Journal of Korean Institute of Intelligent Systems
Vol. 26, No. 3, June 2016, pp. 233-238
http://dx.doi.org/10.5391/JKIIS.2016.26.3.233

ISSN(Print) 1976-9172
ISSN(Online) 2288-2324

JKIIS

차세대 침입탐지에서 이상탐지를 위한 추론 기반 데이터 융합 알고리즘

Data Fusion Algorithm based on Inference for Anomaly Detection in the Next-Generation Intrusion Detection

김동욱* · 한명묵*
Dong-Wook Kim and Myung-Mook Han

***가천대학교 컴퓨터공학과,**
*School of Computer Engineering, Gachon University

요 약

본 논문은 차세대 침입탐지 시스템을 위해서 데이터 융합에서의 불확실한 데이터 처리의 알고리즘을 제안한다. 차세대 침입탐지는 사이버 공간에서 생성되어지는 정보를 지식으로 만들어내기 위해 수많은 네트워크 센서로부터의 데이터가 수집되어진다. 수집된 센서 정보를 지식의 수준으로 이끌어내기 위해서 데이터 융합의 과정이 필요하다. 이를 위해 본 논문에서는 Demster-Shafer 증거이론 추론적 기법을 통하여 서로 다른 데이터들의 특징을 분석하여 불확실한 데이터가 어느 구간에서 신뢰구간을 갖는지를 분류하여, 불확실한 데이터에 대한 표현을 이루어낸다. 본 실험내용에서는 이러한 불확실성 데이터에 대한 이상탐지를 위해 iris plant 데이터세트를 이용한 신뢰구간에 따른 분류를 실행하였다. 이에 대해 각 신뢰구간을 통해서 데이터 분류가 가능하다는 것을 검증하였다.

키워드 : 데이터 융합, 뎀스터-쉐이퍼, 추론방법, 이상탐지

Abstract

In this paper, we propose the algorithms of processing the uncertainty data using data fusion for the next generation intrusion detection. In the next generation intrusion detection, a lot of data are collected by many of network sensors to discover knowledge from generating information in cyber space. It is necessary the data fusion process to extract knowledge from collected sensors data. In this paper, we have proposed method to represent the uncertainty data, by classifying where is a confidence interval in interval of uncertainty data through feature analysis of different data using inference method with Dempster-Shafer Evidence Theory. In this paper, we have implemented a detection experiment that is classified by the confidence interval using IRIS plant Data Set for anomaly detection of uncertainty data. As a result, we found that it is possible to classify data by confidence interval.

Key Words : Data fusion, Dempster-Shafer, Inferential Method, Anomaly Detection

Received: May. 10, 2016
Revised : Jun. 17, 2016
Accepted: Jun. 20, 2016
†Corresponding authors
mmhan@gachon.ac.kr

1. 서 론

침입탐지 시스템(IDS, Intrusion Detection System)은 각종 침입 행위들을 자동으로 탐지하거나, 대응 및 보고하는 보안 시스템으로의 기능을 수행한다. IDS 시스템은 IT기술과 네트워크의 환경의 발달과 함께 지속적인 발전이 필요하다. 그 이유로는 기술의 발달은 새로운 공격의 기술과 침입 수법들이 다양하게 발전하고 있기 때문이다. IDS는 시스템과 네트워크 자원으로부터의 비정상적인 사용과 오용 및 남용 등에 대한 정보를 실시간으로 수집과 분석을 수행한다[1]. 현재 내부와 외부 공격의 고도화함에 따라 탐지를 위한 센서들도 증가하고 패턴이나 분석되어지는 데이터도 방대해짐에 따라 불확실성을 가지는 경우가 많아지고 있다. 이는 탐지율이 낮아지거나, 오탐율이 높아지게 되게 만드는 이유가 된다. 이렇듯 기존의 단순한 Rule set과 Signature 분석으로는 지속적으로 발전되는 다양한 공격 유형과 알려지지 않는 공격에 대해서 대응은 쉽지 않을 것이다[2]. 본 연구에서는 데이터 융합과정에서 이루어지는 불확실성 데이터를 처리하기 위해 추론 기법으로 접근하여 데이터의 불확실성 데이터의 확률적 기반 하에 처리할 수 있는 데이터 융합 기술을 소개한다. 이는 Dempster-Shafer이론으로써 1967년 Arthur Dempster가 제안하고 1976년 Glenn Shafer이 발전시킨 것으로,

