IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 23, 2020, accepted August 28, 2020, date of publication September 1, 2020, date of current version September 15, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.3020814*

# Approximate Reasoning Based on IFRS and DS Theory With Its Application in Threat Assessment

**YANLI LU, XIAOLI LEI, ZHIPING ZHOU, AND YAFEI SONG, (Member, IEEE)**
College of Air and Missile Defense, Air Force Engineering University, Xi'an 710051, China

Corresponding authors: Xiaoli Lei (afeu_lxl@163.com) and Zhiping Zhou (afeu_zzp@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61703426, in part by the China Postdoctoral Science Foundation under Grant 2018M633680, and in part by the Young Talent Fund of University Association for Science and Technology, China, under Grant 20190108.

**ABSTRACT** Threat assessment for aerial attack targets is an important aspect of air defense weapon systems in responding to multiple attacks. We establish a model based on intuitionistic fuzzy rough sets (IFRS) and D-S evidence theory for threat assessment from the required data with uncertainty in stages. Using the overall degree of dependency and attribute importance of the intuitionistic fuzzy information system as a heuristic function, we study algorithms to extract threat elements and rules based on IFRS, to generate an intuitionistic fuzzy rule base for threat assessment with degrees of belief and disbelief. Based on the threat assessment rule base, we study the BPA determination algorithm in multi-stage threat assessment. The intuitionistic fuzzy semantics of degree of belief in the rule conclusion are used to determine the focal elements corresponding to each aggregate rule, and to obtain the degree of support of the data in a stage for each threat level. A case study shows that, compared to a threat assessment method based solely on D-S evidence theory or intuitionistic fuzzy reasoning, the advantage of IFRS knowledge acquisition makes the selection of threat assessment elements and determination of BPA more objective and less dependent on domain experts, so as to yield strong, objective results.

**INDEX TERMS** Threat assessment, intuitionistic fuzzy sets, D-S evidence theory, intuitionistic fuzzy rough sets.

## I. INTRODUCTION

Threat assessment (TA) is at the third level of the JDL information fusion model. It quantifies the ability of an enemy's military deployment or weaponry to pose a threat, along with the enemy's possible action intention. This level of fusion receives output from the situation assessment level as the input, and outputs the view of threat, which describes the enemy's target positions and threat levels as the basis for subsequent weapon-target allocation. For a regional air defense system with limited deployment, facing many types of incoming aerial attack targets, classifying a target of high-threat level as a low-level threat and a target of low-threat level as a high-level threat could lead to the targets posing the fatal threat to the air defense system not being effectively intercepted. This may lead to missing the opportunity to defense and even to face catastrophic failure. Therefore, an important part of air defense combat decision-making is to accurately assess the threat level of an incoming aerial attack target.

The battlefield situation and threat assessment processes data at the decision-making level, and solves a specific domain problem based on the commander's battlefield knowledge and combat experience. Because of limited development in cognitive theory and the military background, research of battlefield-related situation and threat assessment has made limited progress. The lack of a unified theoretical system creates a bottleneck in battlefield information fusion research, which is gaining increased attention. A number of theories and methods are used in threat assessment research, such as the Bayesian network, [1] multi-attribute decision theory, [2], [3] case-based reasoning, [4] fuzzy reasoning, [5] and belief rule base [6] The Bayesian network [1] combines graph theory and Bayesian reasoning, and has a strong ability to deal with uncertainty. However, in application, threat elements are difficult to extract and a priori knowledge is difficult to determine. Based on the multi-attribute decision method, [2], [3] the weight of each attribute is generally

The associate editor coordinating the review of this manuscript and approving it for publication was Wajahat Ali Khan.

evaluated by experts, and values are assigned based on their professional knowledge and experience, which are subject to subjectivity and uncertainty. Furthermore, this method is incapable of self-learning, hence it adapts with difficulty to rapidly changing battlefield situations. The use of these methods reflects different perspectives and opinions of researchers, and there is no unified, generally accepted view.

A future air defense battlefield will face multi-batch, multi-direction, multi-latitude, and continuous saturation attacks in a complex electromagnetic environment. The research objectives of threat assessment vary and involve many factors. Past threat assessments assumed that complete threat information could be obtained, and they assumed a certain environment. However, it will be more difficult to obtain information in a complex electromagnetic attack environment. Lack of key data may make a threat assessment difficult to complete. Threat assessments in future air defense operations will be conducted in an uncertain environment. Based on available data, a threat assessment in an air defense operation gradually reaches a conclusion regarding the defense combat plan and level of threat through dynamic, step-by-step refinement. Most modern incoming aerial targets, especially hypersonic targets, are at high speed and have excellent maneuverability. Static assessment methods discard past observation data, making it difficult to fully analyze the overall characteristics of targets. Threat assessment is a dynamic information fusion process with uncertainty. It is a challenge to effectively assess threat levels based on continuously received information that is incomplete, inaccurate, or uncertain.

Precise processing is ineffective. Given the uncertainty in threat assessment, the solution must rely on cognitive uncertainty and fuzzy thinking [14], [15]. Zadeh proposed the concept of fuzzy sets (FS) [7] An important expansion, intuitionistic fuzzy sets (IFS), [2] can effectively overcome the shortcoming of the single degree of membership in Zadeh's fuzzy sets, and they show a clear advantage in many applications. IFS theory deals simply and effectively with complex systems, especially those with human intervention, and has been effectively applied to fields such as command and control and information fusion. However, the use of FS theory often relies on subjective threat assessment factors and judgement criteria, [3] and does not solve the problems of threat element selection and automatic discovery of decision knowledge. The rough sets (RS) [8] can effectively process uncertain information. It can remove irrelevant or unimportant attributes while maintaining the classification ability of the information system, derive refined information, and effectively support multiple steps in knowledge processing. The intuitionistic fuzzy rough sets (IFRS) [9]–[13] introduces IFS to an RS model, expanding data reduction and rule extraction to the field of fuzzy decisions to enhance flexibility and representativeness. Data analysis and automatic knowledge acquisition based on RS and IFRS have attracted much attention in the field of intelligent decision-making, providing new ideas and methods for the extraction of threat assessment factors and knowledge discovery in uncertain environments.

Dynamic information fusion in threat assessment requires the determination of threat level based on continuously received information that is incomplete, inaccurate, or uncertain. D-S evidence theory [16], [17] has inherent advantages in expressing uncertain and unknown situations. Its combination rules can synthesize knowledge or data from different data sources, and it is widely used in fields such as decision-level information fusion and research in equipment intelligence. However, for threat assessment under uncertainty, problems in D-S evidence theory, such as determination of basic probability assignment (BPA) [18]–[27] remain to be solved. To extract decision rules based on IFRS could be a breakthrough in solving this problem.

This paper presents a multi-stage threat assessment model and algorithms based on IFRS and D-S evidence theory. IFRS data analysis and knowledge reduction are used to obtain a threat assessment knowledge base. Using target attribute data acquired in stages and D-S evidence theory, we study a method to determine BPA based on the established threat assessment knowledge base, i.e., to obtain the degree of support for the threat level from the data in stages, and use the combination rule of evidence theory to synthesize the probability distribution functions of data in various stages to obtain the final threat assessment.

The rest of this paper is organized as follows. Section 2 introduces the relevant concepts of IFRS theory and D-S evidence theory. Section 3 proposes the knowledge reduction algorithms and the BPA generation method for a threat assessment information system by analyzing the problem and the factors affecting it, and presents a model based on IFRS and D-S evidence theory. Section 4 analyzes the effectiveness of our method through a case study. Section 5 presents our conclusions and proposes topics for further study.

## II. IFRS AND D-S EVIDENCE THEORY

### A. INTUITIONISTIC FUZZY ROUGH SETS

Let $U$ be a nonempty finite universe, and $R$ an intuitionistic fuzzy equivalence relation on $U$. $FAS$=$(U, R)$ is referred to as an intuitionistic fuzzy approximation space, and $F(U)$ represents the intuitionistic fuzzy subsets on $U$.

We apply $R$ to partition $U$ to obtain equivalence classes $U/R = \{F_1, F_2, \cdots, F_k\}$ of the intuitionistic fuzzy sets. Let the elements of $U/R$ construct the intuitionistic fuzzy set $X \in F(U)$. Then the resulting lower approximation $R^{-}X$ and upper approximation $R^{+}X$ are a pair of intuitionistic fuzzy sets on $U/R$,

$$R^{-}X(x) = \inf_{F_i \in U/R} \max\{1 - F_i(x), \inf_{y \in U} \max\{1 - F_i(y), X(y)\}\}$$
$$R^{+}X(x) = \sup_{F_i \in U/R} \min\{F_i(x), \sup_{y \in U} \min\{F_i(y), X(y)\}\}. \quad (1)$$

For $FAS$=$(U, \mathbf{R})$, $\mathbf{R} = \mathbf{C} \cup d$ is the IF attribute set consisting of a condition attribute set $\mathbf{C}$ and decision attribute $d$. Let $V$ be the range of the attribute set $\mathbf{R}$ and $G$ an information function.

