ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

정보 융합 기반 퍼지-베이지안 네트워크 공중 위협평가 방법☆

Air Threat Evaluation System using Fuzzy-Bayesian Network based on Information Fusion

윤 종 민* 최 보 민** 한 명 묵*** 김 수 현****
Jongmin Yun Bomin Choi Myung-Mook Han Su-hyun Kim

요 약

정보 기술의 발전과 더불어 전장상황에서도 정보 시스템들의 고도화가 이루어짐으로써 적기에 대한 정보 획득 및 상황분석은 전장상황에서 주요한 요소가 되었다. 전장상황 분석의 핵심 요소인 위협평가는 피아식별을 통해 식별된 항공 정보를 가지고 해당 상황에 대한 위협치를 평가하여 무기할당에 정보를 제공하는 기술로써, 전장상황의 어느 단계 보다 확실한 정보를 요구하는 단계이다. 전장상황에서 대부분의 위협평가 데이터들은 감지된 센서 값에 의해 연산되어 전달되는데, 기존의 기법들에서 발생할 수 있는 센서 데이터들의 잘못된 연관관계 표현 및 데이터 누락은 전장상황에서의 의사결정에 혼란을 야기 시킬 수 있다. 따라서 각종 센서 데이터들의 연관 관계를 올바르게 정의하고, 센서데이터 누락에 따른 예측 불가능한 전투상황에 대한 신뢰도 높은 위협치 연산 알고리즘을 이용하는 효율적인 의사결정 위협평가 시스템이 필요하다.

본 논문에서는 JDL 정보 융합 모델을 기반으로 애매모호한 관계성을 표현하는데 유리한 퍼지 이론, 데이터 습득의 불확실한 전장상황에서 위협치를 추론하고 상황에 대한 학습이 가능한 베이지안 네트워크를 하이브리드하여 새로운 위협평가 방법을 제안한다. 또, 제안된 방법을 이용하여 가상의 전장 시나리오에 따른 위협평가 결과를 보였다.

ABSTRACT

Threat Evaluation(TE) which has air intelligence attained by identifying friend or foe evaluates the target's threat degree, so it provides information to Weapon Assignment(WA) step. Most of TE data are passed by sensor measured values, but existing techniques(fuzzy, bayesian network, and so on) have many weaknesses that erroneous linkages and missing data may fall into confusion in decision making. Therefore we need to efficient Threat Evaluation system that can refine various sensor data's linkages and calculate reliable threat values under unpredictable war situations. In this paper, we suggest new threat evaluation system based on information fusion JDL model, and it is principle that combine fuzzy which is favorable to refine ambiguous relationships with bayesian network useful to inference battled situation having insufficient evidence and to use learning algorithm. Finally, the system's performance by getting threat evaluation on an air defense scenario is presented.

☞ keyword : JDL, Threat Evaluation, Fuzzy, Bayesian Network, Fuzzy-Bayesian Network

1. 서 론

위협평가(Threat Evaluation)는 상대의 항적 정보를 바탕으로 적의 공격으로부터 아군의 자산을 보호하는 것을 목적으로 하는 전술 기법이다[1]. 이는 효율적으로 자산을 보호할 수 있으며, 위협순위리스트를 통하여 적에 대한 대응 우선순위를 설정하여 격추율을 높일 수 있다. 또 다양한 표적들의 유입에 대해 보호해야 하는 자산의 수가 많을 경우, 방어 전략과 대응의 효용성을 높여주는 기법이다.

위협 평가의 목적은 적군에 대한 위협 순위 리스트를 산출하여 아군의 효율적인 무기할당을 수행 하는 데 있다. 이런 위협순위 리스트를 작성하기 위한 위협치를 계산하는 방법은 수학적 접근방식과 인공지능 기반의 접근방식이 있다. 수학적 접근 방식은 비교적 간단한 알고리즘만으로 정규화 된 위협치를 산출해 낼 수 있으며, 인공지능 기반 접근 방법으로는 퍼지와 베이지안 네트워크를 활용한 위협평가 방법[2-4]이 있다.

* 준 회 원 : 가천대학교 일반대학원 전자계산학과 석사과정
chum@daum.net
** 준 회 원 : 가천대학교 일반대학원 전자계산학과 석사과정
cbm0728@gmail.com
*** 종신회원 : 가천대학교 컴퓨터공학과 정교수
mmhan@gachon.ac.kr (교신저자)
**** 정 회 원 : 국방과학연구소
kims@add.re.kr
[2012.05/30 투고 - 2012.06/01 심사(2012/08/30 2차) - 2012./10/09 심사완료]
☆ 이 연구는 국방과학연구소의 지원에 의해 수행되었음(계약번호 UD110057ED)

그러나 전장 상황이 점차 고도화·지능화 되고 있기 때문에 인간의 지능적 행위를 반영하는 인공지능 기반의 접근 방식이 주로 연구되고 있다.

본 논문에서는 기존의 인공지능 기반 위협평가 방법으로 사용되고 있는 퍼지 이론과 베이지안 네트워크 방법을 소개하고, 각각의 방법론이 갖는 이점을 결합한 새로운 위협평가 알고리즘을 제안한다. 이 알고리즘은 유동적인 전장상황에서 연속적인 변수(Continuous variable)를 다루는 데 유리한 퍼지 기법과 불완전한 데이터 추론이 가능한 베이지안 네트워크 하이브리드하여 구현 한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 정보융합 기술 및 퍼지와 베이지안 네트워크에 대하여 설명하고, 3장에서는 제안하는 시스템 모델에 대해 알아본다. 4장에서는 시나리오를 설정하여 제안된 시스템의 평가하고, 5장에서 본 논문의 결론을 서술한다.