본 연구는 2015년 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (한국연구재단-NRF-2015R1D1A1A01060874)

지식베이스내에 정확한 신뢰값을 부여하는 것이 아닌 신뢰 값의 범위를 통하여 신뢰도를 표현하는 방식이다. 확신의 정도와 불확실 구간을 구함으로써, 신뢰 구간으로 얻는다. 이것을 이용한 방법으로 확률적 구간을 통해 데이터가 어느 정도에 신뢰구간의 속하는지를 확인한다. 이와 같은 방법을 통해 침입탐지 데이터 내에서 정상과 이상탐지의 분류 하는 기술에 있어 필요한 분류 검증의 향상을 목표로 진행한다. 본 연구는 데이터 융합을 위한 과정으로써, 불확실정보에 대한 검증을 소개하며, 2장에서는 관련연구를 소개하는데 데이터 융합에 관한 정의와 이와 관련된 불확실성 데이터 처리를 위한 데이터 융합 알고리즘 소개 그리고 본 연구에서 사용되는 Dempster-Shafer이론의 관련 연구내용을 소개한다. 이후 3장에서는 Dempster-Shafer 알고리즘에 대한 기본 소개를 통해 본 연구에서의 제안하는 방법을 나타내며, 5장에서는 실험 결과를 통해 진행한다.

2. 관련 연구

2.1 데이터 융합

데이터 융합의 목표로는 다양한 소스로부터 수집된 데이터에서 특징을 추출하기 위해 새로운 데이터의 생성을 의미한다. 이런 데이터를 생성하기 위해서는 자료들의 특징들을 분류하고 식별해야한다[3]. 수집되어지는 다양한 소스로부터의 데이터들은 시스템 기능에 따라 유형와 표현 수준들이 다르고, 데이터의 타입도 다를 수 있기 때문이다. 이러한 데이터 융합 과정은 임의의 타입들을 정보 융합하는 과정으로써, 하나의 데이터와 다른 여러가지 데이터와의 상관 관계 및 조합방식을 다루는 것으로 정의한다[4][5]. 앞서 말한 데이터 융합문제에는 다양한 문제들이 존재하는데, 이러한 데이터 융합 분류를 그림 1에서와 같이 표현하였다. 데이터 융합 방법의 분류에서의 불확실한 데이터에 대한 처리와 상관관계, 또한 데이터 간의 일치하지 않는 문제, 서로 다른 형식의 데이터 등에 관한 문제가 있다[8]. 이러한 데이터 융합에 있어 각각의 문제에 대해서는 다양한 알고리즘과 개선된 알고리즘을 통하여 해결하는 연구가 활발히 진행되고 있다.

본 연구에서는 데이터 융합과정 문제 중에 불확실한 데이터에 대한 처리를 연구를 진행하였다. 불확실한 데이터에 대한 처리는 다양한 센서로부터 수집될 수 있는 환경 중에서 이미지 프로세싱 분야에서 많이 사용되고 있으며, 인공지능 분야에서도 주어진 데이터의 불확실성을 내포한 영역에서 의사결정을위해 사용되고 있다. 데이터를 처리하기 위한 공학 내에서는 매우 중요한 내용으로 보고 있다.

2.2 데이터 융합 알고리즘

불확실성 데이터를 처리하기 위해 크게 Bayesian 방법과 Dempster-Shafer 방법, Abductive Reasoning, Semantic Method 등으로 크게 연구가 이루어지고 있다.

