditional Probability Distributions

In practice, one would use empirical data to populate the values of the priors, however for the purpose of this research we developed our own priors. Different approaches were taken to assign priors or conditional probability values to each node in the network. Beginning first with the observable nodes: weather, range, and altitude, it is expected that these will all be observed and in the test cases to follow. Because of this, their conditional probability distribution (CPD) values are largely non-consequential, however some logic was used to fill them out. The weather node was filled out to represent an environment where 75% of the time the weather is clear, and 25% it is inclement, though this could easily be filled out with heuristic values for the operational region. For range, it is unlikely for an object to just “appear”, so it is reasonable to assign a higher probability to the “far” class as new objects will likely be flying in from outside of range, and “medium” less likely than “far”, and “near” less likely than “medium”. Altitude is assigned an equal probability to each class.

Next, the raw sensor observation node CPDs were filled out. For size class observations with possible values of “large”, “medium”, and “small”, these were filled out by logic of the opposing force platform distribution. In this case, the majority of the platforms are of size “medium”, followed by “small”, making “large” vehicles the lowest likelihood reflecting the smallest portion of force. This logic is applied to both the camera observation of size, and the radar observation of size, and these values could easily be updated by heuristic or real world data.

After this, the sensor reliability nodes were filled out in accordance with the optimal sensor operation conditions. To reiterate, the camera is most reliable at near range and low altitude, and under clear conditions. The radar is slightly negatively impacted by range, but performs generally well over all altitudes, and inclement weather reduces reliability by 15% across all ranges and altitudes. The IR sensor is positively impacted by altitude, regardless of range, and inclement weather improves its reliability for objects at medium altitudes. These reliability characteristics are based on intuition and meant to highlight the potential operational differences between sensors, not represent highly accurate sensor profiles.

For the class of size and speed measurements, which are both conditioned by the sensor reliability nodes and the raw observation nodes, the logic for filling these CPDs out is as follows. If the sensor is reliable, we trust its measurement more than a not-reliable measurement. Additionally, if both sensor observations agree, we have the highest possible confidence in the agreed classification. If the sensors disagree, but have adjacent classes (e.g.