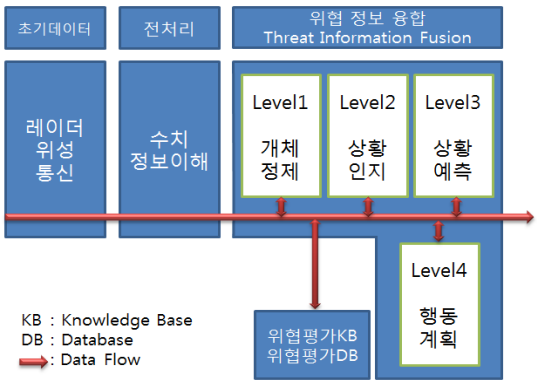
2. 관련연구

2.1 연구동향

전장상황에서 위협을 평가하는 방법으로는 수학적인 접근 방식과 인공지능 기반의 접근 방식이 있으며, 수학적인 접근 방식으로는 속도벡터를 고려한 RSV방법과 최근접 통과 예상거리를 활용한 CPA방법이 있다[5]. 수학적인 접근 방식은 계산 방식이 매우 간단한 장점이 있으나, 과거 센서 장비가 위협평가시에 사용할 수 있는 센서 정보들을 적절히 제공하지 못 할 경우에 사용하기에 유리한 방법이다. 그러나 현대전장에서 점차 다양한 센서에서 다양한 데이터를 제공 받을 수 있게 됨으로써 퍼지 및 베이지안 네트워크 같은 인공지능 기반의 접근방식이 점차 활발히 연구되고 있다.

2.2 정보융합

정보융합(Information Fusion)이란 같은 모집단에서 나온 서로 다른 표본들을 포함하는 데이터 집합을 결합하는 기법 또는 처리 과정을 의미한다[6]. 이는 한 모집단에 대한 여러 가지 데이터를 통해 현상에 대해 다양한 정보를 제공해 주기 때문에 상황 인지와 예측에 용이한 기법이다[7]. 따라서 이러한 이점들을 가지고 전장 상황에서 다양한 센서 데이터들로부터 상황을 인지시켜 의사 결정을 돕도록 하는 구조의 많은 기법들이 연구 중에 있으며, 그 대표적인 모델로는 JDL 모델이 있다[8].



(그림 1) 위협 정보 융합 시스템의 구조

JDL(Joint Directors of Laboratories)모델[9]은 양방향성 자료 흐름도를 순차적인 레벨관계로 나타낸 프레임 워크이다. 즉, JDL모델은 정보융합을 통한 판단 레벨이 계층화 되어있어 계층마다 각각의 요소기술들 을 명시하는 구조로 되어 있다. 이를 활용하여 본 논문에서는 JDL 모델에서의 정보융합 과정을 기반으로 한 위협평가 수행 시스템을 제안하고 있다. 다음 (그림 1)은 본 논문이 제안하는 전장상황에서의 위협평가 시스템의 구조를 나타낸다.

2.2.1 초기데이터

초기데이터는 전장 상황정보를 얻어지는 가공되지 않은 데이터를 의미한다. 이러한 데이터들은 레이더나 위성, 통신 등과 같은 감시 수단으로부터 정보가 수집 되어지고 인간의 그 어떤 행위도 가미되지 않은 순수 초기의 데이터이다.

2.2.2 전처리

전처리는 초기 데이터들의 1차 가공 단계에 해당된다. 즉, 앞서 얻어진 초기 데이터들을 해당 위협정보융합 모듈에서 적합한 특징들만을 추출 하여 다음 단계에서 데이터들을 효율적으로 사용할 수 있게끔 데이터들을 최적화 시켜준다.

2.2.3 위협 정보 융합

정보 융합이 실제적으로 일어나는 단계이다. 이 단계에서는 초기데이터와 전처리를 통해 가공된 데이터들을 해석하고 융합하여 현재의 상황을 인지하여 이에 대해

위협 상황에 대해 분석 및 예측을 수행하게 된다.

・1레벨 : 개체정제(Entity Refinement)

1레벨은 전처리에서 얻은 데이터들을 분석하여, 개체를 정의하고, 연관성이 낮은 정보는 제거한다.

・2레벨 : 상황인지(Situation Awareness)

2 레벨은 1레벨에서 판단된 개체들 간의 관계를 정의한다. 개체들 간의 관계란 적군의 타깃-아군자산과의 관계 및 타 타깃들 간의 관계를 의미한다.

・3레벨 : 상황 예측(Situation Prediction)

3레벨은 1레벨과 2레벨에서 얻은 정보를 이용하여 적기가 아군 자산에 미칠 수 있는 영향과 앞으로의 대처 방법에 대한 의사 결정을 하게 되는 단계이다. 보다 세밀하고 정확한 상황 판단을 위해서 퍼지(Fuzzy) 기법을 이용하고, 신뢰성 있는 미래 예측을 위해 베이지안 네트워크(Bayesian Network)를 이용하기로 한다.

3레벨에서 상황 예측을 위한 근거가 부족 할 시에는 판단을 보류하고 2레벨과 1레벨에게 해당 상황 예측을 위한 정보 수집 요구의 피드백을 요구하게 된다.

・4레벨 : 행동 계획(Action Planning)

4레벨은 3레벨의 예측 결과에 의해 제공된 정보를 가지고 상황을 판단하여 의사결정에 대한 행동을 계획하는 단계 이다.

2.3 공중 위협 파라미터

전장에서의 공중 위협(Threat)이란, 자산의 손실을 발생시키는 원인이나 행위를 말한다. 이러한 위협은 점차 다양화되어 항공기, UAV, 탄도미사일, 레이저 유도 폭탄과 같은 다양한 종류의 형태로 위협의 수단이 점차 증가하였으며, 공중공격에 대한 영향력은 전장의 성패를 좌우하는 요소이다.

이러한 위협은 적기가 가지는 의도성(Intent)과 능력(Capability)의 조합이라고 할 수 있으며[4], 적이 가지는 위협의 정도는 의도성, 능력과 더불어 (거리·시간상에서의) 근접성(Proximity)의 관계를 통하여 정해지게 된다[3]. 따라서, 위협평가는 정보융합의 한 분야로 전장에서 발생되는 각종 센서 데이터들의 융합을 통하여 상황을 인식하고, 이를 통하여 위협치를 얻어낼 수 있다. 다음 (표 1)은 위협에 영향을 미치는 파라미터를 정리한 것이다.

위협은 각각의 파라미터의 관계성과 수치에 따라서 결과가 달라 질 수 있기 때문에 각 파라미터의 정밀한 세팅이 위협평가의 신뢰성을 더할 수 있다. 여기서 파라미터간의 관계성 및 수치에 따른 추론이 가능한 방법으로 퍼지 기법과 베이지안 네트워크를 활용할 수 있다.