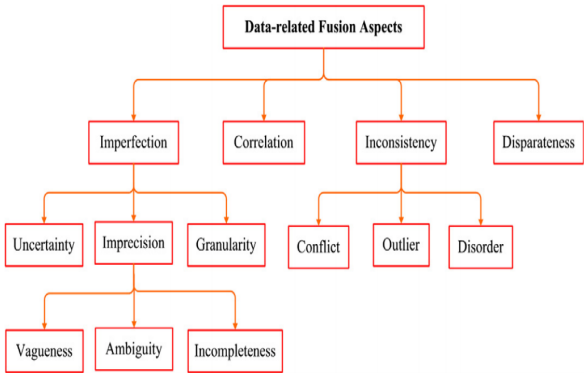

그림 1. 데이터 융합 방법의 분류
Fig. 1. Taxonomy of data fusion methodologies

베이지안 추정에 기초한 정보 융합은 확률론 규칙에 따라 증거를 결합하는 방식을 제공한다[8]. 불확실성은 간격에 따른 값에 따라 Belief 를 나타내고 취하는 조건부 확률을 사용하여 표현 한다. [0, 1]과 같이 0은 부족한 Belief를 표현하며 이와 반대인 전체 구간의 1은 0과 반대인 믿음을 나타낸다[6][7].

뎀스터-쉐이퍼 추론 방법은 베이지안 이론의 일반화한 뎀스터와 쉐이퍼에 의해 도입된 수학 이론을 기반으로 한다. 뎀스터-쉐이퍼 이론은 믿음 구간을 통한 불완전한 지식을 나타내는 데 사용될 수 있는 불확실성을 나타내는 수만큼의 증거의 조합을 제공한다.

Abductive Reasoning은 가장 좋은 설명을 가질 수 있는 추론 가설이 경우에 해당한다는 가정 하에서 선택하는 추론 방식이다. 이는 가장 정확하게 관측 된 이벤트를 설명하는데, 이벤트가 발견되면, 이 발견된 사실을 설명하기 위하여 최선의 설명을 찾기 위해 시도한다. 이 방법은 융합 기법보다는 추론 패턴으로도 나뉠 수 있다.

Semantic 방법으로는 입력정보의 소스 정보를 하나의 소스에서 의존하는 것이 아닌 서로 다른 소스에서도 의미적인 데이터를 결정하는 방법이다. 이는 하나의 소스에 의존하는 것보다 더 정확한 결과를 제공할 수 있다. 이 의미 정보 융합은 기본적으로 원시 센서 데이터의 노드가 생성된 의미 정보를 교환하도록 처리하는 방식이다. 지식과 패턴 매칭을 구축하여 관련 속성에 대한 의미론적 해석을 제공한다[8].

2.3 Dempster-Shafer 침입탐지

불확실한 데이터에 대한 처리 방법은 이외에 여러 복합적인

방법을 통하여 해결되는 연구가 있으나 대표적인 4가지 방법을 소개하였다. 본 관련논문에서는 4가지 기법 중에서 Dempster-Shafer이론을 통한 침입탐지 논문을 소개한다. 네트워크 침입 탐지 방법에서의 높은 오경보율을 줄이기 위하여 Dempster-Shafer 증거 할당과 다중 회귀 신경망(multi-generalized regression neural network) 분류기를 통해 공격 데이터를 식별한다[9].

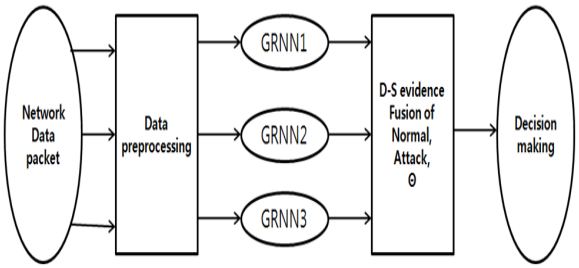

그림 2. 침입탐지 Framework
Fig. 2. Intrusion Detection Framework

이는 추출되어진 특징들은 각각의 기본적인 확률 할당을 결정하는 일반화 된 다중 회귀 신경망 분류기에 의해 식별된다. 그림 2의 침입탐지 Framework에 따라, 네트워크 데이터 패킷을 전처리 과정을 통해 다중 분류기의 출력 결과에 특정 조합으로의 규칙을 이용하여 의사 결정의 최종 질량 함수를 형성하는 증거로서 간주된다. 이로 인해 자기 학습 능력과 일반화된 회귀 신경망에서 일반화 기능의 불확실한 정보를 Dempster-Shafer 이론 기능을 통하여 효과적으로 처리한다. 이로써 불확실한 네트워크 데이터를 인식 할 수 있으며, 크게 오경보 율을 줄이기가 가능하다. 이 방법에서는 KDDCUP99 평가 데이터 세트를 사용한 시뮬레이션에 의해 확인되었으며, 시뮬레이션 결과는 Dempster-Shafer 이론과 다중 회귀 신경망 네트워크와의 네트워크 침입 탐지에 효과적인

