한국형 헬기의 다중센서 위협 시뮬레이터 설계 및 구현

박헌우[O1] 정용웅[1] 정성훈[1] 노상욱[1] 고은경[2] 김숙경[2]
[1]가톨릭대학교 컴퓨터정보공학부
cis@catholic.ac.kr
[2]국방과학연구소
ekgo@add.re.kr

Design and Implementation of Multi-sensor Threat Simulator for KHP

Hunwoo Park[O1] Yongwoong Jeong[1] Sunghoon Jeong[1] Sanguk Noh[1]
Eunkyoung Go[2] Sookyung Kim[2]
[1]School of Computer Science and Information Engineering The Catholic University of Korea
[2]Agency for Defense Development

요 약

전장환경에서 헬기는 헬기생존체계의 다양한 센서를 통하여 수집한 데이터를 기반으로 헬기에 대한 위협을 식별한다. 헬기의 성공적인 임무 수행 및 생존을 위하여 헬기에 대한 위협을 반복적으로 확인할 수 있는 시뮬레이터의 구현은 필수적이다. 본 논문에서는 (1) 헬기의 센서가 수신하는 위협요소를 정의하는 온톨로지 생성기, (2) 전장환경과 유사한 위협을 다양한 분포로 생성하는 위협자료 생성기 및 (3) 다양한 전장 시나리오에서 센서들이 수집한 데이터를 통합하여 위협의 방향과 정도를 사용자에게 실시간으로 보여주는 그래픽 화면표시기를 개발한다. 구현한 헬기의 다중센서 위협 시뮬레이터는 다양한 위협을 생성하는 자동 시나리오 생성기를 이용하여 위협 개체의 탐지 및 분류를 반복적으로 수행한다. 위협 시뮬레이터를 활용한 실험에서 동일한 위협에 대한 통합 정확도를 측정하였다.

1. 서 론

전자기술의 발전은 C3(command, control, and communication)와 센서기술의 급격한 발전을 가져왔으며, 지상과 공중을 연결하는 네트워크 솔루션을 가능하게 할 뿐만 아니라 적군의 반응시간 또한 감소시키는 역할을 하였다. 이러한 전자화된 전장에서 아군 헬기의 생존확률을 높이기 위하여 생존체계에 대한 위협데이터를 정의하고 분석하는 연구는 다양한 형태로 진행되어왔다[1]. 한국형 헬기의 두뇌역할을 수행하는 생존체계장비(Aircraft Survivability Equipment: ASE)는[2, 3] 실시간 전장환경에서 여러 개의 센서로부터 수신하는 위협데이터를 분석하고, 위협시스템을 정확하게 분류 및 통합하여야 한다. 아군 헬기의 임무를 성공적으로 수행하고 위협에 능동적으로 대처하기 위하여 위협을 체계적으로 통합하는 생존체계장비를 구축하는 것은 필수적이다. 따라서 본 논문에서는 위협데이터의 수신으로부터 위협 시스템을 확인하는 과정을 자율적으로 수행하는 위협 시뮬레이터를 설계하며, 실질적인 전장환경과 유사한 시뮬레이션 환경에서 반복적으로 생존체계장비의 성능을 검증할 수 있도록 위협 시뮬레이터를 구현한다. 위협 시뮬레이터는 선행연구를 통하여 획득한 자율적인 위협 인식 에이전트를 사용한다[4]. 자율적인 에이전트는 생존체계장비가 수신하는 위협데이터의 특성과 위협간의 상호연관성을 컴파일과정을 통하여 귀납적 모델로 정형화한다[4]. 통합모델은 자율적인 에이전트의 지식베이스로 형성되며, 상황-행동 추론방식에 의하여 특정한 전장상황[1)]에서 위협시스템을 확인할 수 있도록 한다.

구현한 위협 시뮬레이터는 (1) 헬기의 센서가 수신하는 위협요소를 정의하는 온톨로지 생성기, (2) 전장환경과 유사한 위협을 다양한 분포로 생성하는 위협자료 생성기 및 (3) 다양한 전장 시나리오에서 센서들이 수집한 데이터를 통합하여 위협의 방향과 정도를 사용자에게 실시간으로 보여주는 그래픽 화면표시기로 구성된다. 위협 시뮬레이터는 헬기생존체계의 다중센서에서 수신하는 위협 데이터를 통합하며, 위협 시스템을 정확하게 분류하는가에 대한 반복적인 실험 및 평가를 가능하게 한다.

