情報保護學會論文誌
第14券 第2號, 2004. 4

퍼지적분을 이용한 침입탐지시스템 평가방법

김 미 혜
충북대학교

An Evaluation Method on Intrusion Detection System using Fuzzy Integrals

Mi-Hye Kim
Chungbuk University

요 약

인터넷이 급속하게 발전함에 따라 침입탐지의 유형도 매우 다양해지고 복잡해졌다. 이로 인해 발생하는 피해를 막기 위해 많은 침입탐지시스템이 개발되었다. 본 논문에서는 침입탐지시스템 평가기준에 대해 퍼지적분을 이용한 평가방법을 제시하였다.

ABSTRACT

In a result that the types of intrusion detection are getting diverse in accordance with rapid internet sprawl, many intrusion detection systems have been developed. In this paper, we will propose a novel evaluation on the evaluation criteria for the intrusion detection systems using Fuzzy integrals

Keywords: *IDS, Fuzzy measure, Fuzzy integral.*

Ⅰ. 서 론

침입 탐지란 시스템의 여러 사용 형태나 로그기록을 바탕으로 시스템의 불법 침입을 실시간으로 탐지해 내는 것을 말하고, 이러한 기능을 하는 시스템을 침입탐지시스템이라고 한다. 급속한 인터넷의 발전으로 정보공유가 활성화되고 있는 가운데 시스템의 운영체제나 다양한 응용프로그램이 가질 수 있는 소프트웨어적인 결함으로 인해 다양한 형태의 침입유형이 생겨났다. 이로 인해 서비스 중단이나 중요자료 유출 및 삭제 등의 피해도 상당하다. 이러한 피해를 막기 위해 현재 많은 침입탐지시스템이 존재하고 또 개발되고 있다. 침입탐지시스템 사용자는 보다 우수한 시스템을 선택하길 원할 것이다. 하지만 이에 대한 객관적인 평가 기준과 평가 방법이 필요하나 아직까지 정형화된 방법론이 없다. 본 논문에서는 침입탐지시스템 평가 방법론 개발 과정의 첫 단계로 이미 제시된 침입탐지시스템 평가기준과 각 기준에 대한 평가항목을 가지고 그 두 번째 단계로 퍼지적분을 이용하여 평가하는 방법을 제시하고자 한다. 1974년 Sugeno[1]에 의해 처음 소개된 퍼지측도(fuzzy measure)는 가법성(additivity)을 만족하지 않고, 단조성만을 고려한 일종의 집합치 함수이다. 이러한 퍼지측도에 관한 Sugeno의 퍼지 적분은, 어떤 대상을 여러 항목(또는 관점)에 대해서 평가하고 각 항목에 대해서 평가를 하고 각 평가 항목의 중요도에 차이가 있을 때 이들 평가치를 종합하는데 이용될 수 있다. 특히 퍼지 적분은 주관적인 판단이 개입되는 평가문제에서 유용하게 이용되므로, 의사결정(decision making) 문제, 비선형 분류 (nonlinear

접수일: 2004년 4월 3일; 채택일: 2004년 4월 19일
mhkim@chunbuk.ac.kr

classification), 비선형 다중회귀분석 (nonlinear multiregression) 문제들과 같은 데이터 마이닝 (data mining)이나 정보 융합(information fusion)분야[2,3,4] 뿐 아니라 어떤 대상을 평가하는 방법으로 다양한 분야에서 이용되어왔다.[5,6,7]

본 논문의 구성은 2장에서는 기존에 제시된[8] 7가지 평가기준과 각 평가 기준에 해당하는 평가항목을 소개한 후 퍼지적분을 이용한 평가방법을 제시하고, 3장에서는 퍼지적분의 개념을 일반화한 준노름 퍼지적분을 소개하고, 이를 이용한 평가 방법을 제시고 Sugeno 퍼지적분평가와 비교, 분석하고자 한다.