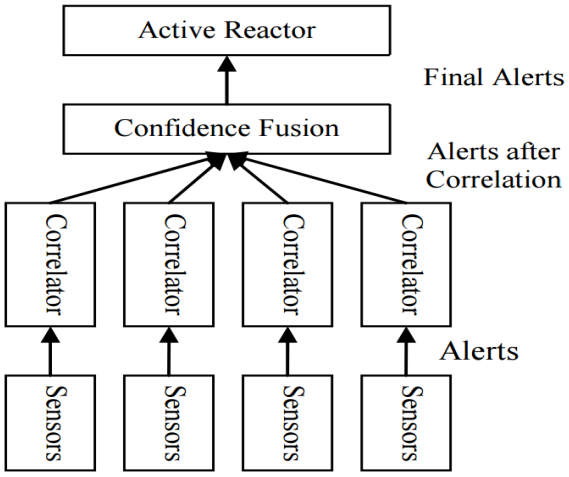

그림 3. 경고 신뢰 융합 시스템 아키텍쳐
Fig. 3. Architecture used in alert fusion system.

방법임을 확인하였다. 이는 단순히 정확한 검출 율을 향상 시킬 뿐이 아닌, 불확실한 네트워크 정보에 의해 발생하는 잘못된 인식 결과에 잘못된 경고 비율을 감소 시킬 수 없었다.

이와 관련하여 Dempster-Shafer 이론을 통한 네트워크 침입탐지의 공격 신호에 대한 응답에 관한 연구 논문이 있다[7]. 이 또한 경고에 대한 신호 정확성을 평가하는 내용으로써, 접근 방식이 불확실성과 알 수 없는 상태에 대한 특정 가설에서의 믿음을 결합하는 Dempster-Shafer 이론을 사용한다. 이를 통해서 검출 결과에 대한 믿음과 타당성의 정량적 측정이 가능하다 말하고 있다. 그림 3에서와 같은 시스템 아키텍쳐에 이러한 경고 융합 알고리즘에서 내부에 설치된 센서 경보들 간의 상관관계 구성요소를 통하여 경보의 품질을 향상 시킬 수 있다 한다. 본 연구 과정에서는 DARPA IDS 평가 데이터 세트를 이용하여, 검출율을 개선하고, 거짓 경보에 대한 비율을 감소시킬 수 있다 하였다.

3. 제안 방법

3.1 Dempster-Shafer 알고리즘

데이터 융합 문제의 Dempster-Shafer 이론은 1981년에 소개된 것으로, 불확실성 처리에 관한 연구로 많이 진행되어 왔다. 뎀스터 쉐이퍼 기법은 많은 응용 분야에 있어서 유효성이 입증된 효과적인 방법으로 사용되고는 했다. 그러나 계산적인 비효율적 단점을 가지고 있고, 속성에 대한 여러 hypothesis가 주어질 때마다, 여러 개의 가설들이 모여 하나의 가설을 이루는 multiple hypothesis 이 허용되어 가능한 가설의 개수는 지수적으로 증가하게 된다. 이러한 문제는 지수적으로 불어나는 가설의 개수를 처리해야하는 복잡도가 늘어나 전체적인 시스템의 효율성에 영향을 주어 성능 저하를 나타내는 단점을 가지고 있다. 그러나 뎀스터 쉐이퍼 이론은 베이지안과 달리 하나의 수치로 표현하기 보다는 신뢰구간을 지정하여 유효한 표현이 가능하며, 정보의 부족에서 오는 불확실성에 대한 차이를 말할 수 있다[1].

불확실성과 부정확성을 처리하기 위해 본 연구에서는 데이터를 융합하는데 있어 필요한 조합 규칙과 측정된 데이터의 사용 가능한 불확실성 데이터에 신뢰 할당 가능성을 추론적 기법으로 적용한다. 이 방법은 Demster-Shafer 증거이론(Theory of Evidence)의 기반한다.