본 논문의 구성은 다음과 같다. 2장에서 위협요소의 분석 및 정의를 위한 온톨로지 생성기를 설계한다. 3장에서 모의 위협 데이터를 생성하는 균일분포, 정규분포 및 지수분포 방식의 위협데이터 생성기를 설명하며, 4장에서는 모의 전장환경에서 위협을 나타내는 그래픽 화면표시기와 자동 시나리오 생성기 및 통합 알고리즘을 구현한다. 5장에서는 구현한 위협 시뮬레이터를 활용하여 동일한 위협에 대한 통합 정확도를 측정하였다. 결론에서 지금까지의 연구결과와 앞으로의 연구방향을 정리한다.

2. 위협요소의 분석 및 정의: 온톨로지 생성기

헬기의 센서가 수신하는 위협요소를 분석하며, 이러한 위협요소를 속성에 대한 계층구조로 정의하는 온톨로지 생성기를 구현한다.

2.1 위협시스템 체계

생존체계 구성 장비의 위협데이터를 분석하고, 각 장비별 위협 데이터의 특성과 위협간의 상호연관성을 분석하고

1) 본 연구는 2006년도 국방과학연구소의 "다중센서 위협데이타 통합기법 연구(UD060072FD)"용역과 2007년도 가톨릭대학교 교비 연구비의 지원으로 이루어졌음.

통합하는 과정에 대한 시스템 체계도는 그림 1과 같다.

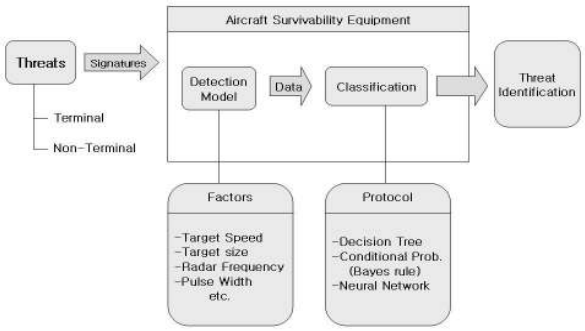

그림 1 - 헬기생존체계장비의 위협데이터 통합과정에 대한 시스템 체계도

위협 시스템에 대한 실시간 데이터가 헬기생존체계장비에 입력되면, 위협을 확인하고 귀납학습 모델에 의하여 생성된 규범의 범주와 비교하여 위협을 분류한다[4]. 이와 같이, 헬기생존체계장비는 현재 상황에 대한 위협을 분류하고 규범에 기반을 두어 결과적인 현재상황을 인식하며, 이에 대한 경고 및 효율적인 대응기법을 추천하게 된다. 이때, 헬기생존체계장비는 (1) 실시간적인 처리가 가능하여야 하며, (2) 잘못된 경고(false alarm)를 최소화하여야 한다. 헬기 승무원은 경고 및 대응기법에 대하여 정확히 이해하고, 빠르게 결정하고, 적절한 행동을 수행하게 된다. 이러한 위협의 분석, 확인, 분류, 경고 및 대응기법 추천과정은 반복되며, 새로운 상황인식으로부터 위의 과정이 반복되게 해야 한다.

2.2 다중센서 수신기 분석

다중센서 수신기는 RWR(Radar Warning Receiver), LWR(Laser Warning Receiver), MWR(Missile Warning Receiver)로 구성되며[5], 표1과 같은 위협 데이터의 속성을 수신한다.

RWR이 수신하는 레이더와 관련된 속성 중 적이 방출한 레이더의 종류를 확인하는데 필요한 속성들로는 주파수(Radio Frequency), 펄스폭(Pulse Width), 펄스반복간격(Pulse Repetition Interval: PRI), 펄스세기(Amplitude)등이 있고 그 위치를 확인하기 위한 속성으로는 신호방향(Angle Of Arrival)이 있다[6, 7, 8, 9].

표1-수신기별 속성

종 류	속 성
RWR	주파수값, 주파수종류, 펄스폭, 펄스반복간격, 펄스크기, 방위각
LWR	방위각, PRF
MWR	방위각

(1) 주파수 값: 각 레이더 유형을 구별하는데 필요한 가장 주요한 요소이다. 레이더 유형별로 특정한 범위의 값을 갖는다.
(2) 주파수 종류: fixed, hopping, agile, bi-channel 등이 있다.
(3) 펄스폭: 펄스의 폭을 나타내는 데이터로써 거리가 멀어지면 펄스폭은 증가한다.
(4) 펄스반복간격: 펄스반복간격이 크면 위협과의 거리가 멀리 떨어져 있으며, 작으면 위협과의 거리가 가까운 경향이 있다. 펄스반복주파수 (PRF)는 PRI의 역수이다.
(5) 펄스 크기(Pulse Amplitude): 펄스 크기는 각 레이더 모델과 운용 모드에 따라 달라진다.
(6) 방위각: 수신된 신호의 방위각이다.

