

## 적기의 위협 평가 자동화를 위한 퍼지 규칙 방법론

최병주<sup>1)</sup> · 김지은<sup>2)</sup> · 김진수<sup>2)</sup> · 김창욱<sup>\*,1)</sup>

<sup>1)</sup> 연세대학교 정보산업공학과

<sup>2)</sup> 국방과학연구소 제1기술연구본부

### Fuzzy Rule-Based Method for Air Threat Evaluation

Byeong Ju Choi<sup>1)</sup> · Ji Eun Kim<sup>2)</sup> · Jin Soo Kim<sup>2)</sup> · Chang Ouk Kim<sup>\*,1)</sup>

<sup>1)</sup> Department of Information and Industrial Engineering, Yonsei University, Korea

<sup>2)</sup> The 1st Research and Development Institute, Agency for Defence Development, Korea

(Received 13 July 2015 / Revised 10 November 2015 / Accepted 18 December 2015)

#### ABSTRACT

Threat evaluation is a process to estimate the threat score which enemy aerial threat poses to defended assets. The objective of threat evaluation is concerned with making an engagement priority list for optimal weapon allocation. Traditionally, the threat evaluation of massive air threats has been carried out by air defence experts, but the human decision making is less effective in real aerial attack situations with massive enemy fighters. Therefore, automation to enhance the speed and efficiency of the human operation is required. The automatic threat evaluation by air defense experts who will perform multi-variable judgment needs formal models to accurately quantify their linguistic evaluation of threat level. In this paper we propose a threat evaluation model by using a fuzzy rule-based inference method. Fuzzy inference is an appropriate method for quantifying threat level and integrating various threat attribute information. The performance of the model has been tested with a simulation that reflected real air threat situation and it has been verified that the proposed model was better than two conventional threat evaluation models.

Key Words : Air Defence(대공 방어), Threat Evaluation(위협 평가), Fuzzy Inference(퍼지 추론)

#### 1. 서론

Paradis *et al.*은 위협 평가를 “어떤 개체가 방어 부대나 이해 관계에 악의, 손상 또는 피해를 가할 의도

와 그것으로 야기되는 위협 수준에 따라 순위를 결정하는 지속적인 과정”으로 정의하였다<sup>1)</sup>. 위협 평가의 목적은 임의의 방어 자산을 향하는 개별 개체의 위협 수준을 추정하는 것으로, 위협 평가를 위해서는 공중 위협이 향하는 목표물과 개체의 위협 수준을 대표하는 위협값을 필요로 한다<sup>2)</sup>. 즉, 적이 의도하는 아군의 지상 목표물이 무엇인지 예측하고 위협 수준을 정량적인

\* Corresponding author, kimco@yonsei.ac.kr

Copyright © The Korea Institute of Military Science and Technology

값으로 산출하는 방법에 대한 논의가 요구된다. 위협 평가의 결과는 교전 우선 순위를 지정할 뿐만 아니라 위협 대응력에도 중대한 영향을 미친다. 특히, 다양한 위협체가 침투하거나 보호할 자산이 많을 경우 그 중요성은 더욱 증가한다.

대공 방어 임무는 전장 상황을 실시간으로 평가하고 위협을 주는 적의 목표물에 가용한 방어 무기를 할당하여 우군의 주요 방어 자산을 보호하는 것을 그 목적으로 한다<sup>3)</sup>. 이는 탐지된 공중 위협의 정성적인 위협 가치를 정량값으로 전환하는 방법에 주안점을 둔다. 위협체를 순위화 하는 것은 위협 평가의 주된 활동으로 이를 위해서는 수많은 위협 변수를 평가하고 수치화하는 특정 기법이 요구된다. 그러나 일련의 위협 평가 과정은 오랜 경험을 통해 축적된 방공 운영자들의 주관적 판단에 의존한다. 이러한 인적 평가 방법은 짧은 시간에 대규모 위협체를 평가해야 하는 전면전 상황에서 취약성이 예상된다. 따라서 전장 정보 융합 모델을 통한 위협 평가 자동화는 복잡한 작전 환경에서도 신속한 작전 템포가 요구되는 현대전의 핵심적인 과제로 대두되고 있다.

## 2. 관련연구

위협도를 평가하는 기법은 크게 두 가지로 나뉜다. 먼저 수리적 기법으로, 시선 방향의 속도 벡터를 고려한 RSV-M(Radial Speed Vector Method)과 최근접점을 이용하는 CPA-M(Closest Point of Approach Method)이 있다<sup>4)</sup>. 두 가지 방법은 도착 임박도를 위협성 결정 요인으로 가정하고, 비행 경로와 접근 속도에 따라 소요 시간을 추정하여 위협을 순위화 한다. 이에 반하여 인간과 같이 여러 가지 정보를 통합하여 위협 평가를 수행하는 인공 지능 기법이 있는데 종류는 다음과 같다. 애매하고 모호한 정보의 가치 손실을 방지하는 퍼지 추론 방법은 Johansson<sup>2)</sup>과 Liang<sup>5)</sup> 등에 의해 연구되었다. 이 방법은 소속 함수(Membership Function)와 추론 규칙을 어떻게 정의하는가에 따라 성능이 변화되는 단점이 있다. 인공 신경망을 활용한 위협 평가는 Dong and Qing<sup>6)</sup>과 Azak and Bayrak<sup>7)</sup>이 제안하였는데, 학습 데이터의 크기에 따른 성능 변화와 과적합 등이 주된 문제점이다. Okello and Thomas<sup>8)</sup>는 위협체의 능력치(Capability)를 정량화하기 위해 베이지안 추론으로 위협체의 종류(기종)를 예측하였다. 한편, Liebhaber and