II. 퍼지적분을 이용한 침입탐지시스템 평가방법

2.1 침입탐지시스템 평가기준 및 항목

여기서는 많은 종류의 침입탐지 시스템들이 국내외에서 만들어지고 있으나 이들을 평가할 수 있는 기준이나 방법에 대한 연구가 미약하고, 게다가 침입수법의 종류가 매우 다양해짐에 따라 침입탐지시스템 역시 달라지므로 이를 평가하는 일은 매우 어렵다. 복잡한 시스템(Complex system)을 모델링 할 경우, 시스템을 기능에 따라 세분 또는 분할하여 다루는 것이 일반적이다. 이 방법은 기능적인 표현에는 시스템의 목적이 포함되기 때문에 시스템을 세분 또는 분할함으로써 시스템의 기본적인 목적을 충분히 표현 할 수 있다. 실제로 복잡한 시스템을 취급할 경우에는 시스템을 세분 또는 분할하는 문제(시스템 모델링)과 평가 대상을 측정하는 기준을 설정하는 문제(평가척도의 설정) 등을 해결 할 필요가 있다. 평가기준 설정 시에는 침입탐지시스템의 모든 특성이 포함될 수 있도록 하는 것이 중요한데 침입탐지시스템 평가 기준에 관한 연구[8]에 의하면 평가 기준 및 그에 해당하는 항목은 다음과 같은 목적을 가진 7개의 평가기준 설정과 각 평가기준에 대한 세부 평가항목으로 다음과 같이 분류를 되었다. 본 논문에서는 이것을 기준으로 하여 다음 절에서 적분평가를 하고자 한다.

① 기능적 측면(Capability) : 침입탐지시스템의 중심 기능에 대한 기능의 다양성과 깊이 평가
- 모니터링(Monitoring) 기능
- 침입탐지(Analysis) 기능
- 대응(Response) 기능
- 보고(Report) 기능

② 편이성 측면(Usability) : 침입탐지시스템의 중심 기능에 대해 배우고 사용하고, 수정함에 대한 편이성 평가

③ 성능적 측면(Performance) : 침입탐지시스템의 기능 수행시의 정확성, 속도, 자원 사용량 등의 성능 평가
- 침입 탐지율
- 침입 오판율
- 실시간 탐지 성능
- 자원 사용율

④ 관리적 측면(Manageability) : 대규모 환경에서 침입탐지시스템 설치, 설정, 제어기능 등의 평가
- 설치 및 제거
- 시스템관리
- 시스템 지원

⑤ 연동성 측면(Interoperability) : 표준 파일 포맷이나 네트워크 연결 등을 통한 다른 시스템 구성 요소와의 연동기능 평가

⑥ 확장성 측면(Scalability) : 대규모 환경으로 확장될 수 있도록 제공하는 기능 평가

⑦ 안정성 측면(Robustness) : 침입탐지시스템 자체 안전성에 대한 평가
- 취약성 부분
- 오용성 부분
- 보안성 부분

2.2 퍼지적분을 이용한 평가방법

여기서는 많은 종류의 침입탐지 시스템들이 국내외에서 침입탐지시스템을 일관된 기준으로 평가 할 수 있는 프레임워크 개발로 얻을 수 있는 이점은 상당하다. 침입탐지시스템을 개발하는 개발자는 자신이 개발하고 있는 시스템이 얼마나 효율적인지 판단 할 수 있고 컴퓨터 시스템에 대한 보안 대책을 마련하고자 하는 시스템 관리자는 여러 종류의 침입탐지시스템들을 비교해서 자신의 환경에 가장 적절한 시스템을 선택 할 수 있다. 일반적으로 복잡한 시스템은 시스템이 처음부터 지니고 있는 복잡성으로 인한 애매성이 존재하므로, 시스템을 세분 또는 분할하는 것 자체도 애매성을 남긴 채 수행되어 왔다. 이와 같이 애매함의 정도를 퍼지니스(fuzziness)로 간주하고,

L.A. Zadeh 가 제안한 퍼지집합(fuzzy ste)[10]으로서 이러한 퍼지니스를 멤버쉽함수(membership function)에 의하여 정량적으로 표현하고 있다. 이와 같이 주관적 평가를 기초로 하는 방법으로 T.L. Saaty가 제안한 AHP(Analytic Hierarchy Process)[5]가 있다. 이것은 평가기준의 중요도가 각 평가기준에 대한 대체안의 평가치는 평가자의 일대비교판단(pairwise comparison judgement)으로 구해지고, 그것을 "가법적"으로 합성하여 대체안에 대한 종합평가가 이루어진다.[5] 그러나, 평가의 주관적 척도는 가법성을 만족하지 못하는 경우가 많다. 이러한 경우의 척도를 구성하기 위하여 퍼지측도(fuzzy measure)[1]가 제안되어 있고, 퍼지측도를 이용하여 비가법적인 평가방법으로 퍼지적분(fuzzy integral) 이 제안되어 있다. 여기서 퍼지적분에 의한 평가법이라는 것은 가법성을 가지지 않는 평가기준의 중요도를 가법성을 만족하지 않는 주관적인 척도를 취급하는 퍼지측도로 하고, 퍼지적분에 의하여 종합평가하는 방법이다. 여기서 주목할 점은 퍼지측도는 가법적인 경우를 특별한 경우로 포함하고 있다는 것이다. 이러한 이유로 퍼지적분은 그 실용적인 가치가 인식되어 왔다. 우선 퍼지적분을 논의하기 전에 본 논문에서 사용될 몇 가지 정의와 기호를 먼저 소개하고자 한다.