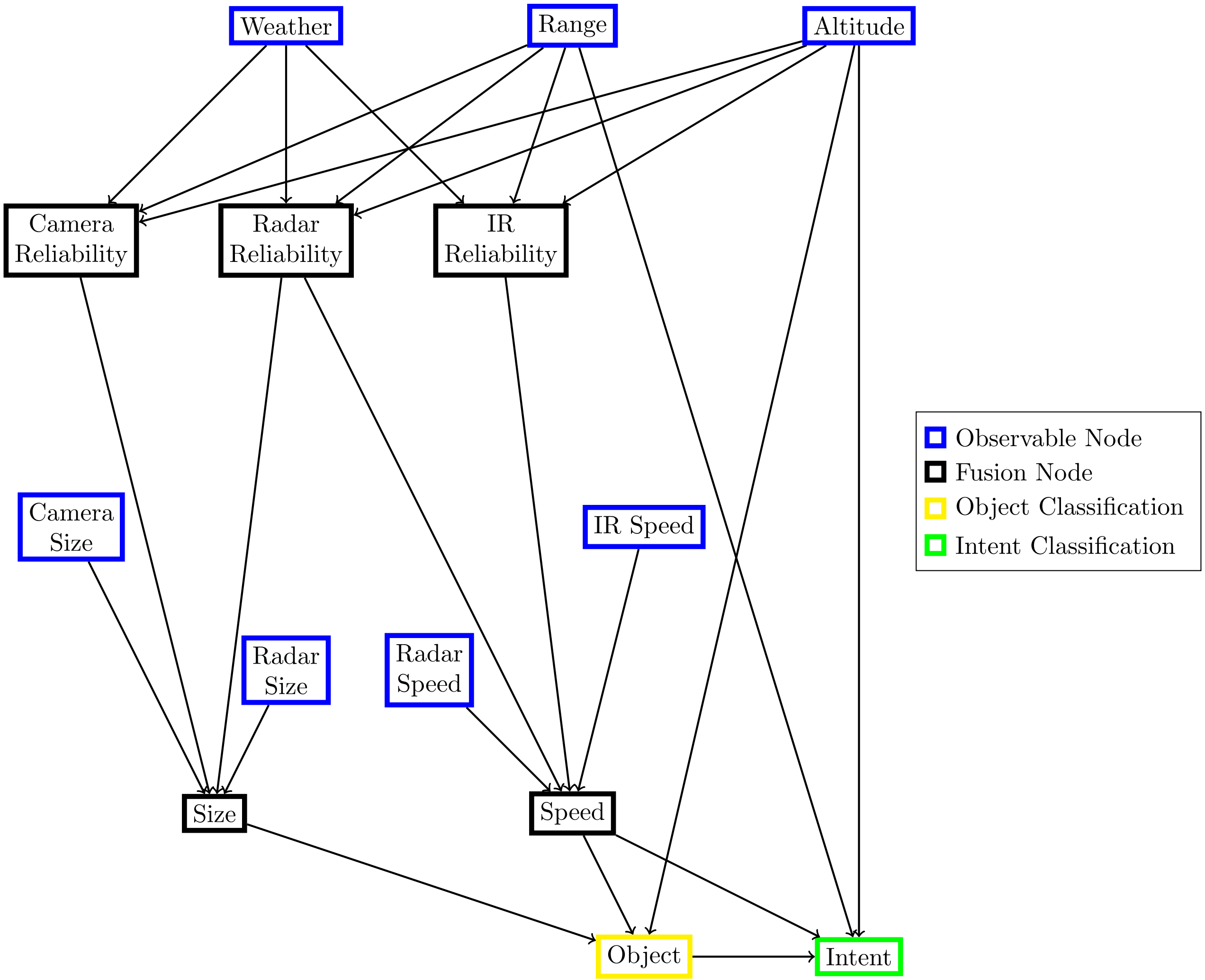

Figure 5. Full Bayesian Network architecture.

large and medium, or medium and small) the probability mass is split across the two, favoring the more reliable sensor observation. For disagreements of non-adjacent classes (large and small), one or both sensors is clearly wrong, so the probability mass is spread evenly while slightly favoring the more reliable sensor's observation.

For the object/platform type CPD, an algorithmic approach was taken to produce the probabilities. Here, for each possible platform type for each conditioning node/feature was marked as having a possible reading for that feature. Taking the fighter for example, it can be observed at all altitudes, its size will either be small or medium, and its speed will be fast or medium. Knowing these possible operating conditions, a routine was developed to assign probabilistic mass for each conditional scenario.

The same logic was applied to generate the final intent classification node CPD, with an additional feature class control loop for the platform type. It is also important to note here that this method of CPD generation could easily be augmented with a first order rule base. Such a rule base could be created and maintained on a database of past engagements allowing for a regularly updated and re-generated CPDs.

4. EXAMPLE TEST CASES

To showcase the utility of the proposed network, we present four test cases defined to highlight the performance of the network in a variety of scenarios. We begin by presenting the network outputs with no observables given as a baseline. The following detail the formal test cases performed:

1. We inspect the results of the network when no observations are supplied.
2. We observe features consistent with a bomber in attack, and discuss how to interpret the tabular results.
3. We make the problem more challenging by introducing disagreements in sensor readings and degrading their performance to showcase the network's ability to reason through uncertainty and reach the correct solution.
4. We simulate two sensor units being brought completely offline, and assess the network's ability to reliably handle the existence of or lack of observables and consistently produce results.
5. We show how an external system capable of classifying objects may be integrated and how its outputs impact the network. This showcases the extensibility and interoperability of Bayesian networks and how their native interfaces enable them to easily accept readings from any system producing observables in the correct format.

The general pattern for test cases is:

- Describe the scenario being emulated, and declare the assumptions and configurations of the trial.
- Present the relevant values of the Bayesian Network as impacted by the configuration
- Discuss important values of the table that have changed, or stayed consistent, as well as the implications of the observed behavior toward mission-oriented quality attributes.

4.1 Test Case 1 - Network Baselining - No Observations

Before diving into specific test cases and scenarios, we will first review outputs of the network when no evidence has been supplied, as shown in Table 1. It should be noted that these values result from the network structure and the processes for producing priors in the absence of empirical data. The purpose of this is to provide a relative starting point for assessing the various scenarios under the assumptions made for this paper. Here, we see that of the four possible objects that can be classified and it is effectively equal probability between each of the options. However, for intent classification, the cruise intent is notably higher than attack and evade/neutralized. Given the lack of observations, this assessment is reasonable as objects operating in the area will spend a disproportionate amount of time moving into or out of position for an attack. This rationale holds consistent for all object and intent combinations, except for missiles which have attack as the highest likelihood. This is also not surprising because while missiles will cruise into position, they will not idly cruise without an attack being the final objective, unlike the other traditional aircraft options.