Fehér<sup>9)</sup>는 미해군의 방공 수행자들을 관찰하여 17가지 위협 변수를 특정하고, 미예측 행위에 가중값을 부여하는 규칙 기반의 위협 평가 모델을 개발하였다.

전통적으로 위협도 산출을 위한 평가 함수의 모델링에는 위협체의 능력치(Capability)와 의도성(Intention)을 판별하는 입력 변수가 사용되었다<sup>10,11)</sup>. 능력치는 방어 자산에 손상이나 피해를 가할 수 있는 공격력을 의미한다. 위협체 종류, 장착 무장의 개수와 효과, 기동 능력 등이 이에 해당된다. 반면, 의도성은 피해를 가할 적의 의지나 결심으로써 속력과 방향, 편대 공격 전술, 기만 비행 등으로 예측할 수 있다. 그러나 이것을 해석하고 정량화하는 것은 상당히 어려운 작업이다. 공격 전술이나 기만 비행 등과 같은 정성적인 정보의 불확실성은 산출된 결과값의 신뢰도를 저하시킨다. 이에 반하여 측정된 센서 데이터를 통한 위협도의 산출은 결과에 대한 설명과 해석이 용이하다. 따라서 다양한 센서 데이터의 가치를 정량화하고 이를 융합하는 방법에 대한 연구가 필요하다.

감시 레이더 등을 통하여 측정되는 센서 데이터는 CPA-M이나 RSV-M과 같은 수리적인 평가 방법에 주로 이용된다. 하지만 다양한 위협 변수의 반영이 부족하여 위협체가 공격을 완료하고 귀환하는 상황 등에서 비합리적인 결과가 나타난다. 이에 반해, 퍼지 추론은 전문가의 여러 가지 평가 규칙과 입력 정보가 반영되어 접근 위협체의 다양한 상태가 평가되고 합리적인 위협값이 산출된다. 따라서 본 연구에서는 측정된 센서 데이터를 이용하여 대공 방어 상황에 적합한 퍼지 추론 위협 평가 모델을 제안하였다.

## 3. 제안 방법론

### 3.1 퍼지 논리

퍼지는 언어 표현을 정량화하는 방법으로 Zadeh<sup>12)</sup>에 의해 정립되었다. 퍼지 논리는 전통적인 부울 논리(Boolean Logic)의 집합 개념과 구별되는 다치 논리(Multi-Value Logic)로써, 퍼지 집합  $A$ 는 전체 집합  $X$ 의 요소  $x$ 와 집합에 대한 소속도를 나타내는 소속 함수  $\mu_A(x)$ 로 정의하며,  $A = \{(\mu_A(x)/x) \mid x \in X\}$ 로 표현할 수 있다. 또한, 퍼지 집합  $A$ 에 대한  $x$ 의 소속도는  $[0,1]$ 로써,  $\mu_A : X \rightarrow [0,1]$ 로 나타낼 수 있으며 이는 퍼지 집합에 대한 확정성(Certainty)을 의미한다<sup>13)</sup>.

3.2 퍼지 규칙 위협 평가

다변수 위협 평가를 수행하는 방공 전문가의 판단기준을 정확히 반영하기 위해서는 그들의 인식 체계를 대변하는 언어적 표현에 대한 적절한 모형이 필요하다. 인간의 이성 과정을 반영하는 퍼지 논리는 수학적 접근의 한계를 나타내는 정보의 불확실성(Uncertainty)을 다루기에 유용한 방법론이다. 본 연구에서는 다음의 퍼지 추론 과정을 제안하여 위협도를 산출한다.

단계 1. 퍼지화(Fuzzification)

인간의 의식 과정을 대변하는 언어는 그 표현에 있어 의미적 모호성을 가진다. 퍼지화는 입력 정보를 언어적 표현(퍼지 집합)에 대해 소속도를 부여함으로써, 그 해석의 다양성을 보존한다. Fig. 1은 퍼지화의 예를 보여준다. 거리정보 32.4 km는 해당 소속 함수를 통해 근거리(Low), 중거리(Medium), 원거리(High) 집합으로 퍼지화된다. 이때, 각 퍼지 집합에 대한 소속도 0.71, 0.50, 0.13은 거리 정보를 수치화한 것으로, “가깝다(Low)”, “보통(Medium)”, “멀다(High)”에 대한 소속 강도를 표현한 것이다. 이러한 방법으로 Table 1의 위협체에 대한 다섯 가지 입력 정보(거리, 고도, 속도, 최근접점, 상대방위)는 Fig. 2의 소속함수를 통하여 세 가지 언어 표현(High, Medium, Low)으로 퍼지화되고, 총 5×3개의 소속도가 산출된다. Fig. 2의 소속 함수는 방

공 임무 경험을 가진 저자에 의해서 수립되었다.