LWR은 레이저 빔 편승 방식의 유도무기(예를 들면, 빔 라이더 방식의 유도탄) 또는 레이저 거리측정기 등에 의하여 아군 헬기가 적 레이저의 표적이 되고 있을 경우에 이를 알려 주는 장비이다. 적기가 사용하는 파장대역을 스펙트럼 분석화하여 탐지한다[10,11].
(1) 방위각: 레이저가 수신되는 각도
(2) PRF: 레이저 펄스 반복 주기. PRF를 통하여 LWR은 레이저 위협을 빔 활강기(Beam rider),거리측정기(Range finder), 표적지시기(Target designator)로 분류한다.

MWR은 기본적으로Pulse Doppler, Infra-Red (IR) 및 Ultra-Violet (UV) 등의 세가지 종류가 있으며, 각각을 조합한 방식도 존재한다. 그 중에서 UV(자외선) 방식의 경우, 미사일의 연료가 연소하면서 발생하는 불꽃의 자외선을 수신한다. 자외선 방식의 MWR은 다른 방식에비하여 선명한 신호를 수신할 수 있기 때문에 신호 처리에 적은비용을 소모하고, 수신기가 신호를 처리하는 부담이 적은 장점을 가진다. 자외선 방식의 MWR의 단점은 적의 미사일 연료의 연소이후의 탐지가 불가능하고, 적군이 쉽게 생성하는 인위적인 기만 신호를 수신할 수 있다는 것이다. 수신속성은 다음과 같다.

(1) 방위각: 수신된 신호의 방위각

2.3 온톨로지 생성기

온톨로지(ontology)[12]는 특정한 개념에 대한 속성들의 계층구조를 형성하여 지식을 구축하는 것으로 정의되며, 온톨로지 생성기(ontology builder)는 다중센서 위협 시뮬레이터에서 헬기의 센서가 수신하는 위협요소들을 사용자가 정의하고, 위협요소들의 구간을 사용자가 지정할 수 있게 한다. 온톨로지 생성기를 통한 위협요소들의 정의는 위협데이터를 소프트웨어적으로 생성할 수 있도록 한다. 그림 2는 수신기 유형별, 즉, RWR, LWR, MWR이 수신하는 위협요소를 속성에 대한 계층구조로 정의하고 유지하는 온톨로지 생성기를 나타낸다.

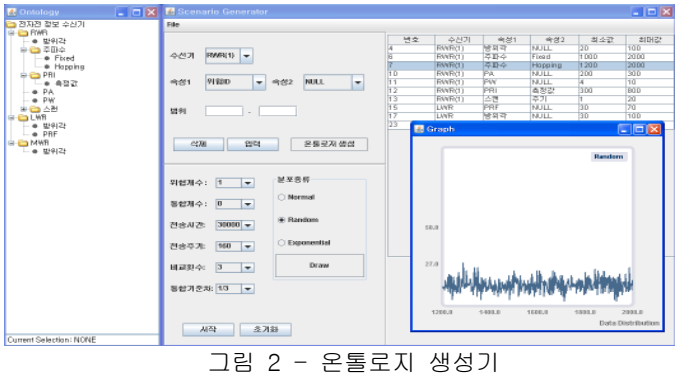

그림 2 - 온톨로지 생성기

3. 모의 위협 데이터의 생성

실질적인 전장환경과 유사한 모의 데이터를 생성하는 위협자료 생성기를 설계 및 구현한다. 모의 위협자료 생성기는 균일분포, 정규분포 및 지수분포 방식을 사용하여 다양한 위협자료를 생성한다.

3.1 위협 시뮬레이터 - 위협데이터 생성기

위협 시뮬레이터는 모의 전장환경에서 헬기의 생존에 필요한 의사결정을 수행하는 시스템으로서, 위협을 조기에 분석하여 위협에 적절한 조치를 취할 수 있도록 해준다. 이러한 위협 시뮬레이터를 통하여 헬기생존체계의 정확성을 반복적으로 시험 및 평가해 보기 위해서는 많은 양의 모의자료를 필요로 하고, 또한 방대한 분량의 모의 데이터를 실질적인 전장환경과 유사하게 생성하는 것이 매우 중요하다.