이 이론은 θ의 참값이 알려지지 않는 확률변수의 분별 프레임이라는 가설의 집합을 정의한다. D-S프레임에 대한 완전한 확률할당은 기본확률할당(basic probability assignment, BPA)으로서 정의되며 이산 BPA 함수(discrete BPA function) m(A)는 다음의 식(1)을 만족하여야 한다.

$$0 \le m(A) \le 1 \quad \text{for all } A \subset \theta \qquad (1)$$
$$\sum_{A \subset \theta} m(A) = 1.0, \quad m(\varnothing) = 0$$

어떤 부분집합의 $A \subset \theta$에 대한 믿음함수(belief function) Bel(A) 및 가능성 함수(plausibility function) Pl(A)가 θ에 대한 BPA로부터 식 (2)와 정의될 수 있다.

$$Bel(A) = \sum_{B \cap A} m(B) \quad Pl(A) = \sum_{B \cap A \neq \varnothing} m(B) \qquad (2)$$

bel(A)와 Pl(A)는 수식(3)처럼 각각 A에 대한 확률의 하한 및 상한으로서 고려될 수 있다.

$$Bel(A) \le P(A) \le Pl(A) \quad A \subset \theta \qquad (3)$$

이러한 이론을 통해 센서의 증거는 일반적으로 조합의 Demster의 규칙을 사용하여 융합된다. 믿음의 E는 bel(E)=$\sum_{B \subseteq E} m(B)$로 정의되며 타당성의 pl(E)=$\sum_{B \cap C = E \neq \varnothing}$으로 정의된다. $m_{1,2}(E) = (m_1 \oplus m_2)(E)$ 정보의 두 가지 소스를 고려하여 다음과 같은 수식(4)로 나타내며, (5)에서의 포함되지 않을 경우 0으로 할당하며, 질량함수 m1, m2가 계산된다[7].

$$m_{1,2}(E) = (m_1 \oplus m_2)(E) = \frac{1}{1-K} \sum_{B \cap C = E \neq \varnothing} m_1(B) M_2(C) \qquad (4)$$
$$m_{1,2}(\varnothing) = 0 \qquad (5)$$

이러한 소스간의 충돌의 양을 수식(6)으로 나타낼 수 있다.

$$K = \sum_{B \cap C = \varnothing} m_1(B) m_2(C) \qquad (6)$$

데이터 융합 문제에서의 불확실성 데이터의 처리는 아주 중요한 문제이다. 이 불확실성에 대한 처리요구는 Demster-Shafer이론과 Bayesian 방법이 많이 비교가 이루어지는데, Demster-Shafer의 이론은 베이지안 추론과 달리 각 소스는 다른 수준의 정보를 기여할 수 있다. 또한 데이터 융합에 있어서 인기 있는 접근 방식 자체를 설립하였으며, 베이지안 방법과 달리 가설 집단의 모든 부분집합에 대해 신뢰도를 배정할 수 있도록 할 수 있어, 모든 부분집합에 대한 분포를 형성할 수 있게 된다[6][11].

3.2 Dempster-Shafer 알고리즘 적용 실험

실험 방법으로 본 연구에서 말하고 있는 DS이론을 통하여 데이터 세트에 대한 신뢰구간을 통해 불확실성 구간을 표현하고, 이에 대한 분류과정을 진행한다. 이를 통하여 데이터 세트에 대한 신뢰 구간이 이에 속하는지를 평가하여, 앞으로의 침입탐지 시스템내에서 데이터 융합에 있어 지식을 추론하는 향후 연구계획을 설명한다.

먼저 데이터 세트는 iris plant 데이터 세트를 이용한 신뢰구간 표현을 진행한다. iris 데이터 세트는 총 3개의 클래스 Iris-setosa, Iris-versicolor, Iris-virginica로 나뉘어 있으며, 이는 각각의 4개의 속성으로 분류된다. 속성 Sepal Length, Sepal Width, Petal Length, Petal Width로 나뉘어져 있다.