Table 1. Results when no Observations present

Observations	
Conditions	none
Range	none
Altitude	none
Size - Camera	none
Size - Radar	none
Speed - Radar	none
Speed - IR	none

Node	Class	Probability
Object	missile	0.257
	fighter	0.257
	bomber	0.239
	uav	0.246
Intent	cruise	0.439
	attack	0.296
	evade/neut	0.265

Object	Intent	Probability
Missile	attack	0.111
	cruise	0.088
	evade	0.058
Fighter	cruise	0.112
	attack	0.073
	evade	0.073
Bomber	cruise	0.106
	attack	0.066
	evade	0.067
UAV	cruise	0.111
	attack	0.068
	evade	0.067

4.2 Test Case 2 - Bomber in Attack

For this scenario, we define a basic scenario in which a bomber is preparing for an attack run. Consistent with the definitions used to produce the CPDs, bombers in this scenario are defined as larger objects that typically travel at medium speeds. When performing an attack, bombers in this scenario will be at close range, and typically operating at a medium altitude. We supply these values as inputs to the network, which are shown under the Observations section in Table 2.

Table 2. Test Case 2 Observations and Results

Observations	
Conditions	clear
Range	near
Altitude	medium
Size - Camera	large
Size - Radar	large
Speed - Radar	medium
Speed - IR	medium

Node	Class	Probability
Object	missile	0.203
	fighter	0.203
	bomber	0.348
	uav	0.245
Intent	cruise	0.233
	attack	0.466
	evade/neut	0.301

Object	Intent	Probability
bomber	attack	0.201
uav	attack	0.100
fighter	attack	0.091
uav	evade	0.084
bomber	evade	0.079
missile	attack	0.075
missile	evade	0.070
bomber	cruise	0.068
fighter	evade	0.067
uav	cruise	0.061
missile	cruise	0.058
fighter	cruise	0.045

By supplying these values, we go into the scenario expecting the bomber to be resolved as the most likely object and a bomber in attack to be the most likely object-intent classification value. As we see in Table 2, the bomber has received 35% of the probability mass for objects, which is a 10.9% absolute increase or 145.6% relative increase in likelihood compared to the network baseline. Furthermore, the object-intent classification value of bomber in attack has increased absolutely 13.5% and 304.5% relatively, containing nearly 2x the probability mass of the next most likely object-intent classification of UAV in attack. Given that the highest stand-alone intent value was attack at 46.6% of the probability mass, it is unsurprising to see a UAV and fighter in attack being the next most likely object-intent classifications. However, this is only unsurprising because of the level of visibility and interpretability that Bayesian networks give us.

4.3 Test Case 3 - Bomber with Stealth under Inclement Conditions

In this scenario, we still keep in mind a bomber performing an attack run given mostly the same observable values, however we want to see how the network performs when inconsistent readings arise or sensor conditions are degraded. Here, we assume the bomber in question is a stealth bomber, and thus will have a much smaller radar profile than a non-stealth counterpart. However, because of the redundancy of sensors in the fusion network, the optical sensor still observes the object at its true size of large. Furthermore, we introduce inclement conditions that have different impacts to the reliability of sensors measuring different items, shown in Table 3.

When supplying the network with these observables, see several interesting outputs. First, we see that the bomber is no longer the highest likelihood object, though it remains a close second to the UAV. The intent of attack still owns the largest share of the probabilistic mass, however. We might expect that this would lead to the highest likelihood object-intent classification being UAV in attack, however the bomber in attack remains as the most likely classification. While the confidence in this classification is much lower, at only 14.9% of the probabilistic mass, or 134.2% of the next most likely class (UAV in attack), the network is still very confident in the determination. These results affirm the ability for a properly constructed Bayesian network to successfully reason through inconsistent sensor readings and challenging situations expected to be encountered in complex and high stakes environments.