헬기의 위협분류 시스템이 정상적인 작동을 하고 있는지 판단하기 위해서는 가능한 많은 현실적인 위협 데이터가 필요하게 되는데, 이러한 데이터를 만들어 내기 위해서 위협데이터 생성기를 이용한다. 또한, 최대한 현실적인 데이터 생성을 위하여 수신기별 위협요소에 대한 시나리오를 가상적으로 설정하며, 지능형 위협분류 어플리케이션에 실시간으로 보내게 된다. 소켓 형식으로 전송되는 이러한 데이터들은 서버를 통하여 전달된다. 그림 3은 위협 시뮬레이터의 체계도를 나타내며, 온톨로지 생성기를 통하여 정의한 위협요소를 바탕으로 위협데이터 생성기가 다양한 분포로 모의 위협 자료를 생성한다. 서버에서 생성된 위협 데이터는 클라이언트에 전달되어 진다.

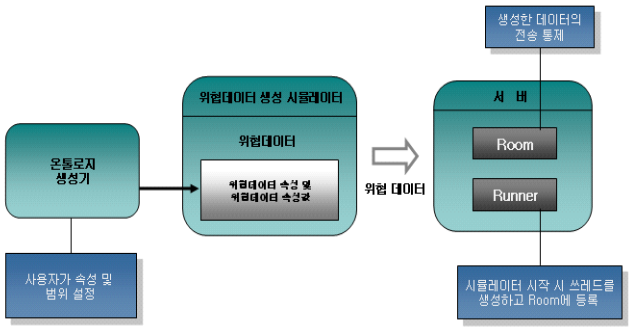

그림 3 - 위협 시뮬레이터의 체계도

(1) 위협데이터 생성기

모의 위협데이터 생성기의 역할은 다음과 같다. (1) 사용자가 온톨로지 생성기를 통하여 수신기별 위협 속성에 대한 속성값을 정의한다. (2) 정의된 속성 값을 바탕으로 균일분포, 정규분포, 지수분포 중 한 가지의 분포로 모의 위협 데이터를 생성한다. (3) 생성한 모의 위협자료의 분포를 그래프로 나타낸다. (4) 생성된 위협 데이터를 지능형 위협 인식 에이전트에 입력자료로 전달한다.

3.2 모의 위협데이터의 분포

다양한 다중센서 위협 데이터 모델에 대한 에이전트의 성능을 확인하기 위하여 정규분포, 균일분포, 지수분포 [13] 의 세 가지 분포를 사용하여 모의실험 데이터를 생성한다. 모의 위협데이터 생성기의 분포방법 선택에 따라 수신기들의 위협 분류 정확도가 각각 다르게 나타난다.

$$n(x;\mu,\sigma) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} \quad (1)$$

for $-\infty < x < \infty$ (where $\sigma > 0$)

수식 (1)과 같이 표현된 정규분포(normal distribution)는 각 속성 값의 범위 내에서 정규 분포를 따르는 데이터를 생성한다. μ는 평균, σ는 표준편차를 의미하며, x는 새로운 모의 데이터를 의미한다.

$$f(x) = \frac{1}{k} \quad \text{for } x = x_1, x_2, \ldots x_k \quad (2)$$

where $x_i \neq x_j$ when $i \neq j$

수식 (2)에 나타난 균일분포(uniform distribution)는 각 속성 값의 범위 내에서 모든 값이 같은 확률로 발생하게 하여 데이터를 생성한다.

$$f(x) = \begin{cases} \frac{1}{\theta} e^{-x/\theta} & x > 0 \\ 0 & x \leq 0 \end{cases} \quad (3)$$

where $\theta > 0$

지수분포(exponential distribution)(수식 (3) 참조)는 각 속성 값의 범위 내에서 지수 분포를 따르는 데이터를 생성한다.

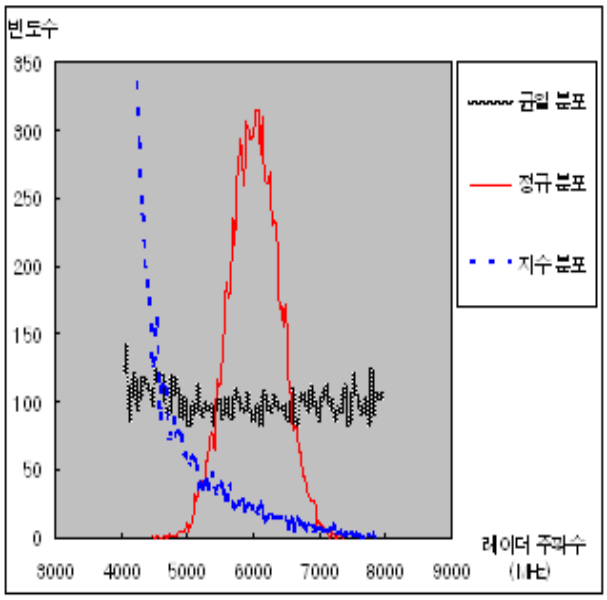

그림 4 - 모의위협데이터의 생성

모의 위협데이터 생성기를 사용하여 세가지 분포를 따르는 모의 데이터를 생성한 결과는 그림 4와 같다.