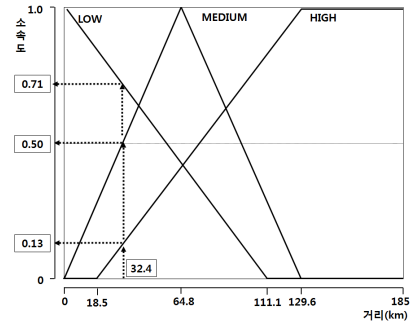


Fig. 1. Fuzzification

Table 1. Input information and linguistic value

입력 정보		언어 표현	
인덱스(i)	요소	인덱스(j)	수준
1	거리	1	High
2	고도	2	Medium
3	속력	3	Low
4	최근접점		
5	상대방위		

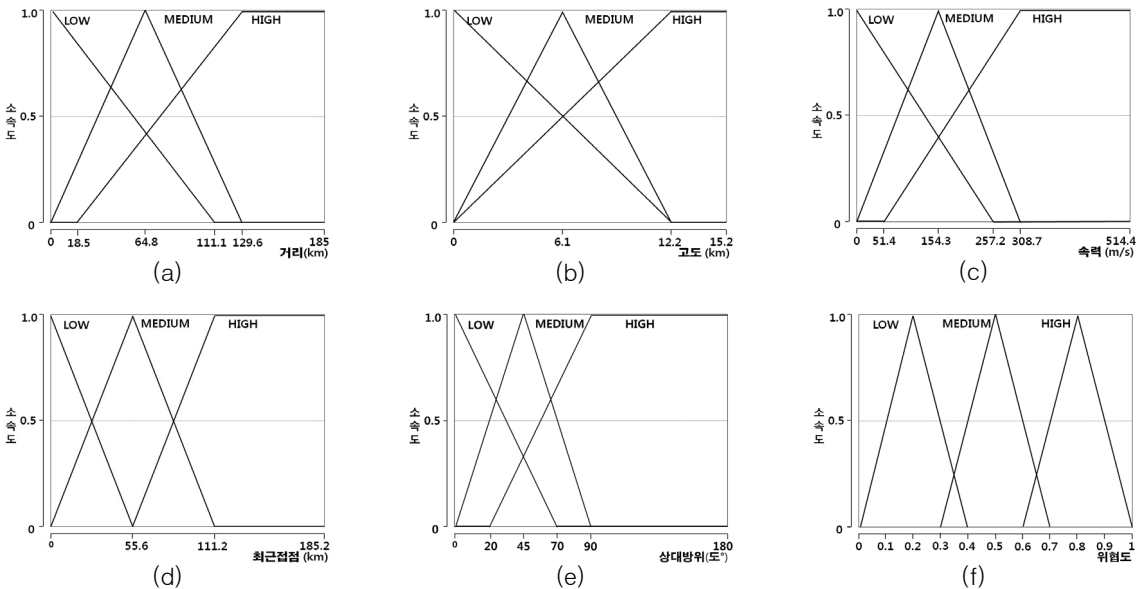


Fig. 2. Membership functions (a) Distance, (b) Altitude, (c) Speed, (d) CPA, (e) Relative course, (f) Threat value

**단계 2. 규칙 평가(Rule Evaluation)**

입력 정보를 언어 표현으로 퍼지화한 것은 위협도를 구하는 것이 목적이다. 예를 들면, 거리는 근접(Low) 할수록 위협도가 높아지고(High), 속력은 증가(High)될수록 위협도가 높아진다(High). 즉, 입력 정보에 따른 위협도의 언어적 표현에서 속력은 비례하고 거리, 고도, 최근접점, 상대방위는 반비례한다. 이를 근거로 퍼지화된 입력 정보는 규칙에서 평가된다. “IF-전건(Antecedent), THEN-후건(Consequent)” 형태를 가지는 퍼지 추론 규칙은 규칙의 명확성을 의미하는 신뢰도와 함께 Table 2에서 정의되었다. 입력 정보는 퍼지 연산자(AND)를 이용하여 전건에서 평가되는데, 퍼지 추론 규칙은 Liang<sup>[5]</sup>의 연구에서 위협도 평가력을 개선하기 위해 저자의 방공 전문 지식을 추가하여 생성하였다.