Table 3. Test Case 3 Observations and Results

Observations	
Conditions	inclement
Range	near
Altitude	medium
Size - Camera	large
Size - Radar	small
Speed - Radar	medium
Speed - IR	medium

Node	Class	Probability
Object	missile	0.234
	fighter	0.234
	bomber	0.261
	uav	0.271
Intent	cruise	0.235
	attack	0.452
	evade/neut	0.313

Object	Intent	Probability
bomber	attack	0.149
uav	attack	0.111
fighter	attack	0.105
uav	evade	0.093
missile	attack	0.087
missile	evade	0.082
fighter	evade	0.078
uav	cruise	0.067
missile	cruise	0.065
bomber	evade	0.060
fighter	cruise	0.052
bomber	cruise	0.051

4.4 Test Case 4 - Network Sensitivity to Offline Sensors

In addition to the network's ability to reason through disagreements in sensor observations and accommodate various sensor performance profiles under degraded environmental weather conditions, the network is also capable of handling one or more sensor systems being taken offline during operation. To showcase this, we explore how consistently the network produces observations when one or more sensing systems are taken offline and unable to supply observations. Here, we create two groups of comparison: first, the optical size sensor against the radar size sensor, and second, the radar speed sensor against the IR size sensor. For every combination of condition, range, and altitude, the object and intent pairing probability value is produced. In the case of the size sensors, we produce outputs for the optical sensor while the radar is offline (and vice versa), and in parallel produce outputs for the radar while the optical sensor is offline (and vice versa). The difference of probabilistic mass between the two readings for each object and intent pairing is recorded as a sample. Table 4 reports the mean absolute difference (MAD) and standard deviation (STD) of the probabilistic mass across both groups for each object intent pair, as a percent of 100, and Figure 6 shows the median and quartile ranges of the relative difference.

Table 4. Mean absolute difference (MAD) and STD of Object, Intent pairs as percent of 100

Object, Intent	MAD	STD
bomber, cruise	0.626	0.810
bomber, evade	0.623	0.598
bomber, attack	0.571	0.542
missile, attack	0.552	0.507
fighter, evade	0.458	0.429
missile, cruise	0.413	0.342
UAV, evade	0.341	0.298
bomber, attack	0.304	0.244
fighter, cruise	0.287	0.293
UAV, cruise	0.287	0.265
fighter, attack	0.260	0.195
missile, evade	0.623	0.598

As we see in Table 4, the maximum MAD across all object intent pairs is 0.626% (on a scale of 100) for a bomber in cruise, while the minimum is 0.232% for a missile in evade/neutral. For 8 of the 12 object intent pairs, the MAD combined with one standard deviation is less than 1% probabilistic mass shift. These results show that even if one sensor producing speed or size goes offline, as long as one of the other sensors redundantly producing the same observable class remains operational, we can expect the network to classify objects and intents with 99% consistency to the optimal scenario where all sensor units are producing observations. Ultimately these results show that not only can Bayesian networks gracefully handle the loss of observations from integrated sensor units, they continue to produce results with high consistency, a system attribute that builds trust and ensures success in highly dynamic and uncertain operational environments.