4. 모의전장상황에 대한 시나리오 생성기 및 그래픽 화면표시기

다양한 전장 시나리오에서 센서들이 수집한 데이터를 통합하여 위협의 방향과 정도를 사용자에게 실시간으로 보여주는 위협 시뮬레이터의 그래픽 화면표시기를 설계 및 구현한다.

4.1 위협 시뮬레이터 - 그래픽 화면표시기

지능형 위협 인식 에이전트는 수신된 모의 위협 데이터를 통합하여 인식된 위협의 종류와 변화과정을 그래픽으로 표현하여 사용자에게 보여주는 기능을 한다. 이 과정에서 모의 위협 데이터간의 통합이 이루어지며, 이러한 통합은 RWR, LWR, MWR로부터 수신된 자료를 통하여 이루어진다. 그림 5는 위협 시뮬레이터의 그래픽 화면표시기 부분에 대한 구조도를 나타낸다. 모의 위협자료에 대한 그래픽 표시를 위하여 위협에 대한 실질적인 분류 및 위협수준에 대한 결정은 자율적인 위협 인식 에이전트에 의하여 수행된다. 자율적으로 상황을 인식하며 이에 대하여 빠르게 반응하는 위협 인식 에이전트에 대한 성능을 평가할 것이다.

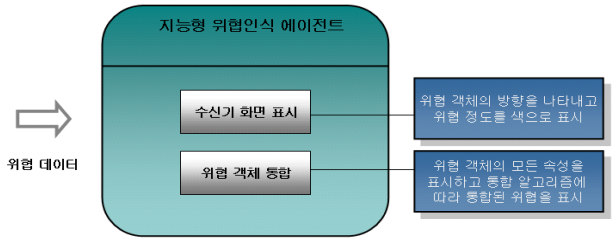

그림 5 - 위협 시뮬레이터의 체계도

(2) 그래픽 화면표시기

4.2 위협에 대한 통합 시나리오

통합 시나리오는 수신기에 수신되는 클래스별의 다양한 위협을 감지하도록 설정되었다. 각 센서에서 수신한 데이터의 방위각이 다르면 서로 독립된 위협으로 탐지한다. 위협의 방위각이 동일하거나 유사하면 동일한 위협일 가능성이 존재한다. 이때, LWR은 미사일의 레이저 유도를 수신한 것이므로 RWR이 수신한 위협이 '미사일유도레이더'라면 같은 위협으로 판단하고 통합할 수 있다. RWR이 수신한 위협이 '탐색레이더'라면 수신된 방위각이 동일할지라도 위협의 객체가 다르므로 이때는 독립된 위협으로 인식해야 한다. MWR은 미사일 위협에 대해서만 수신하는 센서 특성을 갖고 있으므로 다중 센서에서 위협을 탐지했을 경우, 위협을 통합하기 위해서는 각 센서에서 수신된 데이터의 방위각이 동일하고 RWR에서 탐지된 위협이 '탐지레이더'나 '추적 및 전투기레이더' 등이 아닌 '미사일유도레이더'이어야 한다. 헬기와 위협자체가 이동을 하게 되어 시간에 따라 수신된 데이터의 방위각이 계속적으로 변화하게 되는데, 각 센서의 방위각 변화가 동일하면 같은 위협으로 볼 수 있다. 앞에서 방위각이 동일하다고 가정할 때는 이처럼 시간에 따라 변하는 특성을 반영하여도 방위각이 동일한 경우이다. 통합 시나리오 자동생성기의 알고리즘은 그림 6과 같다.

```
function ScenarioGenerate() returns scenario
// 생성될 시나리오를 선택하고, 각 속성을 정한다.//
 local variables:
   scenario: 무작위로 선정된 시나리오의 번호
   Attributes: 시나리오의 속성값(전역변수)
   Seed: 무작위 선정을 위한 Seed값

 random(Seed, scenario)  //시나리오를 무작위로 선택한다.//

//특정한 시나리오의 각 속성을 선택한다.//
 for i = 1 to N
   random(Seed, setScenario[scenario].attribute[i])
 end
 return scenario

end ScenarioGenerate()

 function TestsetGenearte(input scenario) returns null
//선택된 시나리오의 속성을 범위 내에서 임의로 변경한다.//
  local variables:
    a set of ModifyValues : 각 속성의 갱신된 값

// 변화하는 수치를 특정 범위 내에서 임의로 선정한다.//
 for i = 1 to N
   random(seed, ModifyValue[i])
 end

 //시나리오에 입력된 값에 변화값을 넣는다.//
  for i = 1 to N
    setScenario[scenario].attribute[i]
     ← setScenario[scenario].attribute[i] + ModifyValue[i]
  end
  return null
end TestsetGenearte()

main(input testnum) returns Scenarios,
                    a set of Scenarios(scenario), Attribute
//필요한만큼 테스트 데이터를 생성한다.//
 input testnum

 //테스트를 위해 만들어질 실험데이터의 수를 입력받는다.//
  local variables:
    a set of setScenarios(scenario), Attributes
    testnum : 만들어질 테스트 데이터의 수
    count : testnum과 비교하기 위해 사용되는 카운터
ScenarioGenerate(return scenario)
for each count is smaller than testnum then
  TestsetGenearte(input scenario)
 end
return Scenarios
       a set of Scenarios(scenario), Attribute
end main()
```