Table 2. Fuzzy inference rule

규칙	신뢰도	전건(AND)					위협도
		거리	고도	속력	최근접점	상대방위	
1	1.0	L	L	H	L	L	H
2	1.0	H	H	L	H	H	L
3	1.0	M	M	M	M	M	M
4	0.5	H	L	H	L	M	M
5	0.05	L					H
6	0.05	M					M
7	0.05	H					L

규칙 평가는 발화도(Firing Strength)로써 후건 값을 결정한다. 예를 들면, 규칙 1의 경우에 각 입력 정보의 퍼지 집합 소속도는 전건에서 평가되어 그 중에 최소값이 발화도가 되며 후건 즉, 고위협(High) 집합의 소속도가 된다. Table 1에서 입력 정보  $i$ 의 언어표현  $j$ 를 의미하는 퍼지 집합은  $A_{ij}$ 로 정의하고 위협체  $x$ 의 소속도는  $\mu_{A_{ij}}(x)$ 로 표현할 때, 규칙  $k$ 의 후건값을 의미하는 발화도  $\alpha_k$ 는 다음과 같이 계산할 수 있다.

$$\alpha_1 = \min\{\mu_{A_{13}}(x), \mu_{A_{23}}(x), \mu_{A_{31}}(x), \mu_{A_{43}}(x), \mu_{A_{53}}(x)\}$$

$$\alpha_2 = \min\{\mu_{A_{11}}(x), \mu_{A_{21}}(x), \mu_{A_{33}}(x), \mu_{A_{41}}(x), \mu_{A_{51}}(x)\}$$

$$\alpha_3 = \min\{\mu_{A_{12}}(x), \mu_{A_{22}}(x), \mu_{A_{32}}(x), \mu_{A_{42}}(x), \mu_{A_{52}}(x)\}$$

$$\alpha_4 = \min\{\mu_{A_{11}}(x), \mu_{A_{23}}(x), \mu_{A_{31}}(x), \mu_{A_{43}}(x), \mu_{A_{52}}(x)\}$$

$$\alpha_5 = \mu_{A_{13}}(x)$$

$$\alpha_6 = \mu_{A_{12}}(x)$$

$$\alpha_7 = \mu_{A_{11}}(x)$$

**단계 3. 규칙 통합(Rule Integration)**

위협체의 입력 정보는 언어 표현의 퍼지 집합으로 퍼지화되고(단계 1), 이 퍼지 정보들은 규칙을 통하여 평가되었다. 즉, 각각의 규칙은 발화도를 생성하고 이를 기준하여 위협의 소속도를 의미하는 후건값을 결정하였다(단계 2). 여기에서 만약 모든 규칙이 적용되어 활성화 된다면 동일한 언어 표현을 가지는 복수의 위협도가 발생한다. 다시 말해 규칙 1과 5는 고위협, 규칙 3, 4, 6은 중위협, 규칙 2와 7은 저위협의 소속도를 의미하는데, 동일한 위협도 언어 표현에 대해 상이한 소속도가 나타날 수 있다. 따라서 세 부류의 위협도 언어 표현에 대해 각각의 대표값으로 통합이 필요하며 이 통합 소속도를 구하는 과정은 Fig. 3에 도식하였다.

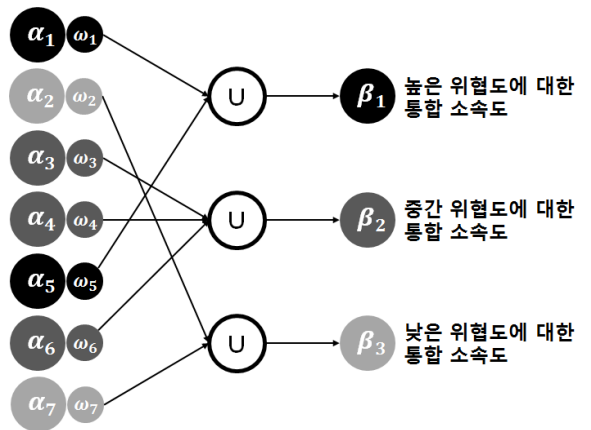


Fig. 3. Rule integration

Fig. 3에서 7개의 규칙 평가는 식 (1)을 이용하여 세 가지 부류(High, Medium, Low)로 구별하여 통합한다.

$$\beta_j = \bigcup_{\forall k} w_k \alpha_{k_j} \tag{1}$$

이때,  $\alpha_{k_j}$ 는 언어 표현  $j$ 의 위협도를 후건으로 하는 규칙  $k$ 의 발화도이다. 즉, 고위협도(High,  $j = 1$ )에 해

당하는  $\alpha_{k_j}$ 는  $\alpha_1$ 과  $\alpha_5$ 이고 이들의 조합으로 통합 소속도  $\beta_1$ 을 계산한다. 이 계산을 위해 U연산을 사용하는데 식 (2)로 표현된 퍼지 연산자 ProbOR(Probability OR)을 적용한다.  $\beta_3$ 도 동일하게 계산하되, 세 개의 집합 연산을 해야 하는  $\beta_2$ 의 경우에는 식 (3)을 사용한다.