(표 1) 위협 파라미터

파라미터	종 류
Intent	Kinematics, Maneuvers, Altitude 등
Capability	피아식별, Speed, Weapon envelope 등
Proximity	CPA, TBH, Rate of Change 등

2.4 퍼지기반 위협평가

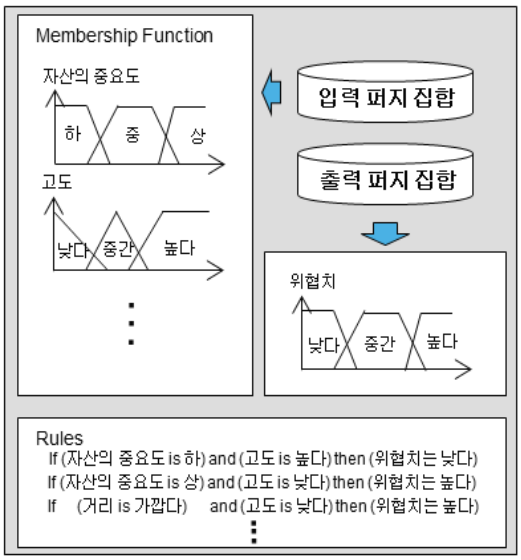
퍼지(Fuzzy Logic)는 현상의 불확실한 상태를 표현해주는 방법으로써[10], 인간의 주관적인 사고나 판단의 과정을 모델화하고 이것을 정량적으로 취급하는 표현수단으로서 '퍼지집합'을 제창한 것에서 시작되었다. 퍼지이론은 인간이 사용하는 모호한 표현을 그대로 처리하고자 하는 이론이며, 이것은 정보의 손실을 줄여 보다 좋은 결론을 유도하고자 하는 학문이라고 할 수 있다[11].

퍼지 집합에 있어서 퍼지부분집합(fuzzy subset) A는 전체집합(universal set) X에 대해 $\mu_A(X) : X \rightarrow [0,1]$로 표현된다. 여기서 귀속도 함수 $\mu_A(X)$의 값이 1값에 가까울수록 원소가 퍼지 집합에 속하는 정도가 크고, 그 반대로 0값에 가까워질수록 원소가 집합에 속하는 정도가 작다고 할 수 있다.

기존의 이진논리를 바탕으로 했던 여러 추론 방법론들에서는 규칙의 조건부에 있는 명제와 사실 사이에 약간의 차이가 존재하더라도 추론 도출에 많은 어려움을 겪는 제약이 있었다. 그러나 기존의 추론 방법들에 퍼지이론이 적용되면서부터 단순한 이진논리만으로 처리할 수 없었던 다양한 추론 상황들에 대해 그 제약을 극복 할 수 있게 되었다[12].

또한, 기존의 추론 방법론들은 언어나 현상을 표현함에 있어서 어려움이 많이 있었지만, 퍼지는 '약간'이나 '매우'와 같이 명확하지 않은 상태 또는 상황을 표현하고 활용할 수 있는 특징으로, 이러한 어려움을 극복할 수 있게 되었다[10]. 즉, 퍼지는 If-Then 알고리즘을 기반으로 사용하고 있으며, 요소들 간의 관계를 모델링하고 표현하는데 최적화된 기법 이라고 할 수 있다.

다음 (그림 2)는 퍼지를 이용하여 요소간의 관계를 모델링하고 타겟의 위협치를 계산하는 과정이다.



(그림 2) 위협치를 계산 하는 과정

(그림 2)의 위협치 계산과정에서 보는 바와 같이 전장상황에서 발생되는 적기에 대한 센서 데이터 값들은 요소간의 관계가 이분법적으로 명쾌하게 정의하기 힘들고 서로 애매모호한 연관성을 가지고 있다. 또 요소간의 관계성이 복잡하게 얽혀 있는 경우도 있다.

따라서 전장상황의 진행에 따라 발생되는 데이터들의 변화를 인지하고, 그 결과를 즉시적으로 산출해 낼 수 있는 퍼지는 위협평가 도구로 이용된다.

2.5 베이지안 네트워크 기반 위협평가

믿음 네트워크(Belief Network)라고도 불리는 베이지안 네트워크(Bayesian Network)는 확률적 추론 그래픽모델이며, 방향성 비순환 그래프이다(DAG:Directed Acyclic Graph)[6]. 이 네트워크 모델은 각 노드간의 연관성을 나타내는 호(Arc = Edge)로 구성되어 있으며, 노드는 확률변수를 의미한다. 노드들 간의 관계는 방향을 가진 호로 표현이 되는데, 이는 원인이 되는 부모 노드와 결과가 되는 자식 노드로 나누어진다. 각 노드는 여러 개의 속성을 가질 수 있고, 각 속성 값의 합은 1이 된다. 부모를 가진 자식 노드들은 의존 관계를 나타내는 확률 테이블(CPT: Conditional Probability Table)을 가지고 있고 부모가 없는 노드들은 초기 확률 값을 갖는다.

다음은 자식노드의 확률 값을 추론 해 내는 식이다.

$$P(A) = \sum_i P(A|B_i)P(B_i)$$

위의 식에서 B는 A노드의 부모 노드이고 i는 부모이다. 이때, 노드의 확률 분포 $P(x_1,x_2,....,x_n)$는 다음과 같이 나타난다.

$$P(x_1,x_2,....,x_n) = \prod_i P(x_i|Parents(X_i))$$

베이지안 네트워크 모델링은 신경망, 규칙 학습 등에 비해 설계자의 사전지식을 활용하기 쉬워 기대치만큼의 성능을 쉽게 얻을 수 있다[13]. 즉, 조건부 확률 식을 활용하여 결과치를 얻을 수 있으며, 불확실한 도메인 값에 대한 결과 값을 추론해 내는 분야에 많이 이용되고 있다.

베이지안 네트워크의 장점은 부분적인 증거만으로도 추론이 가능하기 때문에 불확실한 조건의 상황에서도 신뢰성 있는 확률 값을 추론하는데 유리하고, 베이지안 네트워크 그 자체로 상황에 대한 적응력이 있다는 점이다[14]. 이는 구하고자 하는 노드의 세팅된 CPT테이블에 의존하여 부모노드로가 제공하는 경험적 근거에 의해 예측치가 산출되게 되고, 이러한 과정이 하나의 경험적인 Case가 된다. 또한 이 산출된 Case 집합을 바탕으로 학습이 수행하여 변화된 상황에 대응하는 네트워크의 확률적 특성을 개선시킬 수 있다.