그림 6 - 시나리오 생성기의 의사코드

위협 시뮬레이터는 이러한 통합 시나리오를 자동으로 생성하여, 여러 다양한 데이터로 사용자가 통합 알고리즘의 정확도를 측정해 볼 수 있게 해준다.

4.3 위협에 대한 통합 알고리즘

통합 알고리즘의 목적은 동일한 위협개체에 대하여 3개 또는 2개의 센서에서 데이터를 수신하였을 때 이를 3개의 위협이 아닌 1개의 위협으로 통합하는 것이다. 위협을 통합할 때 필요한 속성으로는 위협번호, 위협클래스(위협ID), 수신된 위협의 방위각, 수신된 센서정보 등이 있다. 위협번호는 각 수신기에서 위협에 대해 자체적으로 부여한 번호이고, 위협클래스(위협ID)는 수신기에서 확인한 위협의 정체이다. 위협번호와 수신된 센서정보는 위협을 통합할 때 각 센서에 대한 중복을 피하기 위한 자료로써 사용된다. 동일한 위협이라면 각 센서에서 분류한 위협클래스(위협ID)가 같아야 하므로, 위협을 통합하기 위해서는 우선 통합할 위협의 위협클래스(위협ID)가 같아야 한다. 그리고 동일한 위협이라면 발생한 위협의 위치가 같은 방향이므로, 각 수신기에서 수신된 위협의 방위각이 수신기의 수신방위각오차보다 작은 범위에서 일치해야 한다. 이러한 통합근거를 바탕으로 에이전트의 통합 알고리즘을 설계하였다.

위협 통합 에이전트에 탑재된 통합 알고리즘은 다음과 같다. 우선 수신된 두 위협의 위협클래스가 같고, 각 위협의 방위각이 수신기의 수신방위각오차범위 내에서 일치하면 그 이후 두 위협에 대해 α번의 비교를 시행하게 된다. α번의 비교를 수행하였을 때 두 위협에 대해 방위각이 오차범위 내에서 일치한 비율이 β이상이면 두 위협을 통합하게 된다. α가 100이고 β가 90%인 때의 예를 들면 다음과 같다. RWR에서 수신한 위협1과 MWR에서 수신한 위협3의 방위각이 오차범위 내에서 일치하고 위협클래스가 같으면 이후에 100번의 비교를 수행하게 된다. 100번의 비교를 수행한 후 그때까지 방위각이 오차범위 내에서 일치한 비율이 90% 이상이라면 두 위협을 통합하게 된다. 이 통합 알고리즘에서 α와 β가 커질수록 정확한 통합이 가능하나 통합이 되어야 할 위협이 알고리즘의 조건을 충족시키지 못하여 통합되지 않는 경우가 발생할 수 있다. 따라서 환경과 상황에 따른 적절한 α와 β값을 설정하는 것이 중요하다.

개별 센서 간의 위협 데이터를 통합하는 과정은 지능형 위협인식 및 분류 에이전트가 보유한 통합 알고리즘을 통하여 수행되며, 통합된 위협은 그림 7과 같은 그래픽 화면표시기의 가상 레이더에 그 결과를 보여준다.