Then IFIS=$(U, \mathbf{C} \cup d, V, G)$ is referred to as intuitionistic fuzzy information system.

Let IFIS=$(U, \mathbf{C} \cup d, V, G)$, $\mathbf{P} \subseteq \mathbf{C}$. The $\mathbf{P}$positive region of $dPOS_{\mathbf{P}}(d)$, is a fuzzy set on $U$. $POS_{\mathbf{P}}(d)$ is expressed $\forall x \in U$ as

$$POS_{\mathbf{P}}(d)(x) = \bigcup_{X_j \in U/d} \mathbf{P}^{-} X_j(x). \tag{2}$$

The classification ability of an information system can be measured by the degree of dependency of the decision attribute $d$ on the condition attributes $\mathbf{C}$, which is referred to as the overall degree of dependency of the information system,

$$\nu_{\mathbf{C}}(d) = \frac{|POS_{\mathbf{C}}(d)|}{|U|} = \frac{\sum\limits_{x \in U} POS_{\mathbf{C}}(d)(x)}{|U|}, \tag{3}$$

where $|POS_{\mathbf{C}}(d)|$ is the cardinality of $POS_{\mathbf{C}}(d) \in F(U)$.

The cardinality of the intuitionistic fuzzy set $X \in F(U)$ is defined as [23]

$$|X| = \left( \sum_{x \in U} \mu_X(x), \sum_{x \in U} (1 - \gamma_X(x)) \right). \tag{4}$$

Whether an attribute is important depends on the degree of its influence on the classification capability of the system. Therefore, the importance of a condition attribute $R \in \mathbf{C}$ can be evaluated by the change in overall degree of dependency of the information system calculated when $R$ is removed. The greater the change in the overall degree of dependency the greater effect of $R$ on the classification ability of an information system, and thus the more important is $R$. If the change in the overall degree of dependency is small, then $R$ has a relatively small impact on the classification ability of the system, hence it is less important.

$\forall R \in \mathbf{C}$, the importanceof $R$ to the information system, $\sigma_{C,d}(R)$ is expressed as

$$\sigma_{C,d}(R) = \nu_{\mathbf{C}}(d) - \nu_{\mathbf{C}-\{R\}}(d). \tag{5}$$

Because the overall degree of dependency of IFIS is an intuitionistic fuzzy value, the distance measure between intuitionistic fuzzy values is defined. Let $x = (\mu_x, \nu_x)$ and $y = (\mu_y, \nu_y)$ be two intuitionistic fuzzy values on $U$. Then the distance measure between $x$ and $y$ is defined by

$$d(x, y) = \sqrt{\frac{(\mu_x - \mu_y)^2 + (\nu_x - \nu_y)^2}{2}}. \tag{6}$$

Based on the degree of dependency and attribute importance, we can define the relative reduction of the information system.

For IFIS=$(U, \mathbf{C} \cup d, V, G)$, $Red(\mathbf{C}) \subseteq \mathbf{C}$ is the relative reduction of IFIS=$(U, \mathbf{C} \cup d, V, G)$ if and only if $Red(\mathbf{C})$satisfies $\nu_{\mathbf{C}}(d) - \nu_{Red(\mathbf{C})}(d) = 0$.

The overall degree of dependency before and after the reduction of the intuitionistic fuzzy information system remains unchanged. However, the conditions that require the overall degree of dependency to be completely consistent are often too stringent. Especially for intuitionistic fuzzy information systems, an object's attribution to an intuitionistic fuzzy equivalence class is represented by the degrees of membership and non-membership. Intuitionistic fuzzyinformation systems are more complex and fragile than ordinary information systems. A small disturbance may affect the calculation of the degree of dependency, which is not conducive to the reduction of redundant attributes. Therefore, we use the concept of approximate relative reduction.

For IFIS=$(U, \mathbf{C} \cup d, V, G)$, $Red(\mathbf{C}) \subseteq \mathbf{C}$ is the approximate relative reduction of IFIS=$(U, \mathbf{C} \cup d, V, G)$ if and only if $Red(\mathbf{C})$ satisfies $\nu_{\mathbf{C}}(d) - \nu_{Red(\mathbf{C})}(d) \leq \varepsilon$, where $\varepsilon \in [0, 0.05]$ is the threshold value. When $\varepsilon = 0$, $Red(\mathbf{C})$ degenerates to a conventional relative reduction.

The attribute reduction of information systems is normally not unique, and the intersection of all the reductions is called the kernel. The reduction with the lowest dimensionality is referred to as the minimum reduction.

### B. D-S EVIDENCE THEORY

The frame of discernment is the most basic concept in evidence theory. Let $\Theta$ denote the frame of discernment; the set of all its subsets is the power set $2^{\Theta}$. Any proposition corresponds to a subset of $\Theta$.

If the function $m$: $2^{\Theta} \rightarrow [0, 1]$ satisfies $m(\emptyset) = 0$ and $\sum_{A \subseteq \Theta} m(A) = 1$, then $m$ is called the probability distribution function on $2^{\Theta}$, and $m(A)$ is called the basic probability assignment of $A$. If $A \subseteq \Theta$ and $m(A) > 0$, then $A$ is called the focal element.

The belief function Bel$(A)$ and plausibility function Pl$(A)$ are defined as:

$$Bel(A) = \sum_{B \subseteq A} m(B), \forall A \subseteq \Theta, \tag{7}$$

$$Pl(A) = \sum_{B \cap A \neq \emptyset} m(B) = 1 - Bel(\neg A). \tag{8}$$

For proposition $A$ in $\Theta$, the brief interval $[Bel(A), Pl(A)]$ can be formed to describe the possibility of $A$.

Independent sources of information can be combined using Dempster's rule of combination.

Let $m_1 m_2, \ldots, m_n$ be $n$ probability distribution functions. Then their orthogonal set $m = m_1 \oplus m_2 \oplus \ldots \oplus m_n$ can be obtained as:

$$\begin{cases} m(A) = (1 - K)^{-1} \times \sum\limits_{\cap A_i = A} \prod\limits_{i=1}^{n} m_i(A_i), & A \neq \emptyset \\ m(A) = 0, & A = \emptyset \end{cases} \tag{9}$$

where $K$ is the conflict factor expressed as:

$$K = \sum_{\cap A_i = \Phi} \prod_{i=1}^{n} m_i(A_i) \tag{10}$$

Dempster's rule of combination is commutative and associative, and is the most commonly used rule of combination in evidence theory.

## III. MODEL AND ALGORITHMS FOR THREAT ASSESSMENT

### A. THREAT ASSESSMENT INFORMATION SYSTEM

A threat assessment information system is a prerequisite for threat assessment. The factors influencing the threat assessment of aerial targets are the basis for the assessment of their threat level. Therefore, in a threat assessment information system, the condition attribute set corresponds to the threat assessment factor set, and the decision attribute to the target's threat level.

Let $U$ be the target's nonempty finite universe, R=C∪W the set of intuitionistic fuzzy attributes containing threat assessment factor set **C**and threat level $W$, $V$ the range of attribute set **R**, and $G$ an information function. Then TAIS= $(U, \mathbf{C}\cup W, V, G)$ is called a threat assessment information system.

A threat assessment factor set usually involves many factors such as the type, speed, distance, heading, altitude, electronic jamming capability, and penetration capability of the target. At the same time, the acquisition of the target's characteristic information is a dynamic process, hence the threat assessment is a dynamic process. The threat level of the target cannot be effectively evaluated using only the characteristic information at a certain moment. Therefore, in addition to the above factors, we select the characteristic information of the target at several representative moments as the basis for assessment. The characteristic information of target speed, distance, heading, altitude, and electronic jamming capability at two representative moments is selected. Thus the threat assessment information system contains 17 condition attributes, $\mathbf{C}=\{A_1, A_2, \ldots, A_{17}\}$={target type, speed, distance, heading, altitude, electronic jamming capability, penetration capability, speed 2, distance 2, heading 2, altitude 2, electronic jamming capability 2, speed 3, distance 3, heading 3, altitude 3, electronic jamming capability 3}.

To deal with the uncertainty of threat assessment factors, intuitionistic fuzzy partitioning is applied to each factor. The aerial attack targets are partitioned into three types according to their radar cross-section, U/$A_1$ $=\{A_{11}, A_{12}, A_{13}\}$={small target, large target, other targets}. The other factors are similarly partitioned as U/$A_2$=$\{A_{21}, A_{22}, A_{23}\}$={high speed, medium speed, low speed}, U/$A_3$ = $\{A_{31}, A_{32}, A_{33}, A_{34}\}$={immediate proximity, close proximity, medium distance, far away}, U/$A_4$ = $\{A_{41}, A_{42}, A_{43}, A_{44}\}$ = {radial, approaching, flanking, diverging}, U/$A_5$ = $\{A_{51}, A_{52}, A_{53}\}$={low altitude, medium altitude, high altitude}, U/$A_6$ = $\{A_{61}, A_{62}, A_{63}, A_{64}\}$={strong, medium, weak, none}, and U/$A_7$ = $\{A_{71}, A_{72}, A_{73}\}$={strong, medium, weak}, and U/$A_8$ = U/$A_2$= U/$A_{13}$, U/$A_9$ = U/$A_3$=U/$A_{14}$, U/$A_{10}$ = U/$A_4$=U/$A_{15}$, U/$A_{11}$ = U/$A_5$=U/$A_{16}$, and U/$A_{12}$ = U/$A_6$= U/$A_{17}$.