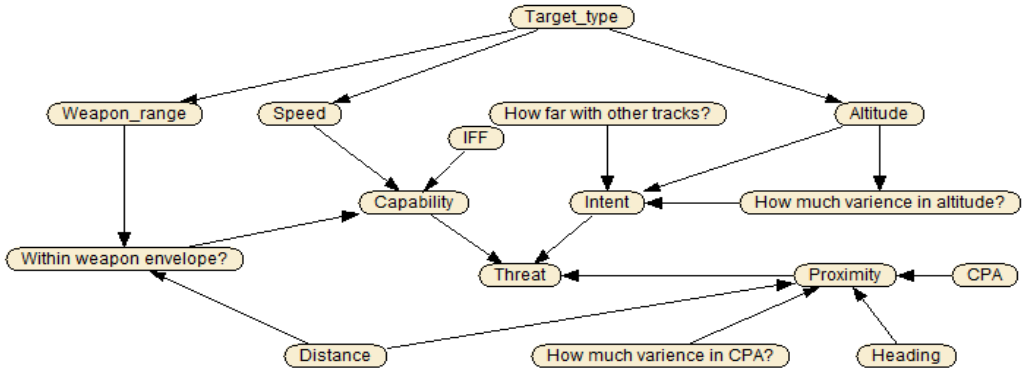
즉, 각 변수들 사이의 의존관계를 그래프화 함으로써 실세계 데이터 영역에 대한 내용을 명확하게 가시화 할 수 있으며, 전문가의 배경지식에 의해 셋팅 되어진 CPT에 의해 앞으로 일어날 상황에 대한 예측을 추론해 낼 수 있다.

그러므로 베이지안 네트워크는 전장 상황에서 발생하는 적기의 움직임에 지속적으로 적응 할 수 있으며, 각각의 센서 데이터들의 학습과 더불어 현재 아군이 갖고 있는 전술적 특성 및 아군 정보를 입력함으로써 신뢰도 높은 위협치 추론을 가능하게 한다.

3. 제안하는 위협평가 시스템

3.1 설계의 범위

2장에서 살펴본 바와 같이 위협평가는 정보융합 과정이다. 이 중 JDL 1레벨까지의 작업은 위협평가의 전 단계인 항적융합단계에서 주로 이루어지고 있다. 따라서



(그림 3) 퍼지-베이지안 네트워크에서 사용되는 기본적인 위협파라미터 구성도

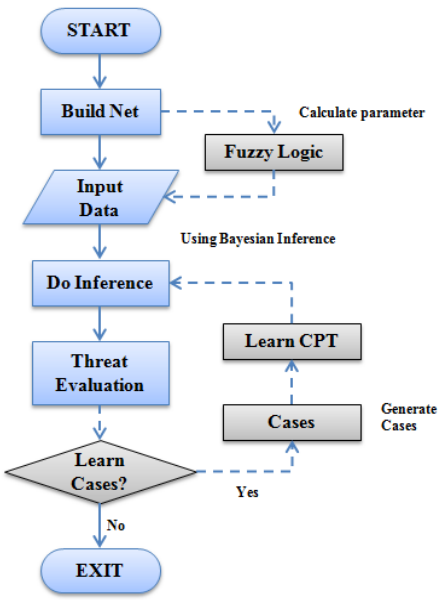
이번 연구에서는 JDL 모델의 2레벨 이후 단계에 대한 설계를 진행한다.

3.2 퍼지-베이지안 네트워크 위협평가

전장상황은 시간에 따라 유동적이며 기존의 위협평가 시스템에서 사용되는 로우 데이터의 획득 과정에서 여러 가지의 noisy의 발생은 데이터를 변질시키거나 유실시키기도 한다. 본 연구에서는 이러한 다이나믹한 전장상황을 고려하여 데이터의 변질 혹은 유실된 상황에서도 신뢰성 있는 위협치를 추론을 수행하고자 새로운 Fuzzy-Bayesian 융합의 위협평가 시스템을 제안한다.

본 연구가 제안하고자 하는 시스템은 변질되어 모호해진 데이터들의 관계를 재 정련해주는 기능의 퍼지시스템과 데이터 처리 과정에서 몇몇 데이터가 유실되는 상황에서도 신뢰성 높은 위협치를 추론해 낼 수 있는 베이지안을 융합시킨 시스템이다. 즉, 퍼지이론과 베이지안 네트워크가 가지는 단점을 보완하고 장점은 최대화하는 상호 보완적인 '퍼지-베이지안 시스템'을 제안하고 있다.

본 시스템에서 사용하는 기본적인 위협 파라미터 구성도는 (그림 3)과 같다. (그림 3)은 센서데이터에서 얻을 수 있는 각종 정보들의 연관성을 베이지안 네트워크에 적용하여 하여 공중위협 파라미터 기준으로 적절히 조정하고 배치시켜 만든 구성도이다. 각 노드는 전문가에 의해 구성된 CPT(Conditional Probability Table)가 세팅 되어 있고 최종노드는 Threat파라미터가 되며 이는 최종적으로 Intent, Capability, Proximity의 연관도를 통하여 결과값이 산출된다. 즉, Threat = Intent × Capability × Proximity로 나타낼 수 있고 각 노드는 센서에서 얻어지는 센서 데이터 및 퍼지에서 얻어온 값을 입력값으로 하는 다양한 파라미터 State값을 산출한다. 이런 과정을 거치며 변화하고 최종적으로 Threat 노드에 영향을 주어 최종적인 위협치를 추론해 낼 수 있다.