$$\mu_A(x) \cup \mu_B(x) = \mu_A(x) + \mu_B(x) - \mu_A(x)\mu_B(x) \quad (2)$$

$$\begin{aligned} \mu_A(x) \cup \mu_B(x) \cup \mu_C(x) &= \mu_A(x) + \mu_B(x) + \mu_C(x) \\ &\quad - \mu_A(x)\mu_B(x) - \mu_B(x)\mu_C(x) - \mu_C(x)\mu_A(x) \\ &\quad + \mu_A(x)\mu_B(x)\mu_C(x) \end{aligned} \quad (3)$$

예를 들면, 고위협도에 대한 통합 소속도  $\beta_1$ 은 규칙 1과 5를, 저위협도의  $\beta_3$ 는 규칙 2와 7을 적용하여 각각의 발화도에 규칙의 신뢰도를 곱하고, 식 (2)의 ProbOR 연산자를 이용하여 계산하면 다음과 같이 표현할 수 있다.

$$\begin{aligned} \beta_1 &= \alpha_1 + 0.05\alpha_5 - 0.05\alpha_1\alpha_5 \\ \beta_3 &= \alpha_2 + 0.05\alpha_7 - 0.05\alpha_2\alpha_7 \end{aligned}$$

한편,  $\beta_2$ 는 식 (3)을 이용하여 계산한다.

$$\begin{aligned} \beta_2 &= \alpha_3 + 0.5\alpha_4 + 0.05\alpha_6 - 0.5\alpha_3\alpha_4 - 0.025\alpha_4\alpha_6 \\ &\quad - 0.05\alpha_6\alpha_3 + 0.025\alpha_3\alpha_4\alpha_6 \end{aligned}$$

#### 단계 4. 비퍼지화(Defuzzification)

이 단계에서 최종적으로 구하고자 하는 것은 언어적 위협도(High, Medium, Low)의 통합 소속도가 아니라, 위협도의 단일 위협값이다. 따라서 통합 소속도를 종합하고 스칼라 값으로 전환하는 과정이 필요하다. Fig. 4에서 위협도 소속 함수는 통합 소속도( $\beta_1, \beta_2, \beta_3$ )만큼 감소한다. 이러한 클리핑(Clipping) 과정을 통하여 해당 소속도의 불확실성을 제거하고 위협도 소속 함수의 최종 형태를 결정한다. 그리고 이것의 무게 중심을 구하면 최종적인 위협값이 산출된다(Clipped Center of Gravity Method). 이 단계를 비퍼지화라고 하며, 최종적인 위협도 소속 함수를  $\mu_C(x_n)$ 로 정의할 때 위협값  $x_n$ 을 0.1부터 1.0까지 1/10 단위로 이산화하여 무게 중심을 구하면 식 (4)와 같이 표현된다.

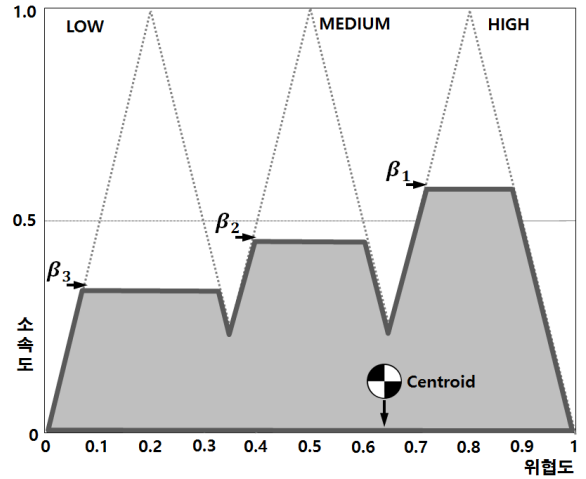


Fig. 4. Clipped center of gravity method

$$\begin{aligned} \text{Centroid} &= \frac{\sum_{n=1}^{10} x_n \mu_C(x_n)}{\sum_{n=1}^{10} \mu_C(x_n)} \\ &= \frac{\sum_{n=1}^3 x_n \mu_C(x_n) + \sum_{n=4}^6 x_n \mu_C(x_n) + \sum_{n=7}^{10} x_n \mu_C(x_n)}{\sum_{n=1}^3 \mu_C(x_n) + \sum_{n=4}^6 \mu_C(x_n) + \sum_{n=7}^{10} \mu_C(x_n)} \\ &= \frac{0.6\beta_3 + 1.5\beta_2 + 3.4\beta_1}{3\beta_3 + 3\beta_2 + 4\beta_1} \end{aligned} \quad (4)$$

#### 4. 실험 및 평가

실험을 위해 Fig. 5의 가상 전장을 모의하였는데, 20 개의 위협체가 해안선에 위치한 ●모형의 방어 자산을 공격하는 것으로 가정하였다. 공격 시나리오에는 위협체의 편대수(2기, 4기, 6기), 기종 분류(고속기, 저속기), 비행 고도(고고도, 중고도, 저고도), 침투 경로(육상, 해상) 등을 포함하였다. 이는 다양한 위협체 상황에 대한 위협 평가 결과를 비교하기 위함이다. 보편적으로 방공 운영자들은 저고도의 해상 경로를 많은 수의 편대로 군집하여 고속으로 침투하는 위협체에 보다 높은 위협성을 부여한다.