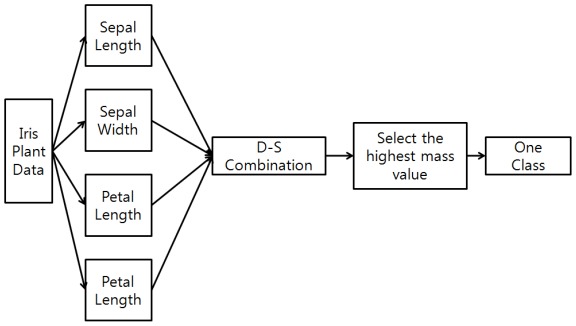

그림 4. Iris data의 신뢰구간 분류 flowchart
Fig. 4. System flow chart for the classification Iris data

표 1. 은 iris plant data가 각 클래스에 대한 각각의 속성의 대한 최대 값과 최소값을 기준으로 데이터가 속해 있는지를 분류하기 위하여 나타낸 값이다. 각각의 클래스에는 속성이 나타나 있는 값들을 DS 조합규칙으로 결합하고, 이에 대한 높은 질량 값을 갖고 있는 값에 대한 클래스를 분류한다. DS이론에 따른 클래스의 각각의 속성에 대한 신뢰 구간을 아래와 같이 나타내어, 각 속성에 대한 값을 Dempster'rule을 통하여 결합시킨다.

표 1. iris data의 경계 값
Table 1. iris data of boundary value

Attribute		Class 1	Class 2	Class 3
1	max	5.8	7	7.9
	min	4.3	4.9	4.9
2	max	4.4	3.4	3.8
	min	2.3	2	2.2
3	max	1.9	5.1	6.9
	min	1.0	3.0	4.5
4	max	0.6	1.8	2.5
	min	0.1	1.0	1.4

4. 실험 결과

제안된 방법을 이용하여 실험결과에 대한 내용은 아래와 같다. 본 실험을 위하여 본 연구에서는 Matlab R2016a를 이용하였으며, 이를 지원하는 IPP Toolbox를 통하여 실험을 진행하였다. 또한 불확실성 데이터는 iris Plant Dataset의 경계값에 대한 기준으로 Matlab

에서 지원하는 구간에 따른 샘플데이터 생성을 이용하여 하나의 클래스에 따른 200의 데이터의 샘플을 생성한 지수적 확률분포를 통해 나타내었다.

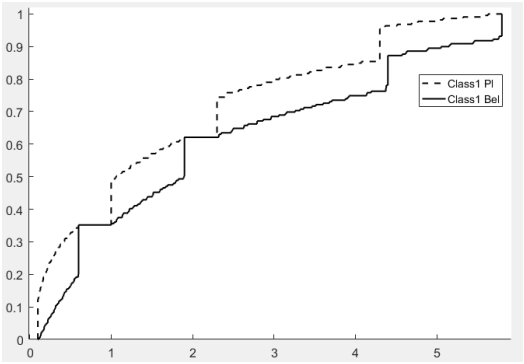

그림 5. Iris-setosa 누적확률 분포
Fig. 5. Iris-setosa cumulative probability distribution

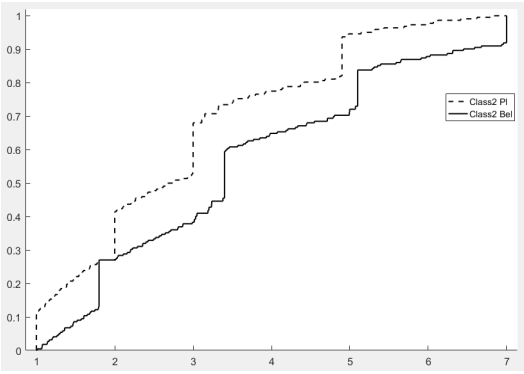

그림 6. Iris-versicolor 누적확률 분포
Fig. 6. Iris-versicolor cumulative probability distribution