(그림 4) Fuzzy-Bayesian Network의 흐름도

(그림 4)는 퍼지-베이지안 네트워크의 흐름도를 나타낸다. 본 시스템은 시작과 동시에 적군과 아군에 대한 정보를 입력받음으로써 Build Net 프로세스를 거쳐 위협평가 네트워크를 생성해 준다. 이렇게 위협평가 환경이 조성되면 평가에 이용될 Input Data를 생성하게 되는데, 이 과정은 항적

융합단계에서 전달받은 1차 가공 데이터를 기반으로 퍼지 이론을 통해 데이터의 모호성을 판별하고 데이터들이 다음 프로세서에 적합하게 이용되도록 재정련 하는 단계이다. 여기서 얻어지는 정보들은 (그림 3)에 보이는 Proximity 파라미터, Capability 파라미터, Intent 파라미터 및 이 노드들의 자식 노드들의 상태 값(State 변수)을 의미한다.

다음은 베이지안 네트워크를 이용한 추론 단계이다. Do Inference 단계는 앞서 전해 받은 Input Data의 정보들을 가지고 베이즈 이론의 조건부 확률 연산을 통해 추론이 이루어지게 된다. 여기서, 퍼지에서 미처 전달받지 못하거나 정련해 주지 못해 몇몇 노드들의 Input Data 부재가 발생한다 할지라도 각 노드들이 지닌 CPT를 기반으로 위협치를 추론해 낼 수 있다.

또한, 이러한 위협 평가 과정이 진행되고 나면 학습단계를 거치게 되는데 이 단계는 사용자의 의지에 의해 수행된다. 학습단계를 통하여 전장상황의 유동적인 변화에 대해 유연하게 대처하여 보다 신뢰성 높은 위협치를 산출 해 낼 수 있는 환경을 구축해 줄 수 있다.

4. 실험 및 결과

본 장에서는 제안하는 위협평가 시스템의 이해를 돕기 위하여 전장 상황에 대한 세 가지 가상 비행 시나리오를 만들어 적용한다.

각각의 시나리오에 시뮬레이션을 수행하고, 각 시나리오의 흐름에 따라 얻어지는 위치, 시간, 속도 및 거리 값들은 2차원 선형 그래프로 표현 한다. 또 각각의 시나리오 상황에 대한 시간변화와 위협치의 변화 값을 이용하여 본 시스템을 검증한다. 본 실험에서 이용하는 로우 데이터들은 적기와 자산에 대한 정보들로 구성되어 있으며 그 표현 형식은 다음 (표 2)와 같다.

(표 2) 로우 데이터 형식

구분	입력형식	요 소
적기	수치값	입력시간, 트랙번호, 위치좌표, 거리, 고도, 속력, 방향각, 가속도, CPA, TCPA, 피아식별
자산	수치값	입력시간, 절대 위치, 자산중요도, 무기 범위, 무기 사거리

전장 상황의 인지하고 이를 통하여 예측을 수행하는 파라미터 값들은 다음 (표 3)과 같다.

(표 3) 상황인지와 예측을 위한 파라미터 타입

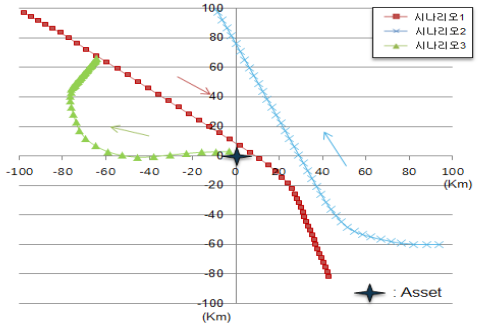
구분	입력형식	요 소
Intent	Low Medium High	트랙간 거리, 운동방향, 고도변화량, 절대고도
Capability	Low Medium High	속도 변화량, 피아식별, 자산과의 상대거리, 자산의 중요도, 무기사거리
Proximity	Close Medium Far	CPA 변화량, 거리변화량, 절대CPA, 절대거리

3.2절에서 보였던 (그림 3)은 본 논문에서 사용한 퍼지-베이지안 네트워크의 구성도이다. Threat변수는 Intent, Capability, Proximity 매개변수들에 직접적으로 의존하며, 위협은 Capability, Intent, Proximity의 조합이라고 생각할 수 있다. 따라서 이 세 Parameter를 중심으로 네트워크가 설계 되었고, 세 파라미터들에 영향을 미치는 요소들을 자식노드로 설정함으로써 본 네트워크를 구성하여 실험을 진행하였다.

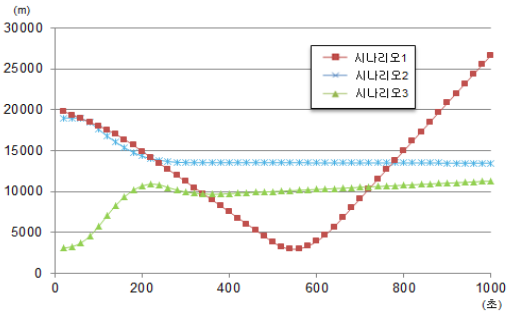
4.1 실험 시나리오 설정

실험 시나리오는 공중 전장상황에 대한 각기 다른 세 가지 비행 시나리오가 설정 되어 있으며 본 모의실험은 이를 시뮬레이션 하여 진행 한다. 시나리오에는 자산으로부터 점차 가까워 주변을 지나가며 정찰임무를 수행하는 적기1, 점차 고도를 낮추며 공격하는 적기2, 이와는 반대로 공격을 마치고 자산으로부터 점차 달아나는 적기3에 대한 비행 궤적을 모의한 것들로 구성한다.

각각의 시나리오는 1000초간의 비행을 시뮬레이션 하였으며, (그림 5)는 수평면상의 각 시나리오 궤적을 표현하고, (그림 6)은 각 시나리오의 수직면상 궤적을 표현한다.