실험 시나리오와 데이터는 Table 3에 좀 더 자세하게 기술하였는데, x와 y는 경도와 위도 좌표를 의미한다. 좌표, 고도, 거리, 최근접점은 km, 비행방위와 상

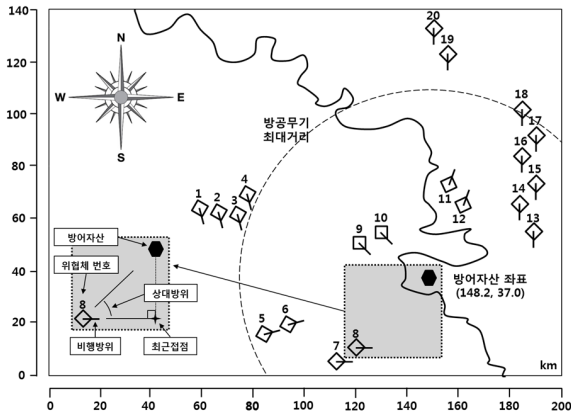


Fig. 5. Simulated air attack

대방위는 도(°), 속력은 m/s 단위를 적용하였다. 이때, 고도 정보에서 3.3 km 이하는 저고도, 10 km까지는 중고도, 그 이상은 고고도로 가정하였다. 비행방위는 북쪽의 0도로 부터 시계방향으로 동쪽은 90도, 남쪽은 180도, 서쪽은 270도를 나타낸다. 거리는 방어 자산에서 위협체까지의 상대적인 거리를 의미하며, 최근접점은 위협체의 현재 비행방위 기준하여 직선 비행을 가정할 때 방어자산에 가장 근접하는 거리를 의미한다. 상대방위는 위협체의 비행방위와 방어자산을 향하는 시선(Radial) 방위의 차이로 [0,180] 값을 가진다. 제안 방법은 CPA-M 및 RSV-M과 비교하여 평가되었다. 이에 대한 위협도 계산법은 Table 4의 실험 결과 하단에 기술하였다. 한편, 방공 전문가에게 의뢰한 위협도 판

Table 3. Test scenario and data

	위협체	시나리오	x (km)	y (km)	고도 (km)	비행방위 (도°)	속력 (m/s)	거리 (km)	최근접점 (km)	상대방위 (도°)
편대A	1	4기 고속기 중고도 해상침투	59.3	64.8	7.8	165	208.3	93.1	78.7	57.6
	2		66.7	63.0	7.5	169	210.9	85.5	75.0	61.3
	3		74.1	61.1	7.9	164	209.9	77.9	64.6	56.0
	4		77.8	70.4	7.6	167	207.3	77.9	61.1	51.7
편대B	5	2기 고속기 저고도 해상침투	83.3	14.8	2.5	75	234.1	68.5	4.7	3.9
	6		92.6	18.5	2.6	78	235.1	58.6	6.6	6.4
편대C	7		111.1	5.6	3.1	95	249.5	48.6	34.6	45.4
	8		120.4	11.1	3.2	92	248.5	38.0	26.9	45.0
편대D	9		122.2	51.9	1.6	135	258.3	29.9	7.9	15.3
	10		129.6	55.6	1.7	137	261.3	26.2	0.9	2.0
편대E	11	2기 고속기 저고도 귀환	155.6	74.1	3.0	20	232.5	37.8	-	171.3
	12		161.1	64.8	2.8	22	232.0	30.7	-	177.0
편대F	13	6기 저속기 저고도 육상침투	188.9	55.6	0.7	180	52.5	44.8	40.7	65.6
	14		183.3	64.8	0.6	182	54.0	44.8	34.2	49.7
	15		188.9	74.1	0.7	183	53.0	55.1	38.7	44.7
	16		185.2	83.3	0.8	181	53.5	59.3	36.2	37.7
	17		188.9	92.6	0.6	182	52.0	68.9	38.8	34.3
	18		185.2	101.9	0.5	183	51.4	74.7	33.6	26.7
편대G	19	2기 정찰기 고고도, 육상	155.6	125.9	10.9	185	155.4	89.2	0.4	0.2
	20		150.0	135.2	11.2	181	156.9	98.2	0.1	0.1

단 결과는 Fig. 6에서 위협체(가로축)에 따른 평가 순위(세로축)로 세 가지 방법론과 함께 비교되었다.