$\mathscr{A}$는 공집합이 아닌 X의 부분집합의 σ-대수로 가정하자. 그리고 다음과 같은 성질을 만족하는 집합치 함수 $g: \mathscr{A} \rightarrow [0, 1]$는 퍼지측도(*fuzzy measure*)라고 불린다.

(1) $g(\emptyset)=0$:
(2) $A, B \in \mathscr{A}$, $A \subset B$ 이면 $g(A) \leq g(B)$이고 ;
(3) $A_n \in \mathscr{A}$, $A_1 \subset A_2 \subset \cdots$, 에 대해

$\bigcup_{n=1}^{\infty} A_n \in \mathscr{A}$을 만족하면

$\lim_{n \to \infty} g(A_n) = g(\bigcup_{n=1}^{\infty} A_n)$ 성립하고,

(4) $A_n \in \mathscr{A}$, $A_1 \supset A_2 \supset \cdots$, 에 대해서

$\bigcap_{n=1}^{\infty} A_n \in \mathscr{A}$을 만족하면

$\lim_{n \to \infty} g(A_n) = g(\bigcap_{n=1}^{\infty} A_n)$ 이 성립한다.

우리는 g가 가측공간(measurable space) $(X, \mathscr{A})$에서 퍼지측도 일 때, $(X, \mathscr{A}, g)$을 퍼지측도 공간(fuzzy measure space) 라고 부른다.

만약 $\mathscr{B}$가 [0, 1]의 Borel 부분집합들의 σ-대수인 곳에서 $B \in \mathscr{B}$ 였을 경우, 어떤 B 값에 대해서도 $h^{-1}(B) = \{x \mid h(x) \in B\} \in \mathscr{A}$ 라면, 실수 값을 가지는 함수 $h: X \rightarrow [0, 1]$ 은 $\mathscr{A}$와 $\mathscr{B}$에 대하여 $\mathscr{A}$-가측(*measurable*) 이다. (단, 아무런 혼동이 없을 때 그냥 가측이라고 부르는 것이 가능하다.)

$$L^0(X) = \{h: X \rightarrow [0, 1] \mid h \text{ 가 } \mathscr{A}\text{와 } \mathscr{B}\text{에 대하여 가측 (measurable) }\}$$

와 같은 가측함수 집합을 생각 할 수 있다. 이 때, $\mathscr{B}$는 통상적으로 [0, 1]의 **Borel** 부분집합들의 σ-대수이다. 주어진 h가 $h \in L^0(X)$인 어떤 경우에 있어서도, 우리는 $\alpha \in [0, 1]$일 때, $H_\alpha = \{x \mid h(x) \geq \alpha\}$라고 쓸 수 있다. 여기서 $\alpha \rightarrow g(H_\alpha)$ 가 왼쪽 연속임을 쉽게 알 수 있다.

$A \in \mathscr{A}$이고, $h \in L^0(X)$라고 가정하자. g에 대한 A 위에 있는 h의 퍼지적분(fuzzy integral)의 정의는 다음과 같다.

$$\int_A h \, dg = \sup_{\alpha \in [0, 1]} [\alpha \wedge g(A \cap H_\alpha)]$$

$A = X$일 때는 퍼지적분은 $\int h \, dg$ 로 나타내도 무방하다.

퍼지적분의 의미를 다음과 같이 생각해 볼 수 있다.[6]

집합 X를 어떤 대상에 대한 평가항목이라 하자. σ-대수를 X의 멱집합(power set)으로 생각하고, 그 원소 에 대해 정의되는 퍼지측도 $g(H)$는 대상의 전체적인 평가에 대해 항목 H의 평가치가 기여하는 정도, 즉 평가항목의 부분집합 H의 중요도(degree of important)라 하자. 그리고 X를 정의역으로 하는 함수 $h(x)$, $x \in X$는 평가항목 x에 대한 평가치라하자. 이 때 전체 평가항목 X에서의 평가함수 h의(중요도 함수 g에 대한) 퍼지적분 식을 단계적으로 해석하면 $\alpha \wedge g(A \cap H_\alpha)$ 에서 α는 X가 유한집합인 경우 $\inf_{x \in H} h(x)$를 의미하며 평가항목의 부분집합 H에 대해 가정 부정적인(보수적인) 평가치를 선택했다는 의미이며, $\alpha \wedge g(A \cap H_\alpha)$는 평가항목 중 가장 부정적인 평가치와 평가항목 H의 중요도에서 작은 것을 선택하는 것이다. 이렇게 선택하는 바

탕에는 가장 안전한(보수적인) 평가치를 가짐과 동시에, 평가치가 평가항목의 중요도 보다 클 수 없다는 의미를 부여하고 있다. 적분결과를 $\sup_{\alpha \in [0,1]} [\alpha \wedge g(A \cap H_\alpha)]$ 로 함으로써 여러 가지 가능한 H 중에서 가장 큰 값을 취하여 전체 평가치를 종합하고 있다. 즉, 이 부분에서 긍정적인(유리한) 항목을 부각시켜 낙관적인 평가를 하는 측면이 있다.