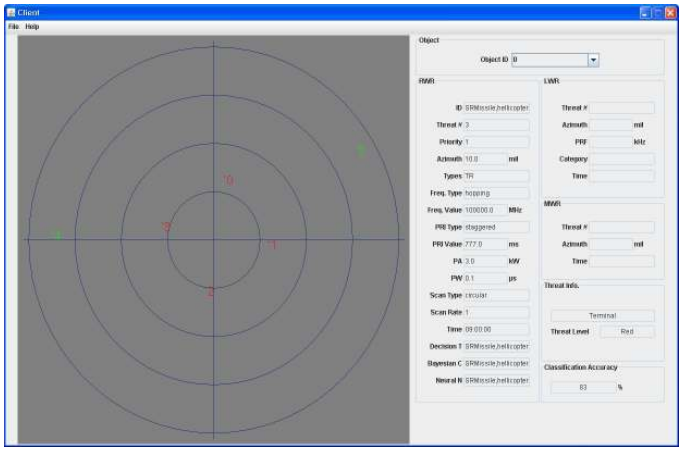

그림 7 - 그래픽 화면표시기의 화면

그래픽 화면표시기는 각 수신기가 수신한 위협의 속성값과, 분류 기법에 따른 알고리즘별 위협분류결과, 통합된 위협개체의 현황을 표시하고 있다.

5. 통합실험 및 결과

시나리오 생성기를 통하여 얻어낸 시나리오를 통해 α(비교횟수)와 β(통합기준치)값에 대한 통합 알고리즘의 정확도를 알아보았다. 이때 시나리오 생성기에서는 실제 헬기 생존 장비의 EWC가 데이터를 수신하는 주기인 320ms와 이의 절반인 160ms로 데이터를 보내도록 하였다. 그리고 실험에서 320ms주기로 데이터를 수신했을 때와 160ms로 데이터를 수신했을 때의 α(비교횟수)값을 다르게 설정하였다. 이에 따라 데이터 수신주기가 320ms일 때는 α(비교횟수)값을 3과 6으로, 160ms일 때는 α(비교횟수)값을 6과 12로 설정하였다. 각 경우는 데이터 수신주기에 따라 1초와 2초를 비교할 때 필요한 비교횟수가 된다. 만약 320ms로 3회를 비교하면 약 1초의 시간, 6회를 비교한다면 약2초의 시간이 걸릴 것이다. 실험 시 동일한 시나리오에 대해 데이터 수신주기만 바꾸어서 실험을 수행하였다. 그리고 통합 알고리즘의 정확도는 전체 위협개수에 대하여 올바르게 통합된 위협개수의 비율로써 측정하였다. 만약 통합이 고려된 전체 위협이 10개인데 에이전트가 올바르게 통합, 인식한 위협이 8개라면 80%의 통합정확도를 가지게 된다. 100개의 시나리오에 대해 α(비교횟수)와 β(통합기준치)값에 대한 평균 통합 정확도를 측정한 결과를 수신주기에 따라 그림 8과 그림 9에 나타내었다.

실험결과 수신주기가 320ms와 160ms인 경우 모두 α(비교횟수)값과 β(통합기준치)값이 커질수록 통합정확도가 높게 나타났다. 그리고 가장 적절한 α(비교횟수)값과 β(통합기준치)값은 320ms에서 6과 66.6%(4번 일치), 160ms에서는 12와 66.6%(8번 일치)로 볼 수 있었다.