By combining the real-time nature of integrated air defense and anti-missile operations, the feasibility of model processing, and the commander's thinking habits, we characterize the threat of an incoming aerial attack target on three levels, U/$W$ $=\{w_1 w_2 w_3\}$={major threat, moderate threat, minor threat}.

We have established the representative data based on historical data and combat doctrine, and can obtain the threat assessment intuitionistic fuzzy information system by processing the data using intuitionistic fuzzy sets theory.

### B. ALGORITHMS TO EXTRACT THREAT ELEMENTS AND ASSESSMENT RULES

Extraction of threat elements is the basis of threat assessment. The threat level of a target depends on various factors. Threat elements differ by combat tasks. Most threat assessment methods make inferences or decisions on the basis that threat elements have been given or are artificially selected. This ignores the problem of selecting the threat elements. We use IFRS to evaluate methods to extract the generated elements of threat assessment and to extract their rules.

For a threat assessment intuitionistic fuzzy information system, the reduction of redundant attributes based on IFRS can realize the extraction of a threat element. Solving the minimum reduction is an NP-hard problem. We use a heuristic search to solve the reduction. The overall degree of dependency and attribute importance of the intuitionistic fuzzy information system are used as the heuristic function, which reduces the search space.

The algorithms obtain the threat assessment intuitionistic fuzzy information system TAIS= $(U, \mathbf{C}\cup W, V, G)$, and perform intuitionistic fuzzy preprocessing on the continuous attribute data. We set the initial value of the reduction set to **C**. In a top-down manner, the amount of change in the overall degree of dependency is calculated after a condition attribute is removed. The condition attribute corresponding to the amount of change that satisfies $\nu_{\mathbf{C}}(d) - \nu_{Red(\mathbf{C})}(d) \leq \varepsilon$ is selected iteratively, and is deleted from the reduction set **C**. The process continues until removing any condition attribute changes the degree of dependency to be greater than $\varepsilon$. The algorithms are described as follows.

The time complexity of Algorithm 1 is mainly reflected in the calculations of the degree of dependency $\nu_{\mathbf{C}}(d) = {|POS_{\mathbf{C}}(d)|}/{|U|}$, and the calculations of the degree of dependence is mainly to calculate the relatively positive region, so the time complexity of the calculation of the relatively positive region has a direct impact on the efficiency of Algorithm 1. The algorithm optimizes the calculation of the relatively positive region $POS_{\mathbf{C}}(d)(x) = \bigcup_{X_j\in U/d} \mathbf{C}^{-}X_j(x)$. In step 2, the algorithm sorts all task values of the decision attribute from smallest to largest, thereby reducing the computational complexity of partitioning, lower approximation and the relatively positive region. In step 5, the calculation of the relatively positive region is divided and $POS_{\mathbf{Y}-\{A_i\}}d(x) = \inf_{S_i\in U/\{\mathbf{Y}-\{A_i\}\}} \max\{1 - S_i(x)), t_i\}$, where $t_i = \sup_{X_j\in U/d} \inf_{y\in U, y\notin X_j} (1 - S_i(y))$. Each calculation of the relatively positive region retains the calculation result of $U/\mathbf{Y}$ from the previous iteration, which simplifies the calculation

**Algorithm 1** Algorithm to Extract Threat Element

Input: Intuitionistic fuzzy information system TAIS=$(U, \mathbf{C} \cup W, V, G)$ after preprocessing. Output: Reduction set $\mathbf{Y} = Red(\mathbf{C})$

Step 1: Initialize $\varepsilon \in [0, 0.05]$, and let $\mathbf{Y}=\mathbf{C}$;

Step 2: Sort the value of decision attribute $W$ on $U$ calculate the partitioning of $W$ on $U$, $U/W = \{X_i | X_i \in U/W\}$, and obtain the set of equivalence classes $\{X_1, X_2, \cdots, X_q\}$;

Step 3: Use equation (3) to calculate the overall degree of dependency of the system, $\nu_{\mathbf{C}}(W)$;

Step 4: $\forall A_i \in \mathbf{Y}$, calculate $U/\{\mathbf{Y} - \{A_i\}\} = \{S_1, S_2, \cdots, S_m\}$;

Step 5: $\forall A_i \in \mathbf{Y}$, $\forall S_i \in U/\{\mathbf{Y} - \{A_i\}\}$, $\forall X_j \in U/W$ calculate $t_i = \sup_{X_j \in U/d} \inf_{y \in U, y \notin X_j} (1 - S_i(y))$ obtain $t = \{t_1, t_2, \cdots, t_m\}$; $\forall x \in U$ calculate $POS_{\mathbf{Y}-\{A_i\}} W(x) = \inf_{S_i \in U/\{\mathbf{Y}-\{A_i\}\}} \max\{1 - S_i(x)), t_i\}$, and obtain $\nu_{\mathbf{Y}-\{A_i\}}(d)$;

Step 6: $\forall A_i \in \mathbf{Y}$ calculate $\sigma'_{\mathbf{Y}-\{A_i\},d}(A_i) = \nu_{\mathbf{C}}(W) - \nu_{\mathbf{Y}-\{A_i\}}(W)$; if $\sigma'_{\mathbf{Y}-\{A_i\},d}(A_i) \leq \varepsilon$, set $\mathbf{Y} = \mathbf{Y} - \{A_i\}$ and return to step 4;

Step 7: $\forall A_i \in \mathbf{Y}$, if $\sigma'_{\mathbf{Y}-\{A_i\},d}(A_i) > \varepsilon$, exit the algorithm and output the reduction set $\mathbf{Y}$.

and reduces the time complexity of Algorithm 1 to a certain extent.

With the above threat element extraction algorithm, the post-attribute reduction intuitionistic fuzzy information system TAIS=$(U, Red(\mathbf{C}) \cup W, V, G)$ can be obtained. Based on TAIS=$(U, Red(\mathbf{C}) \cup W, V, G)$, the logical relations implied by the intuitionistic fuzzy information system can be extracted as

$$(A_{11} \vee A_{12} \vee \cdots \vee A_{1k1}) \wedge (A_{21} \vee A_{22} \vee \cdots \vee A_{2k2}) \wedge \cdots \wedge (A_{m1} \vee A_{m2} \vee \cdots \vee A_{mkm}) \Rightarrow (w_1 \vee w_2 \vee \cdots \vee w_q). \tag{11}$$

By decomposing equation (11), the following logical relationships can be obtained, which are the initial rules of group $p$, $p = k1 \cdot k2 \cdot \cdots \cdot km$:

$$RL1: \begin{cases} A_{11} \wedge A_{21} \wedge \cdots \wedge A_{m1} \Rightarrow w_1 \\ \cdots\cdots \\ A_{11} \wedge A_{21} \wedge \cdots \wedge A_{m1} \Rightarrow w_q \end{cases}$$

$$RL2: \begin{cases} A_{11} \wedge A_{22} \wedge \cdots \wedge A_{m1} \Rightarrow w_1 \\ \cdots\cdots \\ A_{11} \wedge A_{22} \wedge \cdots \wedge A_{m1} \Rightarrow w_q \end{cases}$$

$$\cdots\cdots$$

$$RLp \begin{cases} A_{1k1} \wedge A_{2k2} \wedge \cdots \wedge A_{mkm} \Rightarrow w_1 \\ \cdots\cdots \\ A_{1k1} \wedge A_{2k2} \wedge \cdots \wedge A_{mkm} \Rightarrow w_q, \end{cases}$$

where $A_{i1}, A_{i2}, \cdots, A_{iki}$ are the intuitionistic fuzzy linguistic values corresponding to an intuitionistic fuzzy subset on $U$. This set of rules contains all the rules that can be obtained by the information system. The rule set contains rules with a low degree of belief. Therefore, the degree of belief of rules must be calculated so as to extract the rules that have high degrees of belief or meet user's requirements.

For the intuitionistic fuzzy rule, $RL11$, $C_{11} \wedge C_{21} \wedge \cdots \wedge C_{m1} \Rightarrow w_1$. Let the set of objects be $X_1 \subseteq U$ for decision value $w_1$. Project $A_{11}, A_{21}, \cdots, A_{m1} \in FS(U)$ on $X_1$ to obtain $m$ intuitionistic fuzzy subsets on $X_1$, $C^1_{11}, C^1_{21}, \cdots, C^1_{m1} \in FS(X_1)$. Perform the combination operation on $C^1_{1i}, C^1_{2j}, \cdots, C^1_{mh}$ and obtain the degree of belief of $RL11$ as $\kappa(RL11) = \vee(C^1_{11} \wedge C^1_{21} \wedge \cdots \wedge C^1_{m1})$. The degree of belief of other intuitionistic fuzzy rules can be similarly obtained.