이러한 퍼지적분에 의한 평가법의 알고리즘을 다음과 같이 제시 할 수 있다.

[단계 1] 유한집합 X의 원소로 정해진 평가항목에 대한 멱집합의 원소 $H \in P(X)$에 대해 평가기준의 중요도, 즉 ,전체집합 X에 대해 부분집합 H가 기여하는 정도 $g(H)$를 결정한다.

[단계 2] 각 평가 항목에 대한 평가값 $h(x_i)$을 [0 , 1]의 값으로서 구하고 그 크기 순으로 나열한다. 즉,

$x_i \in X\ (i = 1, 2, \cdots n)$에 대해

$h(x_1) \le h(x_2) \le \cdots \le h(x_n)$ 이라 하고, 순서가 정해진 x_i들에 대해 H_i를 다음과 같이 구할 수 있다.

$H_i = \{x_k \mid k = i, i+1, \cdots, n\}$

[단계 3] 각각의 i에 대해서 $h(x_i) \wedge g(H_i)$를 계산한다.

[단계 4] 단계3에서 구한 모든 값의 max값을 평가치로 한다.

여기서 연속 함수일 때는 sup를 사용하고 (X가 무한 집합인 경우), 이산적인 함수에는 max를 사용함에 유의하자.

2.3 퍼지적분을 이용한 평가 예제

예를 들어 두 회사에서 새롭게 개발한 침입탐지시스템을 평가하는 문제를 생각해보자. 먼저 평가단(혹은 침입탐지시스템을 사용하고자 하는 소비자)은 침입탐지시스템이 갖추어야할 조건을 결정한 후, 각 조건의 상대적인 중요도를 결정해야 할 것이다. 여기서 우리는 앞서 언급한 평가항목과 평가기준 중의 하나인 기능적 측면에 대한 평가를 생각해 보자. 우선, 평가 항목으로 데이터 소스를 선별적으로 설정 할 수 있는지의 여부에 대한 모니터링 기능, 탐지 가능한 가용성, 기밀성, 무결성과 가능한 침입탐지 행위의 종류 및 접근제어(Access control) 설정 기능에 대한 침입탐지기능, 어떤 종류의 알람 방법이나 대응행위가 있는지, 탐지된 공격에 대해 주는 조언이 무엇인지에 대한 대응 기능, 마지막으로 사용자 정의 보고서(로그 쿼리) 생성능력의 여부와 침입 세션 가능성 여부에 대한 보고서 기능을 본다고 하자. 즉 X = {모니터링 기능, 침입탐지 기능, 대응 기능, 보고서 기능} 이라고 하자. 그리고 각 평가항목의 중요도에 대한 퍼지측도를 다음과 같이 나타낸다고 하자.

$g(\{\text{모니터링기능}\}) = 0.4$, $g(\{\text{침입탐지기능}\}) = 0.35$,
$g(\{\text{대응 기능}\}) = 0.5$, $g(\{\text{보고서 기능}\}) = 0.3$,
$g(\{\text{침입탐지 기능, 보고서 기능}\}) = 0.4$,
$g(\{\text{모니터링 기능, 보고서 기능}\}) = 0.5$,
$g(\{\text{모니터링 기능, 침입탐지 기능}\})$
$= g(\{\text{침입탐지 기능, 대응 기능}\}) = 0.6$
$g(\{\text{모니터링 기능, 대응 기능}\})$
$= g(\{\text{대응 기능, 보고서 기능}\})$
$= g(\{\text{모니터링 기능, 침입탐지 기능, 보고서 기능}\})$
$= g(\{\text{침입탐지 기능, 대응 기능, 보고서 기능}\})$
$= 0.7$
$g(\{\text{모니터링기능, 침입탐지기능, 대응기능}\}) = 0.8$,
$g(\{\text{모니터링기능, 대응기능, 보고서기능}\}) = 0.9$
$g(\varnothing) = 0$, $g(\{\text{모니터링 기능, 침입탐지 기능, 대응기능, 보고서 기능}\}) = 1$

여기서 퍼지측도 $g(\cdot)$는 가법성을 만족하지 않는다. 다시 말해서,

$g(\{\text{모니터링 기능}\}) = 0.4$,

$g(\{\text{침입탐지 기능}\}) = 0.35$, 이지만,

$g(\{\text{모니터링 기능, 침입탐지 기능}\}) = 0.6$ 으로 두 퍼지측도의 합인 0.75가 아니다.