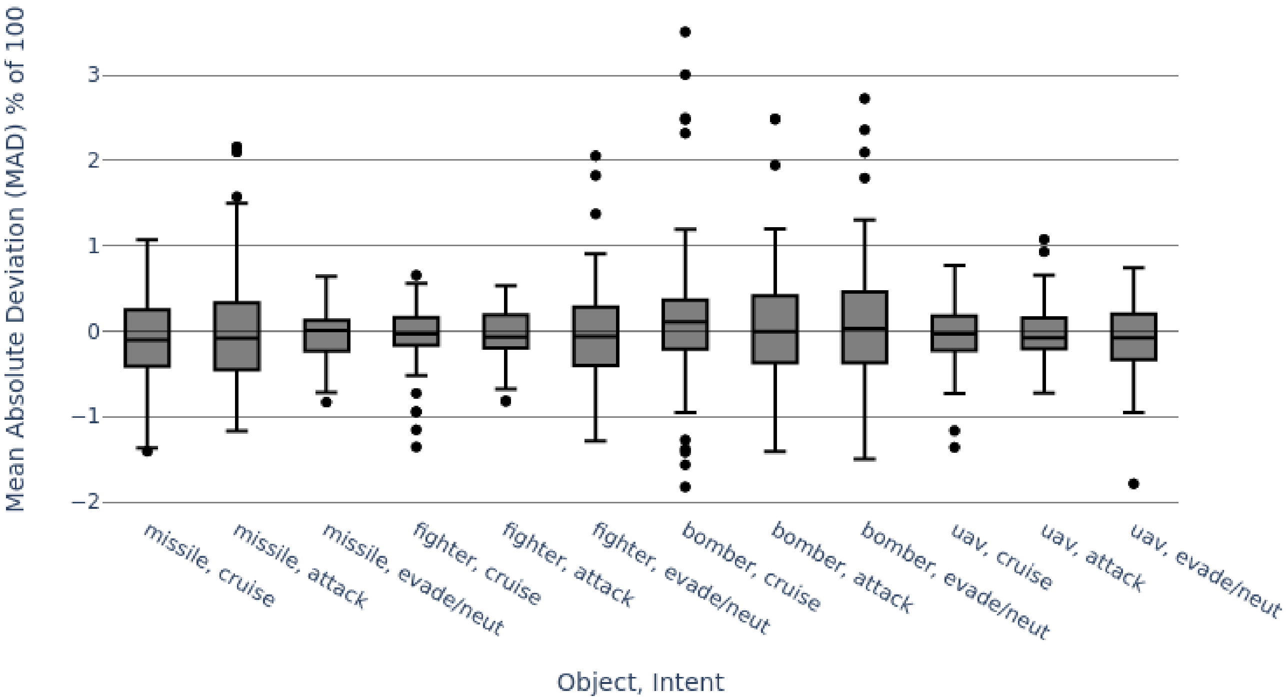

Figure 6. MAD probability shift for various sensors offline.

4.5 Test Case 5 - Externally Resolved Object

Finally, we consider a scenario where we wish to extend our base Bayesian network to include observables from a system that is not originally part of the fusion network. In this case, we assume there exists an external Automatic Tracking and Recognition (ATR) system producing high fidelity object classifications. While we have selected an ATR system for this test case, any system that produces values of the same type that the network uses could be operated on, such as a domain specific knowledge base, or operator contextual knowledge.

Given a "known" observed object type, we can directly plug the value into the Bayesian network by setting the observed value of the object node. Not only does this observable propagate information forward to the final intent classification, the observable also conditions the input nodes to the object table. In this case we say that we have observed the conditions as clear, range as near, altitude as medium, and both speed sensors as medium. Table 5 shows the final inferred intent values when our hypothetical ATR system observes each of the possible objects the system has awareness of, as well as the changes to the unobserved size node.

Table 5. Observations and inferred Size and Intent when integrating ATR Object observations

Observations		Inferred Size Value, by Object from ATR				Inferred Intent			
Conditions	clear	Object	Large	Med	Small	Object	Cruise	Attack	Evade
Range	near	uav	0.197	0.428	0.374	missile	0.532	0.442	0.025
Altitude	medium	bomber	0.311	0.441	0.247	fighter	0.515	0.333	0.152
Speed - Radar	medium	fighter	0.187	0.426	0.387	bomber	0.435	0.535	0.030
Speed - IR	medium	missile	0.187	0.426	0.387	uav	0.403	0.349	0.248

We see that despite observing the same non-object parameters, that observing the object has a unique impact on each of the intents for a given object type. For the upstream size node, we see that observing a bomber shifts the probabilistic mass toward the size being large which is consistent with the assumptions we made about the size of each object class, but has less of an impact on the other object types. The lack of separation is based on the routines used to generate the CPD table priors, but what is important is the ability to impact these values is present in the mechanics of Bayesian networks. This ability for downstream node values to impact upstream nodes could be beneficial if any undeclared consumers of different sections of the network were reliant on the size node specifically, without having access to the object node. As such, any piece of information that we supply to the network reduces uncertainty of the system as a whole, and the interfaces of Bayesian networks enable us to easily fuse relevant information from sources not included in the original network design.

5. CONCLUSION

In this work we presented a novel Bayesian network tasked with classifying the object type and intent of objects operating in hypothetical air defense scenarios. In addition to the Bayesian network design itself, we also characterized the performance of Bayesian networks with respect to quality attributes relevant to operationalizing AI and ML solutions in the defense domain through several test cases.