The degree of belief here, $\kappa(RL1l) = (\mu_\kappa(RL1l), \gamma_\kappa(RL1l))$, is an intuitionistic fuzzy value, where $\mu_\kappa(RL1l)$ represents the degree of support to the degree of belief, and $\gamma_\kappa(RL1l)$ represents the degree of rejection of the degree of belief, i.e., the degree of disbelief:

$$\begin{aligned} \mu_\kappa(RL1l) &= \vee_{x \in X_l} (\mu_{C^l_{11}}(x) \wedge \mu_{C^l_{21}}(x) \wedge \cdots \wedge \mu_{C^l_{m1}}(x)) \\ \gamma_\kappa(RL1l) &= \wedge_{x \in X_l} (\gamma_{C^l_{11}}(x) \vee \gamma_{C^l_{21}}(x) \vee \cdots \vee \gamma_{C^l_{m1}}(x)). \end{aligned} \tag{12}$$

The algorithm is given below.

**Algorithm 2** Algorithm to Extract Assessment Rules

**Input:** Post-reduction intuitionistic fuzzy information system, TAIS=$(U, Red(\mathbf{C}) \cup W, V, G)$;

**Output:** Intuitionistic fuzzy assessment rule set $RC$

Step 1: Set the threshold values $(\alpha, \beta)$, where $0 < \alpha + \beta \leq 1$, and $RC = \emptyset$;

Step 2: $\forall x \in U$, solve $U/W = \{X_i | X_i \in U/d\}$;

Step 3: Extract and decompose the logical relationships in the intuitionistic fuzzy information system to obtain $p$ sets of initial rules $\{RLl, | l = 1, 2, \ldots, p\}$;

Step 4: For each set of initial rules $RLl$, find the degree of belief of each rule, $\kappa(RLl) = \{\kappa(RLl1), \kappa(RLl2), \cdots, \kappa(RLlq)\}$, by equation (12), and select the intuitionistic fuzzy rule with the highest degree of belief to join $RC = RC \cup \{r_l\}$;

Step 5: Screen the rules in $RC$ according to the threshold values $\alpha$ and $\beta$, excluding those rules with degree of belief less than $\alpha$ and degree of disbelief greater than $\beta$, output the intuitionistic fuzzy rule set $RC$, and exit the algorithm.

Since the input of Algorithm 2 is the intuitionistic fuzzy information system that has reduced the redundant condition attributes (according to Algorithm 1), the calculation results of partitioning of $W$ on $U$ of Algorithm 1 can be directly referenced in step2 of Algorithm 2. The time complexity of Algorithm 2 is mainly in the calculation of the degree of belief. If the initial rule set of post-reduction intuitionistic fuzzy information system has a total of $p = k1 \cdot k2 \cdot \cdots \cdot km$ groups and each rule group has $q$ rules, then $w \cdot q$ calculations of degree of belief must be performed. So the time complexity of the algorithm is $O(w \cdot q)$. When the number of intuitionistic fuzzy linguistic values of conditional attributes is larger, the complexity of the Algorithm 2 will be higher.

### C. ALGORITHM TO DETERMINE BPA

Determination of the probability distribution function is a key in the application of evidence theory. For a threat assessment with target attribute data acquired in stages, we apply the threat assessment rule set acquired by IFRS to establish a method to determine BAP.

Let the acquired intuitionistic fuzzy rule set $RC$ contain the following rules:

$$RC1: A_{11} \wedge A_{21} \wedge \cdots \wedge A_{m1} \Rightarrow w_{RC1}(\kappa(RC1))$$
$$RC2: A_{11} \wedge A_{22} \wedge \cdots \wedge A_{m1} \Rightarrow w_{RC2}(\kappa(RC2))$$
$$\cdots\cdots$$
$$RCp: A_{1k1} \wedge A_{2k2} \wedge \cdots \wedge A_{mkm} \Rightarrow w_{RCk}(\kappa(RCp))$$

where $A_1, A_2, \cdots, A_m$ are the rule antecedents, and $W$ is a decision attribute whose value is in the range $\{w_1, w_2, w_3, w_4\}$. Because the values of $W$ are independent, at any one time, each rule takes the value of an element in the range, so $W$ can be used as the framework of discernment, i.e., $\Theta = \{w_1, w_2, \cdots, w_s\}$.

To simplify the description, suppose the data of a target attribute provided by the system in the *i-th* stage consist of $X = (x_1, x_2)$; the attributes corresponding to $x_1$ and $x_2$ are $C_1$ and $C_2$, respectively; $C_1$ contains the IF linguistic values $\{A_{11}, A_{12}, A_{13}\}$; and $C_2$ contains the IF linguistic values $\{A_{21}, A_{22}, A_{23}\}$.

First, IF processing is conducted on the input data. The degree of membership of $x_1$ for $\{A_{11}, A_{12}, A_{13}\}$ is denoted by $\{A_{11}(x_1), A_{12}(x_1), A_{13}(x_1)\}$. The degree of membership of $x_2$ for $\{A_{21}, A_{22}, A_{23}\}$ is denoted by $\{A_{21}(x_2), A_{22}(x_2), A_{23}(x_2)\}$. Next, the degrees of match between the input data $x_1$ and $x_2$ with respect to their IF linguistic values are calculated as

$$t(x_1) = \max_x\{\min(x_1(x), A_{1i}(x))\}$$
$$t(x_2) = \max_x\{\min(x_1(x), A_{2i}(x))\}. \tag{13}$$

Under this condition, the algorithm to determine BPA is as follows

For the information provided by the system in subsequent stages, BPA can be obtained by Algorithm 3 based on the information of the rule items provided in the previous stage. For example, if the information of rule items provided in the second stage is $A_{32}$, then the rule subset $RC'$ containing $A_{32}$ will be searched from the rule set $RC$ and used as the input of algorithm 3 to obtain the BPA corresponding to the second stage. The information of rule item provided in the subsequent stages can be processed in the same way, and the BPA of each stage can also be obtained by Algorithm 3.

### D. THREAT ASSESSMENT MODEL

Based on the above analysis, for the threat assessment of the data of target attributes acquired in stages, we present a threat assessment model based on IFRS and D-S evidence theory, as shown in Figure 1. The key is to use a combination of the knowledge discovery function of IFRS and the decision-making function of D-S evidence theory to assist the combat commander to make threat assessments of current targets based on incomplete, inaccurate, or uncertain information obtained in multiple stages. The model has two parts: extraction of threat assessment elements and assessment rules, and fusion reasoning on the data acquired in stages.

**Algorithm 3** Algorithm to Determine BPA

**Input:** The *i-th* stages of data, $X$, and the rule set, $RC$

**Output:** BPA

Step 1: Determine the IF linguistic valuescorresponding to $X = (x_1, x_2)$ according to the maximum membership principle on the degree of match $t(x_i)$, and extract all rules that contain these IF linguistic values in the rule set $RC$, denoted by $\{RC1, RC2, \cdots, RCk\}$;

Step 2: For all $RCi \in \{RC1, RC2, \cdots, RCk\}$, find $Y_i = \min\{\kappa(RCi), t(x_1), t(x_2)\}$ to generate a new rule subset $RC'$, where $\kappa(RC'i) = Y_i$

Step 3: Extract different decision values that $\kappa(RC'i)$ contains, denoted by $DC{=}\{d_j | j \leq q\}$, $\forall d_j \in DC$; determine the sum of the degree of belief and degree of disbelief of all rules at $d_j$ in $RC'$; and obtain $DZ{=}\{d_j(\sum \mu_\kappa(d_j), \sum \gamma_\kappa(d_j)) | j \leq q\}$;

Step 4: Using $DZ$, determine the focal element set $JY{=}\{d_j | d_j \in DC\} \cup \{\bar{d}_j | \gamma_\kappa(d_j) \neq 0\} \cup \{\cup d_j | d_j \in DC\}$, which comprises three types of focal elements:$d_j$, $\bar{d}_j$, and $\cup d_j$, denoted by $A_j$, $B_j$, and $C_j$, respectively;

Step 5: Determine the pseudo BPA function $Zm$, where $Zm(A_j) = \sum \mu_\kappa(d_j)$, $Zm(B_j) = \sum \gamma_\kappa(d_j)$, $Zm(C_j) = \rho - \max\{\sum \mu_\kappa(d_j)\}$, where $\rho$ is the maximum number of rules that have the same decision value in $RC'$;

Step 6: Normalize $Zm$, yielding $m(A_j)$, $m(B_j)$, $m(C_j)$, and exit the algorithm.