표 1. 기능적인 측면의 각 항목에 대한 평가값

회사	모니터링 기능	침입탐지 기능	대응 기능	보고서 기능	합계
A	0.75	0.8	0.85	0.95	3.35
B	0.79	0.85	0.8	0.9	3.34

평가단에 의해 A, B 두 회사의 침입탐지시스템 제품이 다음과 같은 평가치를 얻었다고 가정하자.

먼저 A 회사의 침입탐지시스템에 대해 퍼지적분을 이용한 평가 값을 다음과 같이 구할 수 있다. 우선,

$x_i \in X(i = 1, 2, \cdots, n)$에 대하여

$h(x_i) \leq h(x_{i+1})$ 이라 하고

$H_i = \{x_k | k = i, i+1, \cdots, n\}$ 이라 하자. 표 1의 평가값에 의하면

$h_A(\{$모니터링 기능$\}) = 0.75$,

$h_A(\{$침입탐지 기능$\}) = 0.8$,

$h_A(\{$대응 기능$\}) = 0.85$,

$h_A(\{$보고서 기능$\}) = 0.95$. 이므로

$x_1 =$ 모니터링 기능, $x_2 =$ 침입탐지기능,

$x_3 =$ 대응기능, $x_4 =$ 보고서 기능, 이라 할 수 있다. 이 때

$h_A(\{$모니터링 기능$\}) \leq h_A(\{$침입탐지 기능$\})$

$\leq h_A(\{$대응 기능$\}) = 0.85 \leq h_A(\{$보고서 기능$\})$

와 같은 크기를 갖기 때문에

$H_1 =$ {모니터링 기능, 침입탐지 기능, 대응 기능, 보고서 기능},

$H_2 =$ {침입탐지 기능, 대응 기능, 보고서 기능}

$H_3 =$ {대응기능, 보고서기능},

$H_4 =$ {보고서기능}임을 알 수 있다.

따라서, 평가항목의 중요도 $g(\cdot)$와 A회사에 대한 평가치 h_A를 이용하여 A회사의 침입탐지시스템에 대한 종합평점을 구하면 다음과 같다.

$$\int h_A \, dg$$

$= h_A(\{$모니터링 기능$\}) \wedge g(\{$ 모니터링 기능, 침입탐지 기능, 대응 기능, 보고서 기능$\})$

$\vee [\, h_A(\{$침입탐지 기능$\}) \wedge g(\{$침입탐지 기능, 대응 기능, 보고서 기능$\})]$

$\vee [\, h_A(\{$대응기능$\}) \wedge g(\{$대응기능, 보고서기능$\})]$

$\vee [\, h_A(\{$보고서 기능$\}) \wedge g(\{$보고서 기능$\})\,]$

$= (0.75 \wedge 1) \vee (0.8 \wedge 0.7) \vee (0.85 \wedge 0.7)$

$\vee\ (0.95 \wedge 0.3) = 0.75$

따라서 A회사의 침입탐지시스템의 기능적 측면에 대한 퍼지적분을 이용한 평가치는 0.75이다. 반면 B회사의 침입탐지시스템의 기능적 측면에 대해 퍼지적분 평가값을 구하면,

$h_B(\{$모니터링기능$\}) = 0.75$,

$h_B(\{$침입탐지기능$\}) = 0.85$,

$h_B(\{$대응기능$\}) = 0.8$,

$h_B(\{$보고서기능$\}) = 0.9$ 이므로

$x_1 =$ 모니터링 기능, $x_2 =$ 대응기능,

$x_3 =$ 침입탐지기능, $x_4 =$ 보고서 기능

으로 A회사와 비교해 보면 x_2와 x_3이 바뀌었음을 알 수 있다.

위와 같은 방법으로 Sugeno 퍼지적분을 이용한 평가치를 구하면

$$\int h_B \, dg$$

$= (0.79 \wedge 1) \vee (0.8 \wedge 0.7) \vee (0.85 \wedge 0.4) \vee (0.9 \wedge 0.3) = 0.79$

이다. 따라서 B회사의 침입탐지시스템의 기능적 측면에 대한 평가치는 0.79이다. 평가점수의 합계는 A 회사가 더 높지만 퍼지적분의 결과로부터 B회사가 A회사보다 침입탐지시스템의 기능적 측면은 더 우수하다고 할 수 있다.