(그림 5) 전체 시나리오 수평면상 궤적

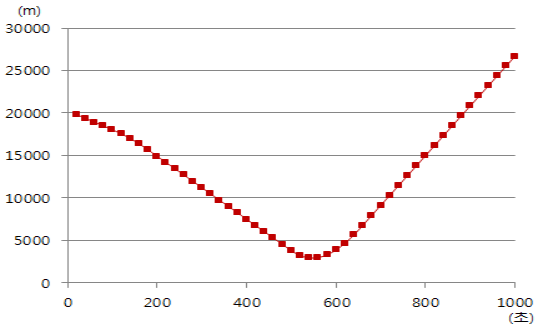


(그림 6) 전체 시나리오 수직면상 궤적

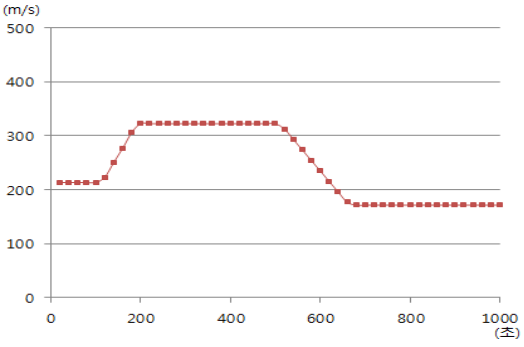
1. 시나리오1 : 적기1

시나리오1은 공격을 목표로 하는 적기로서, x좌표 -100km, y좌표 100km 지점에서 자산 쪽으로 속도를 높이고, 고도를 낮추며, 접근해오다가 500초가 지난 후에 공격을 하게 된다. 그 후 고도를 높이고 속도를 낮추며 퇴각하는 시나리오이다.

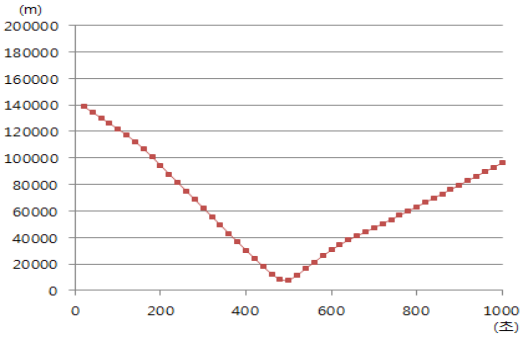
시간별 고도, 속도, 거리 변화는 (그림 7)과 같다.



(그림 7(a)) 시나리오2 고도 변화



(그림 7(b)) 시나리오2 속도 변화

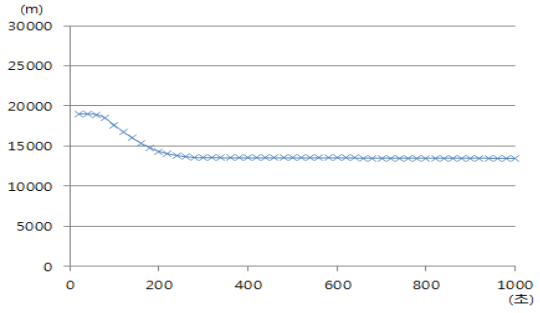


(그림 7(c)) 시나리오2 거리 변화

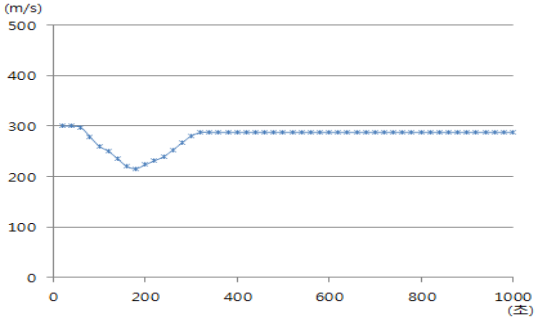
2. 시나리오2 : 적기2

시나리오 2는 정찰 임무를 수행하는 적기에 대한 시나리오로, x좌표 100km, y좌표 -60km 지점에서 움직임을 시작하여 자산 쪽으로 거리를 좁혀오며, 고도를 낮추다가 일정 수준에서 고도와 속도변화 없이 자산과 멀어지는 시나리오이다.

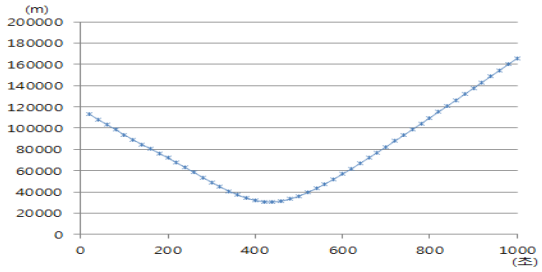
시간의 흐름에 따른 고도, 속도, 거리변화는 (그림 8)과 같다.



(그림 8(a)) 시나리오1 고도 변화



(그림 8(b)) 시나리오1 속도 변화

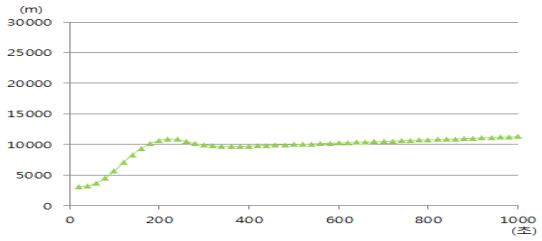


(그림 8(c)) 시나리오1 거리 변화

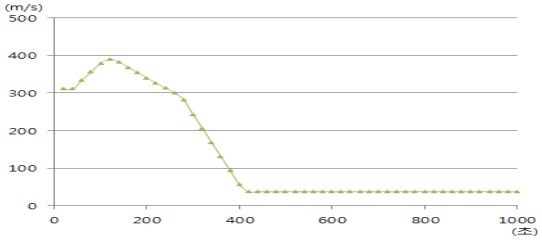
3. 시나리오3 : 적기 3

시나리오3은 이미 공격을 마치고 난 후 퇴각하는 적기에 대한 시나리오로, x좌표 -0.3km y좌표 0.3km 지점에서 고도와 속도를 높이며 멀어지고, 400초가 지난 후에 속도를 완전히 낮추는 시나리오 이다.

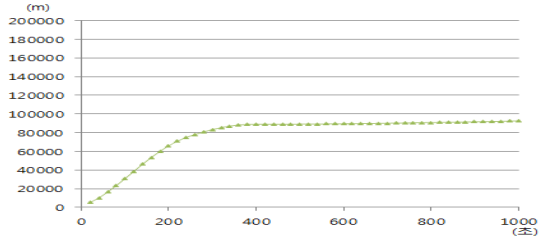
시간별 고도, 속도, 거리 변화는 (그림 9)와 같다.