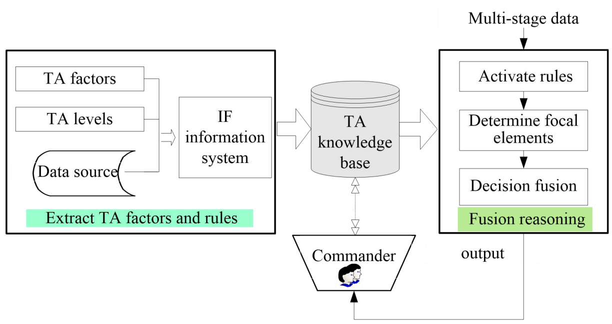


**FIGURE 1.** TA model.

For the threat assessment of aerial attack targets, we construct a threat assessment information system with seven basic factors, dynamic factors at two typical moments, 17 condition attributes, and one decision attribute. The threat intuitionistic fuzzy information system is obtained through intuitionistic fuzzy processing of the information system.

Based on that, Algorithm 1 is used to reduce the redundant attributes of the threat assessment intuitionistic fuzzy information system, and Algorithm 2 is used to extract the intuitionistic fuzzy decision rules. These rules can be revised by the combat commander to obtain the final threat assessment knowledge base.

In the case that the target attribute data are acquired in stages, based on the threat assessment knowledge base, the assessment rules corresponding to the attribute data in each stage are obtained. The intuitionistic fuzzy semantics for the degree of belief in the rule conclusion are used to determine the focal elements. Algorithm 3 is then used to calculate its basic probability assignment, and to calculate the fused reasoning on the conclusion of each stage. For attribute data received in the first stage, the threat assessment knowledge base is used to determine the degree of support by those data to each threat level, i.e., the corresponding probability distribution function $m_1$. Then, the attribute data are received in the second stage. As in the first stage, the probability distribution function to the threat level, $m_2$, of the attribute data obtained in the second stage is determined. The rule combination is used to combine the values of the probability distribution in the first and second stages to obtain a new BPA. The data-receiving and BPA-determining process is repeated in subsequent stages. The BPA from the previous stage is combined with the new BPA in the current stage. A comprehensive BPA is eventually obtained. After all the evidence is combined, a decision must be made based on the result. The main trust quantification functions in evidence theory are the probability distribution function, belief function, and likelihood function. These give a measure of belief to the evidence from different perspectives. These three functions can be assigned or used together as the basis for judgment in decision-making. We use the decision method based on the probability distribution function.

According to the calculation result from the combination, if $\exists A_1, A_2 \subseteq \Theta$, then

$$\begin{cases} M(A_1) = \max\{m(A_i), A_i \subseteq \Theta\} \\ M(A_2) = \max\{m(A_i), A_i \subseteq \Theta \backslash A_1\}. \end{cases} \tag{14}$$

If $M(A_1)$, $M(A_2)$, and $M(\Theta)$ satisfy

$$\begin{cases} M(A_1) - M(A_2) > \delta_1 \\ M(\Theta) < \delta_2 \\ M(A_1) > M(\Theta), \end{cases} \tag{15}$$

then $A_1$ is a result of judgment, where $\delta_1$ and $\delta_2$ are the set threshold values.

The threat assessment result obtained by applying the above model is the target's BPA at a certain threat level. The final decision for the threat level can be made based on this BPA. Sorting the threats of targets at the same threat level can be accomplished by sorting the values of targets' BPA at that threat level. The larger the BPA the greater the threat. This not only ranks the targets but also determines their threat levels.

## IV. CASE STUDY

An example of air defense operations is used to illustrate the reasoning process of threat assessment. In a ground air defense operation, there are three batches of incoming targets. The target attribute data provided by the system in different stages are shown in Table 1.

**TABLE 1. Attribute data of targets in stages.**

| Target | $x_1$ | $x_2$ | $x_3$ |
|---|---|---|---|
| Stage 1 | $A_{63}(0.85, 0.05)$<br>$A_{71}(0.8, 0.1)$ | $A_{63}(0.8, 0.1)$<br>$A_{72}(0.9, 0.0)$<br>$A_{11}(0.79, 0.11)$ | $A_{62}(0.8, 0.1)$<br>$A_{71}(0.9, 0.0)$ |
| Stage 2 | $A_{11}(0.81, 0.09)$<br>$A_{33}(0.8, 0.1)$ | $A_{33}(0.8, 0.1)$<br>$A'_{22}(0.8, 0.1)$<br>$A'_{32}(0.8, 0.1)$ | $A_{12}(0.8, 0.1)$<br>$A'_{21}(0.8, 0.1)$<br>$A'_{33}(0.86, 0.04)$ |
| Stage 3 | $A'_{22}(0.8, 0.1)$<br>$A'_{33}(0.8, 0.1)$ | $A_{43}(0.82, 0.08)$ | $A_{34}(0.75, 0.15)$ |
| Stage 4 | $A_{42}(0.78, 0.12)$ | $A''_{41}(0.8, 0.1)$ | $A''_{43}(0.85, 0.05)$ |

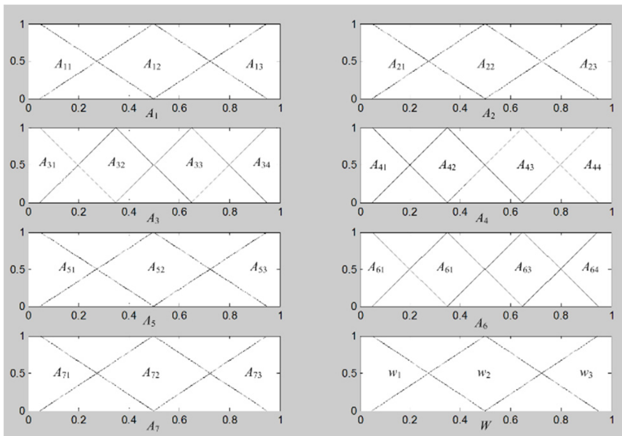

**FIGURE 2. Intuitionistic fuzzy partitioning of attributes.**

For the threat assessment information system, TAIS$=(U, \mathbf{C} \cup W, V, G)$, where $\mathbf{C}=\{A_1, A_2, \ldots, A_{17}\}=\{$target type, speed, distance, heading, altitude, electronic jamming capability, penetration ability, speed 2, distance 2, heading 2, altitude 2, electronic jamming ability 2, speed 3, distance 3, heading 3, altitude 3, electronic jamming ability 3$\}$. According to the tactical principles and the range of values of each characteristic parameter, 500 lines of threat assessment characteristic data are simulated, where the value of each characteristic is normalized to [0, 1]. An initial threat assessment information system is established. Intuitionistic fuzzy partitioning for each attribute is conducted. The membership function $\mu(x)$ is a combination of triangles and trapezoids, as shown in Figure 2. The non-membership function $\gamma(x)$ is determined as follows:

$$\forall x \in [0, 1],\ 0 \le \tau \le 1 - \mu(x),\ \tau \in [0, 0.5]$$
$$\gamma(x) = \begin{cases} 0, & \mu(x) \ge 1 - \tau \\ 1 - \mu(x) - \tau, & \mu(x) < 1 - \tau. \end{cases} \tag{16}$$

(1) According to Algorithms 1 and 2, for $\varepsilon = 0.01, \alpha = 0.6, \beta = 0.4$, we obtain $Red(\mathbf{C})=\{A_1, A_3, A_4, A_6, A_7, A_8, A_9, A_{15}\}$ after removing redundant attributes. The final threat assessment rule set is shown below.