이와 같은 방법으로, 두 회사의 안정성 측면을 퍼지적분을 이용하여 평가해 보기로 하자. 앞에서 언급

표 2. 평가항목 부분집합의 퍼지측도 값

	{취약성 부분}	{오용성부분}	{보안성부분}	{취약성, 오용성부분}	{취약성, 보안성부분}	{오용성, 보안성부분}
퍼지측도값	0.5	0.2	0.8	0.6	0.9	0.8

표 3. 안정성 측면의 항목에 대한 평가값 및 적분평가치

회 사	취약성 부분	오용성 부분	보안성 부분	합 계	Sugeno퍼지적분평가값
A	0.7	0.3	0.9	1.9	0.8
B	0.9	0.8	0.4	2.3	0.6

했듯이 안정성측면에 대한 평가항목은

$X=\{$취약성 부분, 오용성 부분, 보안성 부분$\}$

으로 둘 수 있다. 이에 대한 퍼지측도값을 다음과 같이 설정 할 수 있다. 즉, 이는 전체적인 평가에 대해 평가항목의 부분집합 H의 중요도(degree of important)라 하자.

평가단에 의해 두 회사의 평가치는 다음과 표 3과 같다고 하자.

이를 퍼지적분을 이용하여 두 회사의 안정성 측면을 각각 계산하면 다음과 같다.

A회사의 침입탐지시스템의 안정성 평가치는

$$\begin{aligned}\int h_A\,dg &= (0.3\wedge 1)\vee(0.7\wedge 0.9)\\ &\quad\vee(0.9\wedge 0.8)\\ &= 0.8\end{aligned}$$

이므로 0.8 이고, 반면 B회사의 평가치는

$$\begin{aligned}\int h_B\,dg &= (0.4\ \wedge 1)\vee(0.8\wedge 0.6)\\ &\quad\vee(0.9\wedge 0.5)\\ &= 0.6\end{aligned}$$

이므로 0.6이다. 여기서 우리는 표3에서 보듯이 각 항목에 대한 수치적 평가 합계가 A회사의 제품이 더 높을지라도 중요도가 높은 보안성 부분에서 B회사보다 훨씬 우수한 점수를 받았기에 퍼지적분의 결과로 A회사가 안정성 측면에서는 더 우수하다고 판정할 수 있다.

어떠한 대상을 평가하고자 할 때에는 대상에 따라 적합한 평가기준을 사용하여야 하며, 그 평가기준의 객관성 및 주관성 여부를 파악하여야 한다. 객관적인 성질만으로 평가기준이 주어지는 경에는 가법성을 만족하는 기존의 방법을 사용하면 된다. 그러나, 만약 주관성을 가진 평가기준이 포함되어 있어 평가자의 주관이 개입되어 퍼지니스가 수반된다고 판단되어 질 경우에는 가법성을 완화하여 대상을 측정하는 인간의 주관적인 척도로 해석되는 퍼지측도를 가지고 본 논문에서 제안한 퍼지적분을 이용하는 것이 합리적이라고 할 수 있다. 실제로 X가 유한개의 항목을 가진 유한 집합인 경우 이에 대한 퍼지적분 값은 $h(x_i)$와 $g(H_i)$에 대해 $h(x_k)\wedge g(H_k)$ 보다 작은 것이 $n-1$개 있고, 그 보다 큰 것이 n개 있다. 그런데 $g(X)=1$ 이므로 이를 제외하면

$$\{h(x_i)\mid i=1,2,\cdots,n\}\cup\{g(H_i)\mid i=1,2,\cdots,n\}$$

의 중간값이 된다. 따라서 이 적분값을 확률적 기대값에 상대적인 개념으로 "퍼지기대값"으로 인식 할 수 있어 큰 의미를 부여할 수 있다.

Ⅲ. t-준노름퍼지적분을 이용한 평가 방법

지금까지 Sugeno퍼지적분을 이용한 평가방법은 주관적인 평가기준이 포함되어 평가자 혹은 평가기관의 주관이 개입되어 평가대상의 실정에 맞춘 평가가 가능하다는 이유로 다양한 분야에서 시도되어왔다.[2,3,4,5,6,7,8] 이러한 평가방법은 평가기준의 중요도의 크기에 따라 퍼지적분의 평가치가 달라진다는 사실을 시사한다. 본 장에서는 일반적인 퍼지측도에 대해서 평가방법의 다양성을 내포하는 준노름퍼지적분에 대해 논의하겠다. Suarez 와 Gill은[11,12] t-준노름(seminorm)과 t-준코노름(semiconorm) 두 작용소를 사용하여 두 개의 퍼지적분족을 정의하였다. 즉, 준노름 퍼지 적분은 2.2절에서 소개된 Sugeno의 퍼지적분을 확장한 개념이기도하다. 이 장에서는 t-준노름에 의해 정의된 준노름 퍼지적분에 대한 소개와 그에 대한 이론적 성질을 알아보자.