We showcased how the classifications made by Bayesian networks are intuitive to interpret and understand, by virtue of being probabilistically grounded, which is a useful attribute for systems deployed in defense settings and something that neural networks cannot accommodate. Furthermore, we showed how Bayesian networks are capable of reasoning through inconsistent readings from multiple sensors, and how we can design networks to prioritize readings from sensors operating in their most optimal conditions. We also showed the ability of Bayesian networks to gracefully handle subsystems going offline and their ability to reliably produce consistent classifications in the absence of subsystem observations. And finally, we explored the interfaces by which we can integrate observations from external systems not originally part of the network architecture and how these external readings can reduce uncertainty and improve classifications of the system. This also demonstrates the ability for Bayesian networks to coexist with other neural network-based, black box, or unexplainable models, and how Bayesian networks can perform last mile reasoning over information produced by a variety of systems.

An area of future research would be to draw from the field of Control Theory and consider how subsystems operating at different frequencies would impact the availability of observables. Here, different sensor systems and different decision making algorithms in the system are likely capable of producing measurements or decisions at varying computational rates. Knowing this, it may be possible to design a Bayesian network made up of several "inner" and "outer" control loops where, as information becomes available from faster subsystems, these are used to update the priors of slower outer loops. And, as the higher fidelity outer loops complete their execution, feed these outputs back as priors into the inner loops. Such an architecture would facilitate critical information about the state of the environment being made useful as soon as it comes available. This addresses computational restrictions or inefficiencies that may inadvertently relegate a system to becoming a batch processing routine that blocks until all new measurements become available.

REFERENCES

[1] Danzig, R., "Technology roulette: Managing loss of control as many militaries pursue technological superiority," (2018). (Accessed: 2 August 2024).

[2] Allen, G., "Understanding ai technology," (2020). (Accessed: 2 August 2024).

[3] Gunning, D. and Aha, D., "Darpa's explainable artificial intelligence (xai) program," *AI Magazine* **40**, 44–58 (Jun. 2019).

[4] DARPA, "DARPA Perspective on AI." Online https://www.darpa.mil/about-us/darpa-perspective-on-ai. (Accessed: 15 November 2022).

[5] Qiu, S., Liu, Q., Zhou, S., and Wu, C., "Review of artificial intelligence adversarial attack and defense technologies," *Applied Sciences* **9**(5) (2019).

[6] Yang, X.-S., "2 - mathematical foundations," in [*Introduction to Algorithms for Data Mining and Machine Learning*], Yang, X.-S., ed., 19–43, Academic Press (2019).

[7] Shakarian, P., Baral, C., Simari, G. I., Xi, B., and Pokala, L., [*Neuro Symbolic Reasoning and Learning*], Springer Nature Switzerland (2023).

[8] Saleem, R., Yuan, B., Kurugollu, F., Anjum, A., and Liu, L., "Explaining deep neural networks: A survey on the global interpretation methods," *Neurocomputing* **513**, 165–180 (2022).

[9] Manhaeve, R., Dumancic, S., Kimmig, A., Demeester, T., and Raedt, L. D., "Deepproblog: neural probabilistic logic programming," in [*Proceedings of the 32nd International Conference on Neural Information Processing Systems*], *NIPS'18*, 3753–3763, Curran Associates Inc., Red Hook, NY, USA (2018).

[10] "Logic tensor networks," *Artificial Intelligence* **303**, 103649 (2022).

[11] Yang, Z., Ishay, A., and Lee, J., "Neurasp: embracing neural networks into answer set programming," in [*Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence*], *IJCAI'20* (2021).