$$A_{11} \wedge A_{33} \wedge A_{42} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{41} \Rightarrow w_1(0.72, 0.18)$$
$$A_{11} \wedge A_{33} \wedge A_{42} \wedge A_{64} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{41} \Rightarrow w_1(0.6, 0.3)$$
$$A_{11} \wedge A_{33} \wedge A_{42} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_2(0.81, 0.09)$$
$$A_{11} \wedge A_{33} \wedge A_{42} \wedge A_{64} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_2(0.72, 0.18)$$
$$A_{11} \wedge A_{31} \wedge A_{43} \wedge A_{62} \wedge A_{71} \wedge A'_{23} \wedge A'_{31} \wedge A''_{41} \Rightarrow w_3(0.73, 0.17)$$
$$A_{11} \wedge A_{33} \wedge A_{43} \wedge A_{63} \wedge A_{72} \wedge A'_{22} \wedge A'_{32} \wedge A''_{41} \Rightarrow w_1(0.8, 0.1)$$
$$A_{11} \wedge A_{33} \wedge A_{41} \wedge A_{62} \wedge A_{73} \wedge A'_{23} \wedge A'_{33} \wedge A''_{41} \Rightarrow w_3(0.82, 0.08)$$
$$A_{11} \wedge A_{33} \wedge A_{41} \wedge A_{64} \wedge A_{73} \wedge A'_{23} \wedge A'_{33} \wedge A''_{41} \Rightarrow w_3(0.87, 0.03)$$
$$A_{11} \wedge A_{33} \wedge A_{43} \wedge A_{63} \wedge A_{72} \wedge A'_{22} \wedge A'_{32} \wedge A''_{42} \Rightarrow w_1(0.85, 0.05)$$
$$A_{13} \wedge A_{31} \wedge A_{41} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{44} \Rightarrow w_3(0.8, 0.1)$$
$$A_{13} \wedge A_{32} \wedge A_{43} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_1(0.89, 0.01)$$
$$A_{11} \wedge A_{33} \wedge A_{42} \wedge A_{63} \wedge A_{72} \wedge A'_{22} \wedge A'_{32} \wedge A''_{42} \Rightarrow w_2(0.62, 0.28)$$
$$A_{11} \wedge A_{33} \wedge A_{41} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_2(0.6, 0.3)$$
$$A_{11} \wedge A_{33} \wedge A_{43} \wedge A_{63} \wedge A_{71} \wedge A'_{21} \wedge A'_{33} \wedge A''_{43} \Rightarrow w_1(0.61, 0.29)$$
$$A_{11} \wedge A_{34} \wedge A_{43} \wedge A_{63} \wedge A_{72} \wedge A'_{21} \wedge A'_{33} \wedge A''_{43} \Rightarrow w_3(0.75, 0.25)$$
$$A_{11} \wedge A_{32} \wedge A_{41} \wedge A_{63} \wedge A_{72} \wedge A'_{21} \wedge A'_{31} \wedge A''_{43} \Rightarrow w_3(0.6, 0.3)$$
$$A_{11} \wedge A_{33} \wedge A_{41} \wedge A_{63} \wedge A_{71} \wedge A'_{21} \wedge A'_{32} \wedge A''_{42} \Rightarrow w_2(0.65, 0.25)$$
$$A_{12} \wedge A_{34} \wedge A_{42} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{32} \wedge A''_{43} \Rightarrow w_3(0.7, 0.2)$$
$$A_{12} \wedge A_{34} \wedge A_{42} \wedge A_{62} \wedge A_{71} \wedge A'_{21} \wedge A'_{33} \wedge A''_{43} \Rightarrow w_3(0.68, 0.22)$$
$$A_{12} \wedge A_{34} \wedge A_{42} \wedge A_{62} \wedge A_{71} \wedge A'_{21} \wedge A'_{33} \wedge A''_{43} \Rightarrow w_2(0.8, 0.1)$$
$$A_{13} \wedge A_{31} \wedge A_{42} \wedge A_{61} \wedge A_{74} \wedge A'_{21} \wedge A'_{32} \wedge A''_{41} \Rightarrow w_1(0.8, 0.1)$$
$$A_{13} \wedge A_{32} \wedge A_{41} \wedge A_{61} \wedge A_{74} \wedge A'_{21} \wedge A'_{32} \wedge A''_{41} \Rightarrow w_1(0.73, 0.17)$$
$$A_{12} \wedge A_{32} \wedge A_{41} \wedge A_{62} \wedge A_{71} \wedge A'_{21} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_3(0.87, 0.03)$$
$$A_{12} \wedge A_{34} \wedge A_{41} \wedge A_{62} \wedge A_{71} \wedge A'_{21} \wedge A'_{33} \wedge A''_{43} \Rightarrow w_3(0.8, 0.1)$$
$$A_{13} \wedge A_{33} \wedge A_{41} \wedge A_{62} \wedge A_{71} \wedge A'_{22} \wedge A'_{32} \wedge A''_{44} \Rightarrow w_3(0.8, 0.1)$$
$$A_{13} \wedge A_{33} \wedge A_{43} \wedge A_{62} \wedge A_{71} \wedge A'_{21} \wedge A'_{32} \wedge A''_{41} \Rightarrow w_1(0.6, 0.3)$$
$$A_{13} \wedge A_{31} \wedge A_{42} \wedge A_{61} \wedge A_{73} \wedge A'_{21} \wedge A'_{33} \wedge A''_{41} \Rightarrow w_1(0.88, 0.02)$$
$$A_{13} \wedge A_{31} \wedge A_{43} \wedge A_{61} \wedge A_{73} \wedge A'_{21} \wedge A'_{32} \wedge A''_{41} \Rightarrow w_1(0.85, 0.05)$$
$$A_{13} \wedge A_{31} \wedge A_{43} \wedge A_{64} \wedge A_{73} \wedge A'_{21} \wedge A'_{32} \wedge A''_{41} \Rightarrow w_1(0.6, 0.3)$$
$$A_{12} \wedge A_{34} \wedge A_{42} \wedge A_{64} \wedge A_{71} \wedge A'_{21} \wedge A'_{33} \wedge A''_{43} \Rightarrow w_2(0.65, 0.25)$$
$$A_{12} \wedge A_{32} \wedge A_{41} \wedge A_{64} \wedge A_{71} \wedge A'_{21} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_3(0.9, 0)$$

(2) For target $x_1$, after acquiring the data in the first stage, the rule subset $RC1$ containing $A_{63}$ and $A_{71}$ in the rule set is searched:

$$A_{11} \wedge A_{33} \wedge A_{42} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{41} \Rightarrow w_1(0.72, 0.18)$$
$$A_{11} \wedge A_{33} \wedge A_{42} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_2(0.81, 0.09)$$
$$A_{13} \wedge A_{31} \wedge A_{41} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{44} \Rightarrow w_3(0.8, 0.1)$$
$$A_{13} \wedge A_{32} \wedge A_{43} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_1(0.89, 0.01)$$
$$A_{11} \wedge A_{33} \wedge A_{41} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_2(0.6, 0.3)$$
$$A_{11} \wedge A_{33} \wedge A_{43} \wedge A_{63} \wedge A_{71} \wedge A'_{21} \wedge A'_{33} \wedge A''_{43} \Rightarrow w_1(0.61, 0.29)$$
$$A_{11} \wedge A_{33} \wedge A_{41} \wedge A_{63} \wedge A_{71} \wedge A'_{21} \wedge A'_{32} \wedge A''_{42} \Rightarrow w_2(0.65, 0.25)$$
$$A_{12} \wedge A_{34} \wedge A_{42} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{32} \wedge A''_{43} \Rightarrow w_3(0.7, 0.2)$$

$RC1$ and the data of the first stage for $x_1$ are used as the input of Algorithm 3 to obtain BPA.

For $RC1$, $Y_i$=min$\{\kappa(RC1i), (0.85,0.05), (0.8, 0.1)\}$. A new rule subset $RC1'$ is formed, where $\kappa(RC1'i) = Y_i$:

$$A_{11} \wedge A_{33} \wedge A_{42} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{41} \Rightarrow w_1(0.72, 0.18)$$
$$A_{11} \wedge A_{33} \wedge A_{42} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_2(0.8, 0.1)$$

$$A_{13} \wedge A_{31} \wedge A_{41} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{44} \Rightarrow w_3(0.8, 0.1)$$
$$A_{13} \wedge A_{32} \wedge A_{43} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_1(0.8, 0.1)$$
$$A_{11} \wedge A_{33} \wedge A_{41} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_2(0.6, 0.3)$$
$$A_{11} \wedge A_{33} \wedge A_{43} \wedge A_{63} \wedge A_{71} \wedge A'_{21} \wedge A'_{33} \wedge A''_{43} \Rightarrow w_1(0.61, 0.29)$$
$$A_{11} \wedge A_{33} \wedge A_{41} \wedge A_{63} \wedge A_{71} \wedge A'_{21} \wedge A'_{32} \wedge A''_{42} \Rightarrow w_2(0.65, 0.25)$$
$$A_{12} \wedge A_{34} \wedge A_{42} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{32} \wedge A''_{43} \Rightarrow w_3(0.7, 0.2)$$

$RC1'$ contains different decision values, $DC$={$w_1$, $w_2$, $w_3$}. For all $w_j \in DC$, the sum of the degrees of belief and non-belief of all the rules whose values are $w_j$ in $RC1'$ is obtained, resulting in $DZ$={$w_1$ (2.1,0.57), $w_2$(2.05, 0.65), $w_3$ (1.5,0.3)}.

The focal element set $JY$={$w_1$, $w_2$, $w_3$, {$w_2$, $w_3$}, {$w_1$, $w_3$}, {$w_1$, $w_2$} {$w_1$, $w_2$, $w_3$}} is determined according to $DZ$. The corresponding pseudo-$BPA$ is $Zm(w_1)$=2.1, $Zm(w_2)$=2.05, $Zm(w_3)$=1.5, $Zm(\{w_2, w_3\})$=0.57, $Zm(\{w_1, w_3\})$=0.65, $Zm(\{w_1, w_2\})$=0.3, $Zm(\{w_1, w_2, w_3\})$=0.9. Normalizing $Zm$ yields the first group of $BPA$:$m_1(w_1)$=0.2599, $m_1(w_2)$=0.2540, $m_1(w_3)$=0.1859, $m_1(\{w_2, w_3\})$=0.0706, $m_1(\{w_1, w_3\})$=0.0805, $m_1(\{w_1, w_2\})$=0.0372, $m_1(\{w_1, w_2, w_3\})$=0.1115.