다음의 두 가지 조건을 만족하는 함수

$\top:[0,1]\times[0,1]$을 t-준노름 ($t-$seminorm) 이라 한다.

(1) $x\in[0,1]$인 각각의 x 값에 대하여,

$$\top(x,1)=\top(1,x)=x$$

(2) 만약 $x_1,x_2,x_3,x_4\in[0,1]$인 경우,

$x_1 \le x_3,\ x_2 < x_4$ 일 때
$\top(x_1, x_2) \le \top(x_3, x_4)$ 이 성립한다.

식 (1)은 일종의 경계조건을 의미하고 식 (2)는 함수의 단조성을 의미하고 있다.

다음과 같은 함수들은 t-준노름의 예제들이다.

(1) $\top_1(x, y) = x \wedge y$
(2) $\top_2(x, y) = xy$
(3) $\top_3(x, y) = 0 \vee (x + y - 1)$

위에서 소개한 세 개의 t-준노름은 다음과 같은 크기 순서가 성립한다.

$$0 \le 0 \vee (x + y - 1) \le xy \le x \wedge y \le 1 \qquad (1)$$

$\top$ 을 t-준노름 이라고 가정하자. $L^0(X)$의 원소인 모든 h 에 대하여, 집합 A상의 h의 준노름 퍼지적분(seminormed fuzzy integral)은 다음과 같이 정의된다.

$$\int_A h \top g = \sup_{\alpha \in [0,\,1]} \top(\alpha,\ g(A \cap H_\alpha)).$$

t-준노름의 예제 중 첫 번째 함수 $\top(x, y) = x \wedge y$에서도 보듯이 분명히 준노름 퍼지적분은 Sugeno 퍼지적분을 일반화한 적분임을 알 수 있다. 또한 식 (1)에서 처럼 t-준노름의 크기가 주어졌기 때문에 준노름 퍼지적분 역시 어떤 t-준노름을 쓰느냐에 따라 적분값의 크기가 주어질 것이다. 다시 말해서,

$$\int h \top_3 g \le \int h \top_2 g \le \int h \top_1 g$$

과 같은 크기가 주어진다. 이는 주어진 평가기준에 대한 중요도로 다양한 평가방법을 활용하므로서 평가결과치가 구간의 값으로 나오는 것을 의미한다. 2장에서 다루었던 침입탐지시스템의 기능적인 측면과 안정성 측면에 대하여 주어진 세 가지 경우의 준노름 퍼지적분 평가값을 구해보자.

앞에서 평가했었던 A 회사에 대한 침입탐지시스템의 기능적측면을 $\top_2(x, y) = xy$ 입장에서 평가하면,

$$\begin{aligned}
&\int h_A \top_2 g \\
&= \top_2[\, h_A(\{\text{모니터링 기능}\}),\ g(\{\text{모니터링 기능, 침입탐지 기능, 대응 기능, 보고서 기능}\})] \\
&\quad \vee \top_2[\, h_A(\{\text{침입탐지 기능}\},\ g(\{\text{침입탐지 기능, 대응 기능, 보고서 기능}\})] \\
&\quad \vee \top_2[\, h_A(\{\text{대응 기능}\}),\ g(\{\text{대응 기능, 보고서 기능}\})] \\
&\quad \vee \top_2[\, h_A(\{\text{보고서 기능}\}),\ g(\{\text{보고서 기능}\})] \\
&= \top_2[\, 0.75,\ 1] \vee \top_2[\, 0.8,\ 0.7] \\
&\quad \vee \top_2[0.85,\ 0.7] \vee \top_2[0.95,\ 0.3] \\
&= 0.75
\end{aligned}$$