다음 그림 5는 Iris-setosa의 Class1에 대한 표1의 경계선을 기반의 기본확률할당을 생성하여 이산 확률 샘플을 Dempster'rule을 적용하여 나타낸 누적확률 분포 그래프이다. 이는 입력데이터가 주어졌을 경우 각 속성에 해당하는 경계값을 통해 그 값이 포함되는 영역인지를 누적 확률 구간을 통하여 신뢰도를 나타낼 수 있다. 이는 클래스에 대한 신뢰확률을 결정하여, 각 클래스에 속성 경계 구간에 포함하는지와 그 경계 값에 포함하지는 않는지를 확인하여 불확실성을 인지할 수 있다. X축에서는 데이터 누적확률구간이며, 기울기는 시뮬레이션 결과의 무작위 데이터의 불확실성을 표현하며, Pl은 데이터의 확률구간의 가능성을 가진 누적분포 구간을 나타내며, Bel 그래프는 불확실성 데이터에 대한 신뢰구간을 표현한다. 입력데이터가 Class1에서 각 속성의 경계에 대한 데이터가 속할 수 있는지를 확인할 수 있는데, 만일 입력데이터가 5로 나타내었을 시 Class1의 속성 1 경계값에 속하는 값으로, 속성1을 확인해보면 확률분포구간은 90%~98%로 볼 수 있다.

그러나 Class1에 대한 경계 값을 벗어난 그 이상의 값을 입력 받을 경우에는 다른 Class2에 나타난 속성을 참조해야 한다. 그림 6에서 5 이상의 값인 6이상 값을 포함한 속성1에 대한 구간을 확인해본 바, 4.9~7의 입력데이터가 속할 수 있는 구간은 69%~100%으로 확인되며, 그 이상의 값은 Class3에 대한 속성으로 참조가 가능하다. 이러한 방법을 통하여 적절한 구간 내 경계 값을 기반으로 최소 신뢰도와 최대 가능성을 표현을 통해 표2에 나타난 속성 값의 신뢰구간을 통하여 입력 값에 대한 신뢰구간을 통해 확실성을 얻을 수 있다.

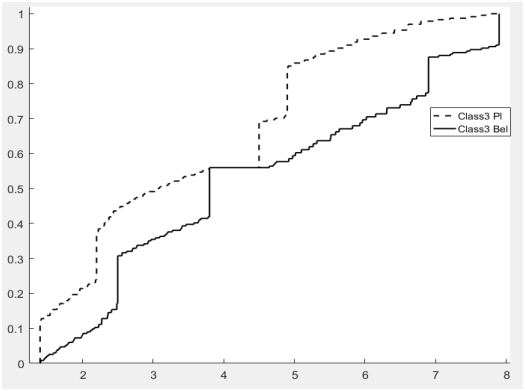

그림 7. Iris-virginica 누적확률 분포
Fig. 7. Iris-virginica cumulative probability distribution

표 2. 샘플 데이터의 대한 확률분포구간
Table 2. cumulative probability distribution of the Sample data for interval

Attribute	Class 1		Class 2		Class 3	
1	5.8	78~100	7	71~100	7.9	59~100
	4.3		4.9		4.9	
2	4.4	62~88	3.4	28~72	3.8	10~57
	2.3		2		2.2	
3	1.9	31~61	5.1	39~95	6.9	56~99
	1.0		3.0		4.5	
4	0.6	0~35	1.8	0~41	2.5	0~31
	0.1		1.0		1.4	

5. 결론 및 향후 연구

본 논문에서는 불확실성 데이터 처리를 위해 데이터 세트에 대한 경계 값을 구분해 신뢰구간을 계산하여 표현한다. 이후 입력 값이 각 클래스에 대한 속성 경계 값에 포함하는지를 확인하여 불확실 데이터에 대한 처리와 적절한 클래스 속성에 배치할 수 있는 지를 확인할 수 있었다. 입력된 데이터에 따라 어느 경계선에 속하고 이에 대한 가능성과 신뢰도 통해 불확실 정보를 포착할 수 있는 방안이 제시되는 방안은 침입탐지 시스템에서의 이상탐지 요구사항과 비슷하나, 본 연구 내용처럼 단순한 다른 클래스에서의 참조되는 것이 아닌 새로운 가공법을 요구 할 수 도 있을 수 있다. 또한 경계 값에 관한 기준 사항은 데이터 융합과정에서의 부정확한 데이터 처리에 큰 영향을 미칠 수 있기 때문에 이에 대한 방안 연구도 필요할 것이다. 본 실험을 통해서 Dempster-Shafer 이론을 통한 신뢰구간의