(그림 9(a)) 시나리오3 고도 변화



(그림 9(b)) 시나리오3 속도 변화

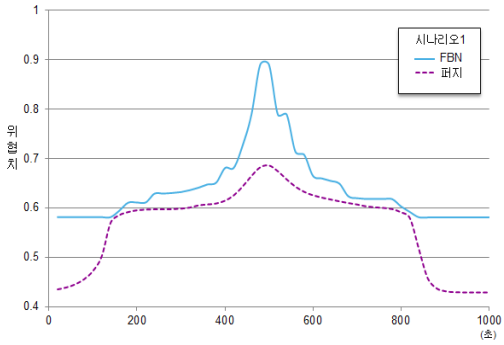


(그림 9(c)) 시나리오3 거리 변화

4.2 위협평가 알고리즘 성능

본 장에서는 전장에서 센서 데이터인 속도 측정값이 들어오지 않는 상황을 모의한 실험을 진행한다.

다음 (그림 10)은 시나리오1 상황에서 속도 값을 센서에서 제공해주지 않았을 때 퍼지-베이지안 네트워크와 퍼지를 이용한 위협치 변화를 보인다.



(그림 10) 속도 데이터가 유실된 위협평가 결과

(그림 10)을 보면 각 위협평가 알고리즘이 비슷한 추이를 보이는 것을 확인 할 수 있으나, 퍼지의 경우 최대 위협치와 최소 위협치가 상대적으로 너무 낮은 것을 확인 할 수 있다.

특히, (표 4)를 보면 구간별 평균 위협치는 적기1이 자산에 최근접하는 400~600초 구간에도 상대적으로 낮은 위협치를 보이는 것을 확인 할 수 있다.

(표 4) 구간별 평균 위협치 변화

시간(초) / 구분	0~200	200~400	400~600	600~800	800~1000
FBN	0.585	0.629	0.772	0.636	0.584
퍼지	0.499	0.599	0.654	0.610	0.478

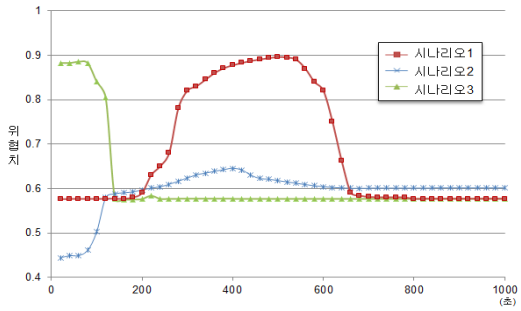
위 실험 결과에서 볼 수 있듯이 상대적으로 퍼지는 전장상황에서 흔히 발생할 수 있는 센서 데이터의 유실에 취약할 수 있는 것을 확인 하였다.

4.3 위협평가 결과

본 장에서는 퍼지와 베이지안 네트워크를 이용한 위협평가 결과와 제안하는 퍼지-베이지안 네트워크를 이용한 위협평가 결과를 비교한다.

4.2.1 퍼지를 사용한 위협평가 결과

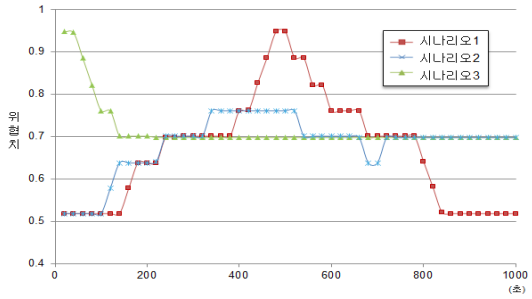
(그림 11)은 퍼지를 이용한 위협평가 결과를 표현한 그래프이다.



(그림 11) 퍼지를 사용한 위협평가

4.2.2 베이지안 네트워크를 사용한 위협평가 결과

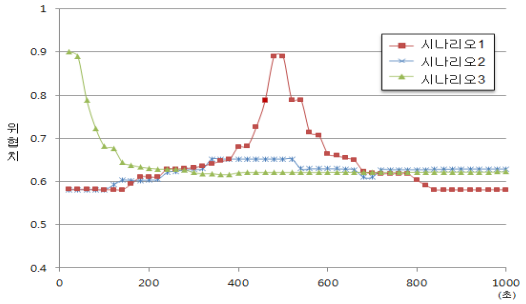
(그림 12)는 베이지안 네트워크를 이용한 위협평가 결과를 표현한 그래프이다.



(그림 12) 베이지안 네트워크를 사용한 위협평가

4.2.3 퍼지-베이지안 네트워크를 사용한 위협평가 결과

(그림 13)은 퍼지-베이지안 네트워크를 이용한 위협평가 결과를 표현한 그래프이다.



(그림 13) 퍼지-베이지안 네트워크를 사용한 위협평가

각 알고리즘을 사용하여 위협평가를 한 각 시나리오 결과는 그림 11, 12, 13과 같다.

시나리오1은 최초 약120km 떨어진 지점에서 발견된 뒤, 400초대 까지 점차 거리를 좁히며 위협치가 높아지다가 500초 이후에 점차 거리가 멀어지면서 위협치가 낮아진다. 또 (그림 7)에서 보는 바와 같이 속도와 고도변화의 폭이 작은 것을 확인 할 수 있다. 퍼지를 이용한 위협평가 결과에서는 100초 지점에서 급격한 위협 상승을 보였고 그 뒤로 400초 지점까지 완만한 위협치 변화가 일어나는 결과를 보이고 있으며, 베이지안 네트워크의 경우에는 급격한 계단식 위협치 변화를 나타내고 있다. 그러나, 퍼지-베이지안 네트워크 위협평가 결과는 위협치 변화의 폭이 작아졌으며, 급격한 계단형이 아니라, 완만한 변화를 보이고 있는 것을 확인 할 수 있다.

시나리오2는 약140km 지점에서 발견된 뒤, 고도를 낮추고 속도를 높이며, 자산쪽으로 500초 지점까지 접근해 오면서, 위협치를 점차 높여간다. 500초 지점에서 공격을 마친 뒤에는 고도 값을 점차 높이며, 속도를 낮추고 점차 자산과 멀어져감에 따라 위협치가 낮아지는 결과를 보인다. 퍼지를 이용한 위협평가 결과에서는 200초 이후의 위협치 변화가 급격하게 나타나는 결과를 보이고 있으며, 베이지안 네트워크의 경우에는 시간에 따른 위협치 변화가 계단형태를 보이고 있다. 그러나, 제안하는 위협평가 결과는 위협치 변화의 폭이 기존 알고리즘보다 작고 200초~400초 구간과 600초~700초 구간에서는 미세한 위협변화까지 표현하고 있다.