Table 4의 실험 결과에서 위협체 10의 경우를 보면,

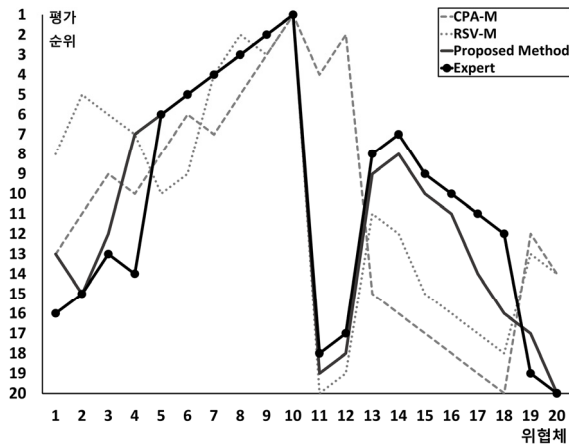


Fig. 6. Threat evaluation

CPA-M이 0.579, RSV가 0.599, 제안방법이 0.702의 위협값을 산출하여, 동일하게 1순위의 위협체로 판단하였다. 그러나 다른 경우에는 차이를 보였는데, Fig. 6에서 위협체 1부터 10까지의 순위의 추이를 볼 때, 흑색 실선의 제안 방법에 비해 CPA-M(긴 점선)과 RSV-M(짧은 점선)은 전문가 결과(원형 표식 실선)와 큰 편차를 보인다. 또한, 저고도의 육상 침투를 모사한 위협체 13-18의 경우에 더 큰 차이를 보이는데, 이것은 CPA-M과 RSV-M의 평가 방법이 고도에 대한 위협성을 고려하지 않았기 때문이다. 위협체 19-20의 경우도 동일한데, 전문가 및 제안 방법의 결과는 높은 고도에 대한 낮은 위협성을 반영하여 순위를 낮게 평가한 반면에, CPA-M와 RSV-M는 고도 변수의 반영 없이 도착 임박성만 고려하여 위협도를 산출하였다. 한편, 위협체 11-12에서 CPA-M은 이탈하는 적기의 방위 변수에 대한 고려없이 근접도만 판단하여 위협 평가 순위를 높게 부여하였다.

Table 5는 제안방법과 CPA-M, RSV-M의 성능 비교

Table 4. Test result(Threat value)

위협체	CPA-M	RSV-M	Proposed Method	위협체	CPA-M	RSV-M	Proposed Method
1	0.097	0.251	0.520	11	0.369	-0.374	0.411
2	0.109	0.309	0.501	12	0.454	-0.455	0.420
3	0.116	0.289	0.537	13	0.053	0.170	0.561
4	0.114	0.257	0.574	14	0.051	0.112	0.573
5	0.192	0.205	0.626	15	0.041	0.081	0.546
6	0.218	0.242	0.645	16	0.039	0.068	0.539
7	0.217	0.438	0.670	17	0.033	0.055	0.516
8	0.277	0.555	0.679	18	0.031	0.046	0.500
9	0.423	0.538	0.680	19	0.104	0.104	0.480
10	<u>0.579</u>	<u>0.599</u>	<u>0.702</u>	20	0.096	0.096	0.407

CPA-M(Closest Point of Approach Method)

현재의 방향과 속력으로 비행할 때 방어자산과 가장 인접하는 최근접점(CPA)을 구하고, 이를 경유하여 방어자산까지 도착하는 소요시간으로 위협성을 평가한다. 소요시간이 작을수록 위협값은 증가하므로 위협지수는 시간의 역수(1/Time)로 계산한다. 단, 상대방위가 [90°,180°]이면 시간 증가에 따라 거리가 멀어지므로 현재 거리를 기준으로 산출하였다(위협체 11,12).

RSV-M(Radial Speed Vector Method)

방어자산에 대한 위협체의 시선속도(Radial Speed)를 기준으로 방어자산까지의 소요시간을 계산한다. 소요시간이 작을수록 위협값은 증가하므로 위협지수는 시간의 역수(1/Time)로 계산한다. 단, 상대방위가 [90°,180°]이면 (-)값이 산출되는데 도착임박성은 절대값에 비례한다(위협체 11,12).

를 보여준다. 여기에서 MAE(Mean Absolute Error)와 RMSE(Root Mean Squared Error)는 전문가 결과 대비 평균적인 예측 오차를 의미한다. Table 5에서 제안 방법이 방공 임무의 전문성을 고려하여 소속 함수를 정의하고, 적절한 퍼지 규칙 통합과 퍼지값의 스칼라 전환 과정으로 설계되었기 때문에 가장 우수한 성능을 보였다.

Table 5. Performance comparison

	CPA-M	RSV-M	Proposed Method
MAE	5.70	4.50	<u>1.30</u>
RMSE	6.96	5.26	<u>2.17</u>

한편, Fig. 7은 제안 방법으로 산출한 20개 위협체(가로축)에 대한 위협도(세로축)를 보여준다. 편대A(위협1-4)의 막대 그래프 상단과 수치는 편대내 최대 위협값, 하단은 개별 위협값, 막대의 길이는 두 값의 차이를 나타내는데 나머지 편대(Clusters)도 동일하다. Fig. 5에서 방어 자산을 기점으로 편대A(위협체 1-4)는 북서쪽에, 편대F(위협체 13-18)는 북동쪽에 위치한다. 이러한 상황에서 막대 그래프 하단의 개별 위협값을 기준으로 교전 순위를 정한다면 방어 부대는 북동쪽과 북서쪽을 번갈아 가면서 교전 해야 한다. 이는 비효율적인 교전 상황으로써, 혼선이 야기되고 레이더의 추적 범위가 초과되어 무장 발사가 실패할 수 있다. 따라서 위협체를 편대 단위로 군집화하고 위협성을 평가하는 연구의 필요성이 제기된다.