The target attribute data of the second stage data are received. Rule subset $RC2$ in rule set $RC1'$ containing $A_{11}$ and $A_{33}$ is searched:

$$A_{11} \wedge A_{33} \wedge A_{42} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{41} \Rightarrow w_1(0.72, 0.18)$$
$$A_{11} \wedge A_{33} \wedge A_{42} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_2(0.8, 0.1)$$
$$A_{11} \wedge A_{33} \wedge A_{41} \wedge A_{63} \wedge A_{71} \wedge A'_{22} \wedge A'_{33} \wedge A''_{42} \Rightarrow w_2(0.6, 0.3)$$
$$A_{11} \wedge A_{33} \wedge A_{43} \wedge A_{63} \wedge A_{71} \wedge A'_{21} \wedge A'_{33} \wedge A''_{43} \Rightarrow w_1(0.61, 0.29)$$
$$A_{11} \wedge A_{33} \wedge A_{41} \wedge A_{63} \wedge A_{71} \wedge A'_{21} \wedge A'_{32} \wedge A''_{42} \Rightarrow w_2(0.65, 0.25)$$

$RC2$ and the target attribute data of the second stage are used as the input of Algorithm 3, and the second group of $BPA$ can be obtained as $m_2(w_1)$=0.24, $m_2(w_2)$=0.3761, $m_2(\{w_2, w_3\})$=0.0862, $m_2(\{w_1, w_3\})$=0.1193, $m_2(\{w_1, w_2\})$=0.1743.

(3) Combining the above two groups of $BPA$yields $m(w_1)$=0.3552, $m(w_2)$=0.4501, $m(w_3)$=0.0843, $m(\{w_2, w_3\})$=0.0284, $m(\{w_1, w_3\})$=0.0385, $m(\{w_1, w_2\})$=0.0435.

(4) Similarly, the third group of $BPA$can be obtained by acquiring the target attribute data of the third stage: $m_3(w_1)$=0.212, $m_3(w_2)$=0.4236, $m_3(\{w_2, w_3\})$=0.0605, $m_3(\{w_1, w_3\})$=0.1212, $m_3(\{w_1, w_2\})$=0.1827;

(5) Combining the two groups of $BPA$in (4) and (3) yields $m(w_1)$=0.3549, $m(w_2)$=0.5859, $m(w_3)$=0.0354, $m(\{w_2, w_3\})$=0.0028, $m(\{w_1, w_3\})$=0.0078, $m(\{w_1, w_2\})$=0.0132.

(6) Similarly, the target attribute data of the fourth stage are received, and the fourth group of $BPA$ can be obtained as $m_4(w_1)$=0.35, $m_3(w_2)$=0.4, $m_3(\{w_2, w_3\})$=0.1, $m_3(\{w_1, w_3\})$=0.05, $m_3(\{w_1, w_2\})$=0.1.

(7) Combining the two groups of $BPA$in (6) and (5) yields $m(w_1)$=0.329, $m(w_2)$=0.657, $m(w_3)$=0.01, $m(\{w_1, w_2\})$=0.004. The BPA determination process for target $x_1$ is shown in Table 2.

**TABLE 2. BPA determination process for target $x_1$.**

| $m$ | BPA |
|---|---|
| $m_1$ | $m_1(w_1)$=0.259<br>$m_1(w_2)$=0.2540<br>$m_1(w_3)$=0.1859<br>$m_1(\{w_2, w_3\})$=0.0706<br>$m_1(\{w_1, w_3\})$=0.0805<br>$m_1(\{w_1, w_2\})$=0.0372<br>$m_1(\{w_1, w_2, w_3\})$=0.1115 |
| $m_2$ | $m_2(w_1)$=0.24<br>$m_2(w_2)$=0.3761<br>$m_2(\{w_2, w_3\})$=0.0862<br>$m_2(\{w_1, w_3\})$=0.1193<br>$m_2(\{w_1, w_2\})$=0.1743 |
| $m_3$ | $m_3(w_1)$=0.212<br>$m_3(w_2)$=0.4236<br>$m_3(\{w_2, w_3\})$=0.0605<br>$m_3(\{w_1, w_3\})$=0.1212<br>$m_3(\{w_1, w_2\})$=0.1827 |
| $m_4$ | $m_4(w_1)$=0.35<br>$m_3(w_2)$=0.4<br>$m_3(\{w_2,w_3\})$=0.1<br>$m_3(\{w_1, w_3\})$=0.05<br>$m_3(\{w_1,w_2\})$=0.1 |
| $m$ | $m(w_1)$=0.329<br>$m(w_2)$=0.657<br>$m(w_3)$=0.01<br>$m(\{w_1,w_2\})$=0.004 |

According to equations (14) and (15), the threshold values are set to $\delta_1 = 0.3$ and $\delta_2 = 0.1$ and the threat level of the first batch of targets, $x_1$, is medium at $w_2$, with degree of support 0.657, denoted by $w_2$ (0.657). It is worth mentioning that before continuing to determine BPA in later stages, if the combined BPA has already met the decision criteria in a stage, the $BPA$ in later stages no longer must be determined, thereby saving calculation time.

Using the same method, for the second batch of targets $x_2$, we get $m(w_1)$=0.8521, $m(w_2)$=0.12, and $m(\{w_1 w_2\})$=0.0279. $x_2$ is determined as a major threat at $w_1$, with degree of support 0.8521, denoted by $w_1$ (0.8521). For the third batch of targets $x_3$, we get $m(w_1)$=0.0258, $m(w_2)$=0.3102, $m(w_3)$=0.643, and $m(\{w_1, w_3\})$=0.021. $x_3$ is determined as a minor threat at $w_3$, with degree of support 0.643, denoted by $w_3$ (0.643). The results of threat assessment are shown in Table 3. The threats for the three batches of targets shown in Table 1 are $x_2 \succ x_1 \succ x_3$. Therefore, to destroy the second batch of targets can be considered the priority.

In addition, if different batches of targets are determined to be at the same threat level, one can comprehensively consider the degree of support of the targets at that threat level and the degree of support to other threat levels through ranking the degrees of support.

As shown in Table 2, with the gradual acquisition of data in stages, the distribution of BPA gradually focused, and the ranking of threat degree gradually became clear. For target $x_1$, after the acquiring the data in the first stage, the BPA obtained is relatively dispersed, mainly because the information provided by the data in the first stage is limited. After the acquiring the data in the second stage, BPA focuses on $w_2$, and thereafter, the degree of support for $w_2$ from the data in the stages gradually increases and meets the requirements of the decision criteria, thus obtaining the decision result.

In order to test the efficiency of proposed methods and compare it with intuitionistic fuzzy reasoning based threat assessment [5], the attribute data of the four stages in Table 1 are combined to obtain the complete target attribute data. According to the method in [5], we get the threat degree of target $x_1$ is 0.526, the threat degree of target $x_2$ is 0.971, the threat degree of target $x_3$ is 0.214, where the threat degree corresponds to the threat level. According to the threat degree of each target, the threats for the three batches of targets by intuitionistic fuzzy reasoning [5] are $x_2 \succ x_1 \succ x_3$. It can be seen that the results obtained by using the method in [5] are consistent with that in this paper, which demonstrates the effectiveness of our models and algorithms. However, real threat assessment requires the determination of threat level based on continuously received information that is incomplete, inaccurate, or uncertain. The method based on intuitionistic fuzzy reasoning [5] cannot deal with the problem of threat assessment under the condition of incomplete data. In Table 1, the attribute data of the four stages of $x_1$ and $x_2$ does not cover all items in the attribute set $Red(\mathbf{C})=\{A_1, A_3, A_4, A_6, A_7, A_8, A_9, A_{15}\}$, which is quite common in reality, because of the existence of various uncertainties in the operational process, not all the data needed for threat assessment can be obtained. Compared to a threat assessment method based solely on intuitionistic fuzzy reasoning or D-S evidence theory, the advantage of IFRS knowledge acquisition makes the selection of threat assessment elements and determination of BPA more objective and calculates the threat degree of the air raid target under uncertain environment. The calculation results in Table 3 can provide better decision support to the threat judgment of the commander.