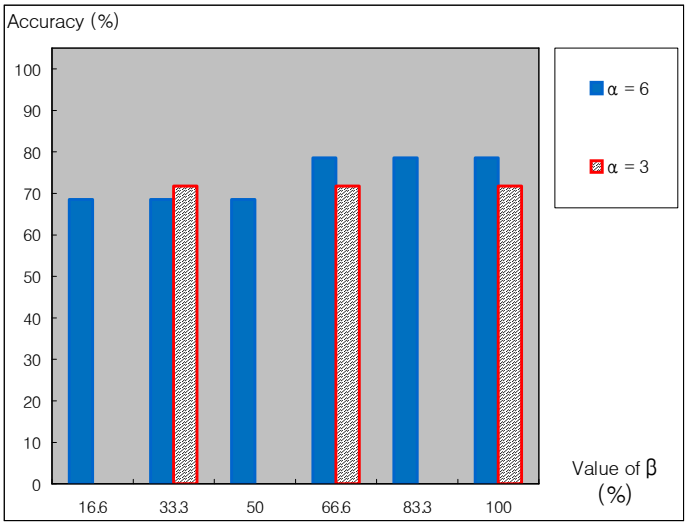

그림 8 - 320ms로 데이터를 수신했을 때의 실험결과

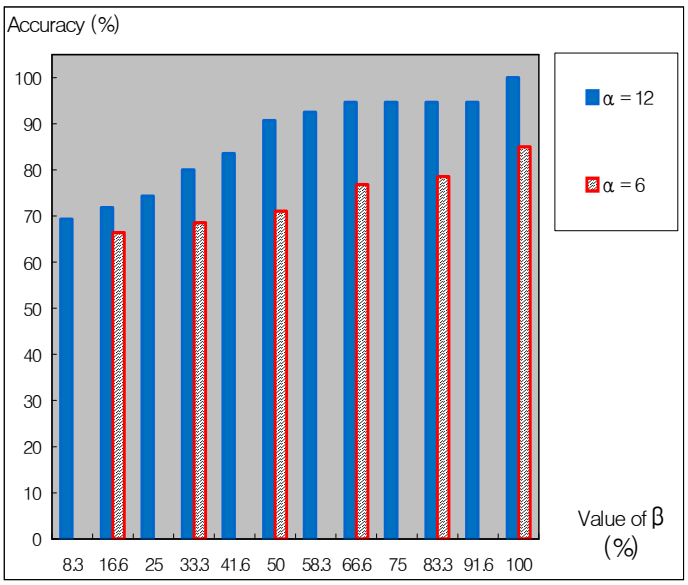

그림 9 - 160ms로 데이터를 수신했을 때의 실험결과

6. 결론

본 논문에서는 실시간 다중 에이전트 환경에서의 자율적인 상황인식 기법을 이용하는 다중센서 위협 시뮬레이터를 구현하였다. 위협데이터를 수신하는 수신기의 분석을 통하여 수신된 위협 데이터의 특성을 파악하였으며, 이를 바탕으로 위협 데이터 수신 시나리오를 통합하였다. 또한, 상황-행동 규칙을 보유한 위협인식 에이전트를 개발하였다. 헬기생존체계의 실질적인 개발 및 평가를 위하여 다양한 분포로 생성한 모의 위협 자료를 이용하여 위협데이터 통합 시스템을 반복적으로 실험하였다.

앞으로의 연구방향은 (1) 적의 탐색레이더가 아군을 탐지한 후 (2) 추적레이더로 추적하여 (3) 격추 위협을 발사한 경우, 연관된 위협을 통합하는 기법을 연구할 것이다. 위협 통합시스템은 개선된 실험결과를 통하여 헬기생존체계가 실시간 전장환경에서 실질적이고 유연한 의사결정을 수행할 것이다.

참고문헌

[1] J. Heikell, "eletronicwarfareself-protetion of battlefield helicopters: A holistic view.", Helsinki University of Technology, doctoral dissertation, 2005.

[2] J. Patrick and N. James, "A Task-Oriented Perspective of Siutation Awareness." In S. Banbury and S. Tremblay (Eds), A cognitive approach to situation awareness: theory and application. Chapter 4, Burlington, VT: Ashgate Publishing Company, 2004.

[3] Aircraft survivability equipment (ASE): Ensuring lethality and dominance of Army aviation over tomorrow's battlefield, Association of the United States Army.

[4] 정용웅, 노상욱, **고은경**, **정운섭** "다중센서 위협 데이터의 귀납적분류.". **정보과학회논문지 : 소프트웨어 및 응용**, **제35권**, **제3호**, pp189~196. 2008.

[5] Integrated Defense Systems, http://www.boeing.com

[6] Koxinga, A Brief History of Chinese Naval Radar and EW developments, http://China-Defense.com.

[7] EW Tutorial, http://ourworld.compuserve.com.

[8] Lee D. Kennedy, F/A-18 electronic warfare suite cost and operational effectiveness analysis methodology: Phase 1 - radio-frequency countermeasures, Johns Hopkins APL Technical Digest.

[9] SIGNAL SORTING METHODS and DIRECTION FINDING, University of Hawaii' at Manoa.

[10] 홍경희, 조길호, 박명진, 신내호, 정관, 레이저의 군사적이용, 육군사관학교 화랑대연구소, pp202~207, 2001.

[11] Laser Beamrider Missile Countermeasures, http://www.multidimensionalimaging.com/.

[12] 노상규, 박진수, 온톨로지 웹2.0에서 3.0으로, 가즈토이, 2007.

[13] John E. Freund, "Mathematical Statistics," Prentice Hall, 1992.