[12] Kambhampati, S., "Can large language models reason and plan?," *Annals of the New York Academy of Sciences* **1534**, 15–18 (Mar. 2024).
[13] DARPA, "Knowledge-directed artificial intelligence reasoning over schemas (kairos)." Online https://www.darpa.mil/program/knowledge-directed-artificial-intelligence-reasoning-over-schemas. (Accessed: 2 August 2024).
[14] Zhang, J., Chen, B., Zhang, L., Ke, X., and Ding, H., "Neural, symbolic and neural-symbolic reasoning on knowledge graphs," *AI Open* **2**, 14–35 (2021).
[15] "grakn." Online https://github.com/LuoXiaoHeics/grakn. (Accessed: 2 August 2024).
[16] "Typedb." Online https://typedb.com/. (Accessed: 2 August 2024).
[17] "Graphdb." Online https://graphdb.ontotext.com/documentation/10.0/reasoning.html. (Accessed: 2 August 2024).
[18] "Stardog." Online https://docs.stardog.com/inference-engine/advanced-reasoning-features. (Accessed: 2 August 2024).
[19] "Rdf." Online https://www.w3.org/RDF/. (Accessed: 2 August 2024).
[20] "Owl." Online https://www.w3.org/OWL/. (Accessed: 2 August 2024).
[21] Gazzo Castañeda, L. E., Sklarek, B., Dal Mas, D. E., and Knauff, M., "Probabilistic and deductive reasoning in the human brain," *NeuroImage* **275**, 120180 (2023).
[22] Heath, C. and Tversky, A., "Preference and belief: Ambiguity and competence in choice under uncertainty," *J. Risk Uncertain.* **4**, 5–28 (Jan. 1991).
[23] Kahneman, D. and Tversky, A., "Prospect theory: An analysis of decision under risk," *Econometrica* **47**(2), 263–291 (1979).
[24] Maltese, D. and Lucas, A., "Data fusion: quite silent search function in naval air defense," in [*Infrared Technology and Applications XXV*], Andresen, B. F. and Strojnik, M., eds., **3698**, 36 – 47, International Society for Optics and Photonics, SPIE (1999).
[25] Maltese, D. and Lucas, A., "Data fusion: principles and applications in air defense," in [*Signal Processing, Sensor Fusion, and Target Recognition VII*], Kadar, I., ed., **3374**, 329 – 336, International Society for Optics and Photonics, SPIE (1998).
[26] Zhang, W., Yang, F., and Liang, Y., "A bayesian framework for joint target tracking, classification, and intent inference," *IEEE Access* **7**, 66148–66156 (2019).
[27] Basso Brancalion, J. F. and Kienitz, K. H., "Threat evaluation of aerial targets in an air defense system using bayesian networks," in [*2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*], 897–900 (2017).
[28] Johansson, F. and Falkman, G., "A bayesian network approach to threat evaluation with application to an air defense scenario," in [*2008 11th International Conference on Information Fusion*], 1–7 (2008).
[29] Wang, Y., Sun, Y., Li, J.-Y., and Xia, S.-T., "Air defense threat assessment based on dynamic bayesian network," in [*2012 International Conference on Systems and Informatics (ICSAI2012)*], 721–724 (2012).
[30] Wang, X., Zuo, J., Yang, R., Zhang, Z., Yue, L., and Liu, H., "Target threat assessment based on dynamic bayesian network," *Journal of Physics: Conference Series* **1302**, 042023 (aug 2019).
[31] Bell, K., Corwin, T., Stone, L., and Streit, R., [*Bayesian Multiple Target Tracking, Second Edition*] (2013).
[32] Alin, A., Butz, M. V., and Fritsch, J., "Tracking moving vehicles using an advanced grid-based bayesian filter approach," in [*2011 IEEE Intelligent Vehicles Symposium (IV)*], 466–472 (2011).
[33] Wainscott-Sargent, A., "Dod's increasing demand for data fusion in space," (Feb 2023).
[34] Ye, X., Kamath, G., and Osadciw, L. A., "Using bayesian inference for sensor management of air traffic control systems," in [*2009 IEEE Symposium on Computational Intelligence in Multi-Criteria Decision-Making(MCDM)*], 23–29 (2009).
[35] Ayra, E. S., Ríos Insua, D., and Cano, J., "Bayesian network for managing runway overruns in aviation safety," *Journal of Aerospace Information Systems* **16**(12), 546–558 (2019).
[36] Dellaert, F. and Thorpe, C., "Robust car tracking using kalman filtering and bayesian templates," in [*Proceedings of SPIE Intelligent Transportation Systems*], **3207**, 72 – 83 (January 1998).
[37] Elfring, J., Appeldoorn, R., and Kwakkernaat, M., "Multisensor simultaneous vehicle tracking and shape estimation," in [*2016 IEEE Intelligent Vehicles Symposium (IV)*], 630–635 (2016).
[38] Zhang, W., Zhang, J., Bao, M., Zhang, X.-P., and Li, X., "Multitarget tracking based on dynamic bayesian network with reparameterized approximate variational inference," *IEEE Internet of Things Journal* **9**(13), 11542–11559 (2022).
[39] Pavlovic, V., Rehg, J., Cham, T.-J., and Murphy, K., "A dynamic bayesian network approach to figure tracking using learned dynamic models," in [*Proceedings of the Seventh IEEE International Conference on Computer Vision*], **1**, 94–101 vol.1 (1999).