**TABLE 3.** Results of threat assessment.

| Target x1 | Target x2 | Target x3 |
|---|---|---|
| $m(w_1)$=0.329 | $m(w_1)$=0.8521 | $m(w_1)$=0.0258 |
| $m(w_2)$=0.657 | $m(w_2)$=0.12 | $m(w_2)$=0.3102 |
| $m(w_3)$=0.01 | $m(\{w_1,w_2\})$=0.0279 | $m(w_3)$=0.643 |
| $m(\{w_1, w_2\})$=0.004 | | $m(\{w_1, w_3\})$=0.021 |
| $w_2$ (0.657) | $w_1$ (0.8521) | $w_3$ (0.643) |

## V. CONCLUSION

We established a threat assessment model based on IFRS and D-S evidence theory to deal with the threat assessment from multi-stage data with uncertainty caused by the battlefield environment and detection equipment. We studied a threat element extraction algorithm based on IFRS. This algorithm uses heuristic search for reduction solutions. The overall degree of dependency and attribute importance of the intuitionistic fuzzy information system are used as the heuristic function, which reduces the search space in the attribute reduction process. We proposed a rule extraction algorithm for threat assessment that can generate assessment rules with degrees of belief and disbelief. On that basis, we studied a BPA determination algorithm based on intuitionistic fuzzy rules. The algorithm obtains assessment rules corresponding to the attribute data of each stage. Based on the threat assessment knowledge base and using the intuitionistic fuzzy semantics of degree of belief in the rule conclusion, this algorithm determines the focal elements corresponding to respective aggregated rules. In addition, the algorithm obtains the degree of support of the multi-stage data to each threat level, and produces a final threat assessment by iterative evidence combination. We experimentally verified the effectiveness of our models and algorithms by calculating the threat levels of three batches of targets whose attribute data were obtained in four stages. Our method combines the advantages of expert knowledge combination in D-S evidence theory and knowledge reduction of IFRS. Compared to the threat assessment method based on D-S evidence theory or intuitionistic fuzzy reasoning alone, our method is less dependent on domain experts and is strong in objectivity of the results. However, our method increases the amount of computation for assessment reasoning especially when the number of conditional attributes and intuitionistic fuzzy linguistic values of conditional attributes are large We hope next to study more efficient and more general heuristic reduction algorithms to improve the efficiency of the algorithms to extract threat elements and rules.

## REFERENCES

[1] N. Okello and G. Thorns, "Threat assessment using Bayesian networks," in *Proc. 6th Int. Conf. Inf. Fusion*, vol. 2, 2003, 1102 1109.
[2] Q. Changwen and H. You, "A method of threat assessment using multiple attribute decision making," in *Proc. 6th Int. Conf. Signal Process.*, vol. 2, Aug. 2002, pp. 1091–1095.
[3] Y. Wang, S. Y. Liu, and W. Zhang, "Threat assessment method with uncertain attribute weight based on intuitionistic fuzzy multi-attribute decision," *Acta Electron. Sin.*, vol. 42, no.12, pp. 2509–2514, Dec. 2014.
[4] C. G. Looney and L. R. Liang, "Cognitive situation and threat assessments of ground battlespaces," *Inf. Fusion*, vol. 4, no. 2, pp. 297–308, 2003.
[5] L. Ying-Jie, W. Bao-Shu, and L. Yan-Li, "Techniques for threat assessment based on adaptive intuitionistic fuzzy reasoning," *J. Electron. Inf. Technol.*, vol. 29, no. 12, pp. 2805–2809, 2007.
[6] L.-L. Chang, J. Jiang, J.-B. Sun, Y.-W. Chen, Z.-J. Zhou, X.-B. Xu, and X. Tan, "Disjunctive belief rule base spreading for threat level assessment with heterogeneous, insufficient, and missing information," *Inf. Sci.*, vol. 476, pp. 106–131, Feb. 2019.
[7] C. Virgil Negoita, "Fuzzy sets," *Fuzzy Sets Syst.*, vol. 133, no. 2, p. 275, Jan. 2003.
[8] Z. Pawlak, "Roughsets," *Int. J. Comput. Inf. Sci.*, vol. 5, pp. 341–356, 1982.

[9] C. Cornelis, M. De Cock, and E. E. Kerre, "Intuitionistic fuzzy rough sets: At the crossroads of imperfect knowledge," *Expert Syst.*, vol. 20, no. 5, pp. 260–270, Nov. 2003.
[10] L. Zhou and W.-Z. Wu, "Characterization of rough set approximations in atanassov intuitionistic fuzzy set theory," *Comput. Math. with Appl.*, vol. 62, no. 1, pp. 282–296, Jul. 2011.
[11] W.-Z. Wu, C.-J. Gao, T.-J. Li, and Y.-H. Xu, "On dual intuitionistic fuzzy rough approximation operators determined by an intuitionistic fuzzy implicator," in *Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing. RSFDGrC* (Lecture Notes in Computer Science), vol. 8170, no. 1. Berlin, Germany: Springer, 2013, pp. 147–156.
[12] W. Xu, Y. Liu, and W. Sun, "Upper approximation reduction based on intuitionistic fuzzy T equivalence information systems," in *Rough Sets and Knowledge Technology, RSKT* (Lecture Notes in Computer Science), vol. 7414, no. 1. Berlin, Germany: Springer, 2012, pp. 63–70.
[13] B. Huang, Y.-L. Zhuang, H.-X. Li, and D.-K. Wei, "A dominance intuitionistic fuzzy-rough set approach and its applications," *Appl. Math. Model.*, vol. 37, nos. 12–13, pp. 7128–7141, Jul. 2013.
[14] Q. Wu, L. Zhou, Y. Chen, and H. Chen, "An integrated approach to green supplier selection based on the interval type-2 fuzzy best-worst and extended VIKOR methods," *Inf. Sci.*, vol. 502, pp. 394–417, Oct. 2019.
[15] Q. Wu, W. Lin, L. Zhou, Y. Chen, and H. Chen, "Enhancing multiple attribute group decision making flexibility based on information fusion technique and hesitant pythagorean fuzzy sets," *Comput. Ind. Eng.*, vol. 127, pp. 954–970, Jan. 2019.
[16] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping," *Ann. Math. Statist.*, vol. 38, no. 2, pp. 325–339, Apr. 1967.
[17] G. Shafer, *A Mathematical Theory of Evidence*. Princeton, NJ, USA: Princeton Univ. Press, 1976.
[18] X. Deng, Q. Liu, Y. Deng, and S. Mahadevan, "An improved method to construct basic probability assignment based on the confusion matrix for classification problem," *Inf. Sci.*, vols. 340–341, pp. 250–261, May 2016.
[19] C. Zhang, Y. Hu, F. T. S. Chan, R. Sadiq, and Y. Deng, "A new method to determine basic probability assignment using core samples," *Knowl.-Based Syst.*, vol. 69, pp. 140–149, Oct. 2014.
[20] P. Xu, X. Su, S. Mahadevan, C. Li, and Y. Deng, "A non-parametric method to determine basic probability assignment for classification problems," *Int. J. Speech Technol.*, vol. 41, no. 3, pp. 681–693, Oct. 2014.
[21] J. Zhang and Y. Deng, "A method to determine basic probability assignment in the open world and its application in data fusion and classification," *Int. J. Speech Technol.*, vol. 46, no. 4, pp. 934–951, Jun. 2017.
[22] L. Yanli, L. Yingjie, and H. Jixue, "Attribute reduction based on intuitionistic fuzzy rough set," *Control Decis.*, vol. 24, no. 3, pp. 335–341, 2009.
[23] L. Lei, Y. Song, and X. Luo, "A new re-encoding ECOC using reject option," *Int. J. Speech Technol.*, May 2020.
[24] Y. Song, Q. Fu, Y.-F. Wang, and X. Wang, "Divergence-based cross entropy and uncertainty measures of Atanassov's intuitionistic fuzzy sets with their application in decision making," *Appl. Soft Comput.*, vol. 84, Nov. 2019, Art. no. 105703.
[25] B. Zhang, M. Zhang, Y. Song, and L. Zhang, "Combining evidence sources in time domain with decision Maker's preference on time sequence," *IEEE Access*, vol. 7, pp. 174210–174218, 2019.
[26] Y. Song, X. Wang, W. Quan, and W. Huang, "A new approach to construct similarity measure for intuitionistic fuzzy sets," *Soft Comput.*, vol. 23, no. 6, pp. 1985–1998, Mar. 2019.
[27] Y. Song, X. Wang, J. Zhu, and L. Lei, "Sensor dynamic reliability evaluation based on evidence theory and intuitionistic fuzzy sets," *Int. J. Speech Technol.*, vol. 48, no. 11, pp. 3950–3962, Nov. 2018.

**YANLI LU** was born in Shaanxi, China, in 1979. She received the Ph.D. degree from Air Force Engineering University, in 2008. She is currently a Lecturer with the College of Air and Missile Defense. She has published more than 20 articles in rough sets, intuitionistic fuzzy sets, evidence theory, and uncertainty reasoning.

**XIAOLI LEI** was born in Shaanxi, China, in 1982. She received the Ph.D. degree from Shaanxi Normal University, in 2007. She is currently a Lecturer with the College of Air and Missile Defense. Her research interests include fuzzy sets, evidence theory, and uncertainty reasoning.

**ZHIPING ZHOU** was born in Gansu, China, in 1983. He received the M.D. degree from Air Force Engineering University, in 2011. He is currently a Lecturer with the College of Air and Missile Defense. His research interests include threat assessment, fuzzy sets, rough sets, and uncertainty reasoning.

**YAFEI SONG** (Member, IEEE) was born in Henan, China, in 1988. He received the Ph.D. degree from Air Force Engineering University, in 2015. He has been a Postdoctoral Researcher with Air Force Engineering University since April 2017, where he is currently a Lecturer with the College of Air and Missile Defense. He has published more than 30 articles in evidence theory, fuzzy sets, and uncertainty reasoning.