시나리오3은 최초 자산과 가장 가까운 거리에서 낮은 고도를 갖고 있어서, 높은 위협치를 보였으나, 공격후 점차 자산 쪽에서 멀어짐에 따라 위협치가 낮아지고 100초 이후에 가장 낮은 위협치를 보이고 있다. 퍼지를 이용한 위협평가 방법과 베이지안 네트워크를 이용한 위협평과

결과 150초 지점에서 이미 급격한 위협치 변화로 가장 낮은 위협수치에 접근하였으며, 그 이후 다른 위협치의 변화를 보이지 않는다. 하지만 퍼지-베이지안 네트워크 위협평가 방법은 계속해서 미세한 위협치 변화를 보이고 있는 것을 확인할 수 있다.

각각의 실험 결과를 통하여 퍼지-베이지안 네트워크를 이용한 실험 결과가 기존의 알고리즘이 가지는 단점인 급격한 변화 및 계단식 위협평가 결과를 개선하여 미세한 위협치의 변화가 표현 가능 한 것을 확인하였다.

5. 결 론

위협평가는 전장상황에서 가장 초기에 이루어지는 작업이다. 이는 전장운용에 효율성을 높일 수 있는 필수적인 요소이며, 정보융합의 한 분야이다. 위협에 대한 대비는 전장의 성패를 좌우하는 영역이기 때문에 전장 상황에서의 위협평가는 그 중요성이 더 크다고 할 수 있다. 특히, 전장상황에서 발생하는 각각의 파편적인 센서 정보들은 정확한 의사결정 및 판단을 혼란하게 할 수 있어 정보의 융합이 필수적이다.

정보융합의 대표적인 모델이며, 정보 융합을 통한 판단 레벨이 계층화되어있는 JDL을 이용하여 전장 위협평가 시스템 설계를 진행하였고 다양한 센서로 부터 얻은 데이터들을 종합적으로 분석 처리하는 위협평가방법을 제안하였다.

특히, 본 논문이 제안한 방법의 특징은 퍼지와 베이지안 네트워크의 장점을 더한 퍼지-베이지안 네트워크 방법을 이용한 것이다. 퍼지-베이지안 네트워크 위협평가 방법을 사용한 결과, 전장상황에서 나오는 센서데이터들의 연관관계를 표현하고 즉시적인 평가가 가능하게 되었다. 또 실험을 통하여 센서데이터의 손실이 많은 전장상황에 대한 세밀한 위협평가가 가능한 것을 확인 하였다.

참 고 문 헌

[1] Stephane Paradise, A.R.Benaskeeur, M.Oxenham, “Threat evaluation and weapons allocation in network centric warfare. In Proceedings of the 8th, pp. 1078-1085, 2005.

[2] Yawei Liang., “A fuzzy knowledge based system in situation and threat assessment”, Journal of Systems Science & Information 4(4), 791–802, 2006.

[3] Fredrik Johansson, “Evaluating the Performance of TEWA Systems”, Doctor Degree Thesis. Orebro University, 2010.

[4] Dean J.Morrissey. “A study on the use of fuzzy logic in situation and threat assessment”, Master Degree Thesis. Royal Military College of Canada, 2005.

[5] Mohamad Khaled Allouche, “A pattern recognition approach to threat stabilization”, DRDC Valcartier, 2006.

[6] 한상훈, 하덕주, 최종후. “데이터 퓨전: 개념, 문제, 대안,” 한국 통계학회, 추계 학술 대회 논문집, 2004.

[7] 박성원, 권지웅, 최진영. “데이터 퓨전을 이용한 얼굴영상 인식 및 인증에 관한 연구” 한국지능시스템학회, pp.302~306, 2001.

[8] T. Neumann, “multisensor Data Fusion in the decision process on the bridge of the vessel,” Gdynia Martime University, Ddynia, Poland. 2007.

[9] An Steinberg, FE White, Cl Bowman, “Revisions to the JDL Data Fusion Model,” Dtic.mil, 1999.

[10] L. A. Zadeh, “Fuzzy sets”, Inform. Contr., vol.8, pp.338-353, 1965.

[11] 조동욱, 김지영. “퍼지이론 핸드북”, 상조사, 1995.

[12] W. Pedrycz, F. Gomide, “An Introduction to Fuzzy Set: Analysis and Design”, MIT Press, 1998.

[13] Judea Pearl. “Fusion, propagation, and structuring in belief networks”, Artificial Intelligence, 29:241-288, 1986.

[14] Judea Pearl, “Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference”, Morgan Kaufmann, 1988.

◐ 저 자 소 개 ◑

윤 종 민

2011년 경원대학교 컴퓨터소프트웨어학과(공학사)
2012년 가천대학교 일반대학원 전자계산학과(석사과정)
관심분야 : 위협평가 알고리즘, 네트워크 보안 etc.
E-mail : chum@daum.net

최 보 민

2012년 경원대학교 컴퓨터미디어학과(공학사)
2012년 가천대학교 일반대학원 전자계산학과(석사과정)
관심분야 : 위협평가 알고리즘, 네트워크 보안 etc.
E-mail : cbm0728@gmail.com

한 명 묵

1980년 연세대학교 공과대학 졸업(공학사)
1987년 뉴욕공과대학교 컴퓨터공학과 석사 졸업(공학석사)
1997년 오사카시립대학교 정보공학부 졸업(공학박사)
1998년~현재 : 가천대학교 IT대학 교수
관심분야 : 정보보호, 데이터마이닝, 위협평가 알고리즘, 네트워크 보안 etc.
E-mail : mmhan@gachon.ac.kr

김 수 현

2003년 계명대학교 컴퓨터공학 졸업(공학사)
2007년 한국과학기술원 컴퓨터공학 석사 졸업(공학석사)
2007년~2009년 국방과학연구소 연구원
2009년~2011년 LIG넥스원 연구원
2011년~현재 국방과학연구소 연구원
관심분야 : 육군 방공지휘통제, 위협평가, 무기할당
E-mail : kims@add.re.kr