포함하는지를 평가하여, 이를 이용한 불확실 데이터의 신뢰도가 어느 정도를 포함하는지를 알 수 있었다. 앞으로, 정확한 경계값에 대한 신뢰구간을 정하는지는 사용자에 따른 분석이 필요한 부분이 있어 이를 밑받침 해줄 수 있는 과정에 대한 연구가 더 필요한 부분이 있으며, 실험에서 또한 불확실성 데이터를 생성하는 샘플 조건을 만드는 부분에서도 차후에는 직접적인 침입탐지의 데이터를 활용하여 결과를 보아야 한다. 이는 차후에 신뢰구간을 정할 수 있는 부분이 보완이 되어 진다면 진행할 사항이며, 사용자에 따른 신뢰구간을 데이터세트에 따른 전처리 과정을 포함하여 더욱 깊이 있는 실험을 할 예정에 있다.

References

[1] Bass, Tim. *Intrusion detection systems and multisensor data fusion*. Communications of the ACM 43.4 99-105 :(2000).

[2] Barford, Paul, Somesh Jha, and Vinod Yegneswaran. *Fusion and filtering in distributed intrusion detection systems*. Proc. Allerton Conference on Communication, Control and Computing. 2004.

[3] Klein, Lawrence A. *Sensor and data fusion: a tool for information assessment and decision making*. Vol. 324. Bellingham eWA WA: Spie Press, 2004.

[4] Khaleghi, Bahador, et al. *Multisensor data fusion: A review of the state-of-the-art*. Information Fusion 14.1 pp. 28-44. 2013.

[5] Lalmas, Mounia. *A formal model for data fusion. Flexible Query Answering Systems*. Springer Berlin Heidelberg, 274-288. 2002.

[6] Seo, Young Mi Jee, Hong Ke, Soontak Lee, *Rainfall Frequency Analysis and Uncertainty Quantification Using Dempster-Shafer Theory*, Korea Water Resources Association 2010 KWRA conference pp.1390-1394, 2010

[7] MLA Deng, Xinyang, and Yong Deng. *Multisensor Information Fusion Based on Dempster-shafer Theory and Power Average Operator*. Journal of Computational Information Systems 9.16 pp.6417-6424. 2013

[8] Castanedo, Federico. *A review of data fusion techniques*. The Scientific World Journal 2013 (2013).

[9] Yuan, Ye, Shuyuan Shang, and Li Li. *Network intrusion detection using DS evidence combination with generalized regression neural network*."Journal of Computational Information Systems 7.5 (2011): 1802-1809.

[10] Yu, Dong, and Deborah Frincke. *Alert confidence fusion in intrusion detection systems with extended Dempster-Shafer theory*. Proceedings of the 43rd annual Southeast regional conference-Volume 2. ACM, 2005.

[11] Burroughs, Daniel J., Linda F. Wilson, and George V. Cybenko. *Analysis of distributed intrusion detection systems using Bayesian methods*. Performance, Computing, and Communications Conference, 2002. 21st IEEE International. IEEE, 2002.

[12] Chen, Qi, and Uwe Aickelin. *Anomaly Detection Using the Dempster-Shafer Method*. DMIN. 2006.

[13] Chen, Qi, et al. *Data classification using the Dempster-Shafer method*" Journal of Experimental & Theoretical Artificial Intelligence 26.4, 493-517. (2014)

저 자 소 개

김동욱(Dong-Wook Kim)

2015년 : 가천대학교 컴퓨터공학과 공학사
2015년~현재 : 가천대학교 일반대학원 IT융합공학과 석사과정

관심분야 : Data Mining, data fusion
Phone : +82-31-750-5818
E-mail : kog7306@naver.com

한명묵(Myung-Mook Han)

1980년 : 연세대학교 공과대학 졸업 (공학사)
1987년 : 뉴욕공과대학교 컴퓨터공학과 석사졸업
1997년 : 오사카시립대학교 정보공학부 졸업 (공학박사)
1998년~현재 : 가천대학교 IT대학 교수
1998년~현재 : 한국지능시스템학회 이사

관심분야 : Security, Algorithm, Data Mining
Phone : +82-31-750-5522
E-mail : mmhan@gachon.ac.kr