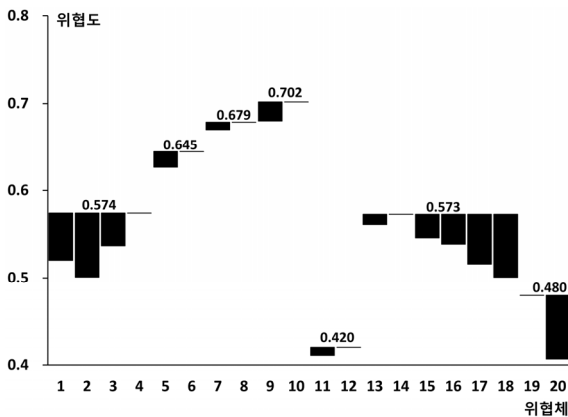


Fig. 7. Threat evaluation with respect to clusters

## 5. 결론

본 연구는 퍼지 추론을 이용한 위협 평가 방법을 제안하였다. 실험을 통하여 제안 방법이 MAE가 1.30, RMSE가 2.17의 작은 오차로 CPA-M이나 RSV-M보다 현장 전문가 평가에 부합됨을 확인하였다. 즉, 전통적인 평가 방법보다 복잡하고 다채로운 상황을 잘 반영하고, 위협체의 비행 정보를 다각도로 평가한 것이다. 하지만 위협체를 편대 단위로 교전 순위화하는 군집화 방법<sup>[14]</sup>과 이를 통합하는 온라인 위협 평가의 연구가 향후 과제로 대두되었다.

## 후 기

본 연구는 국방과학연구소의 지원을 받아 수행되었음. (UD140067CD)

## References

- [1] S. Paradis, A. Benaskeur, M. Oxenham and P. Cutler, "Threat Evaluation and Weapons Allocation in Network-Centric Warfare," Proc. 8th International Conference on Information Fusion, 2005.
- [2] F. Johansson and G. Falkman, "A Comparison between Two Approaches to Threat Evaluation in an Air Defense Scenario," Proc. 5th International Conference on Information Fusion, 2002.
- [3] J. N. Roux and J. H. Van Vuuren, "Threat Evaluation and Weapon Assignment Decision Support: A Review of the State of the Art," ORION: The Journal of ORRSA, Vol. 23, No. 2, pp. 151-187, 2007.
- [4] D. H. Hong, J. H. Yoo, S. C. Shin, S. H. Kim and Y. W. Park, "A Threat Evaluation Method on the Air Track in Short Range Air Defense Systems," Proc. Fall Conference on Korean Institute of Communication and Information Sciences, pp. 414-415, 2011.
- [5] Y. Liang, "An Approximate Reasoning Model for Situation and Threat Assessment," Proc. 4th International Conference on Fuzzy Systems and Knowledge Discovery, Vol. 4, pp. 246-250, 2007.



- [6] A. X. Dong and L. G. Qing, "Application of Neural Network in the Field of Target Threat Evaluation," Proc. International Joint Conference on Neural Network, Vol. 6, pp. 4237-4240, 1999.
- [7] M. Azak and A. E. Bayrak, "A New Approach for Threat Evaluation and Weapon Assignment Problem, Hybrid Learning with Multi-Agent Coordination," Proc. 23rd International Symposium on Computer and Information Sciences, pp. 1-6, 2008.
- [8] N. Okello, & G. Thoms, "Threat Assessment using Bayesian Networks," Proc. 6th International Conference on Information Fusion, pp. 1102-1109, 2003.
- [9] M. J. Liebhaber and B. Feher, "Air Threat Assessment: Research, Model, and Display Guidelines," Space and Naval Warfare Systems Command, San Diego, CA, 2002.
- [10] X. T. Nguyen, "Threat Assessment in Tactical Airborne Environments," Proc. 15th International Conference on Information Fusion, Vol. 2, pp. 1300-1307, 2002.
- [11] J. Roy, S. Paradis and M. Allouche, "Threat Evaluation for Impact Assessment in Situation Analysis Systems," Proc. SPIE: Signal Processing, Sensor Fusion, and Target Recognition XI, Vol. 4729, pp. 329-341, 2002.
- [12] L. A. Zadeh, "Fuzzy Sets," Information and Control, Vol. 8, No. 3, pp. 338-353, 1965.
- [13] Andries P. Engelbrecht, "Computational Intelligence: an Introduction," John Wiley & Sons, Inc. England, pp. 211-238, 2007.
- [14] B. J. Choi, J. E. Kim, J. K. Jung and C. O. Kim, "Non-centroid Clustering using Flights Adjacent Distances for Efficient Threat Evaluation," Proc. Spring Conference on Korean Institute of Industrial Engineers, pp. 175-181, 2015.