으로 Sugeno의 평가방법과 같은 수치가 나왔다. 반면, B회사에 대한 평가를 같은 방법으로 하면

$$\begin{aligned}
&\int h_B \top_2 g \\
&= \top_2[\, h_B(\{\text{모니터링 기능}\}),\ g(\{\text{모니터링 기능, 침입탐지 기능, 대응 기능, 보고서 기능}\})] \\
&\quad \vee \top_2[\, h_B(\{\text{대응 기능}\},\ g(\{\text{침입탐지 기능, 대응 기능, 보고서 기능}\})] \\
&\quad \vee \top_2[\, h_B(\{\text{침입탐지 기능}\}),\ g(\{\text{침입탐지 기능, 보고서 기능}\})] \\
&\quad \vee \top_2[\, h_B(\{\text{보고서 기능}\}),\ g(\{\text{보고서 기능}\})] \\
&= \top_2[\, 0.79,\ 1] \vee \top_2[\, 0.8,\ 0.7] \\
&\quad \vee \top_2[\, 0.85,\ 0.7] \vee \top_2[\, 0.95,\ 0.3] \\
&= 0.79
\end{aligned}$$

이다. t-준노름 $\top_3(x, y) = 0 \vee (x + y - 1)$ 를 이용한 준노름퍼지 평가값도 같은 방법으로 평가값을 구할 수 있고 아래 표 4와 같은 결과를 볼 수 있다.

우리는 여기서 준노름 퍼지적분 평가치나 앞서 제시한 Sugeno 퍼지적분 평가치가 다르지 않음을 볼 수 있다. 그러나 침입탐지시스템의 안정성 측면에 대한 평가 결과를 비교하면, A회사에 대한 준노름퍼지 평가치를 구하면

$$\int h_A \top_2 g$$

표 4. 기능적인 측면의 준노름 퍼지적분 평가치 비교

회사	모니터링	침입탐지	대응	보고서	합계	$\int h \top_1 g$	$\int h \top_2 g$	$\int h \top_3 g$
A	0.75	0.8	0.85	0.95	3.35	0.75	0.75	0.75
B	0.79	0.85	0.8	0.9	3.34	0.79	0.79	0.79

표 5. 안정성 측면의 준노름 퍼지적분 평가치 비교

회사	취약성	오용성	보안성	합계	$\int h \top_1 g$	$\int h \top_2 g$	$\int h \top_3 g$
A	0.7	0.3	0.9	1.9	0.8	0.72	0.7
B	0.9	0.8	0.4	2.3	0.6	0.48	0.4

$= \top_2[h_A(\{$오용성 부분$\}),\ g(\{$오용성 부분, 취약성 부분, 보안성 부분 $\})]$
$\vee \top_2[h_A(\{$취약성 부분$\},\ g(\{$취약성 부분, 보안성 부분$\})]$
$\vee \top_2[h_A(\{$보안성 부분$\}),\ g(\{$보안성 부분$\})]$
$= \top_2[0.3,\ 1] \vee \top_2[0.7,\ 0.9] \vee \top_2[0.9,\ 0.8]$
$= 0.72$

와 같이 Sugeno 퍼지적분 평가값 $\int_A h \top_1 g = 0.8$과는 다르다는 것을 알 수 있다. B회사에 대한 준노름퍼지적분 평가치를 같은 방법으로 다음과 같이 구할 수 있다.

$\int h_B \top_2 g$
$= \top_2[h_B(\{$보안성 부분$\}),\ g(\{$오용성 부분, 취약성 부분, 보안성 부분 $\})]$
$\vee \top_2[h_B(\{$오용성 부분$\},\ g(\{$오용성 부분, 취약성 부분$\})]$
$\vee \top_2[h_B(\{$취약성 부분$\}),\ g(\{$취약성 부분$\})]$
$= \top_2[0.4,\ 1] \vee \top_2[0.8,\ 0.6] \vee \top_2[0.9,\ 0.5]$
$= 0.48$

이다. $\int h \top_3 g$에 대한 두 회사의 평가치도 같은 방법으로 구할 수 있고 그 결과는 표 5에 두었다.

표 4의 침입탐지시스템의 기능적인 측면의 준노름 퍼지적분 평가치를 비교하면 값의 변동이 없음을 알 수 있다. 이는 각 항목에 대한 평가치의 변동이 크지 않기 때문에 발생하는 현상 중의 하나이다. 반면 표 5 에서와 같이 항목 간의 점수 차이가 큰 안정성 측면에 대한 준노름 적분값은 A회사인 경우 0.7에서 0.8까지의 변동성을 제시하고 B회사인 경우에는 0.4에서 0.6까지의 변동성을 제시하므로 평가결과치가 구간값으로 나오게 된다. 이것은 시스템 평가시 평가대상 시스템의 실정에 맞춘 평가가 가능하다고 할 수 있다.

Ⅳ. 결 론

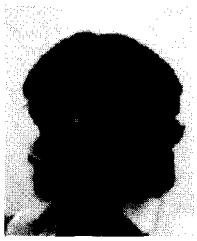
지금까지 침입탐지시스템 평가기준에 관한 연구[8]에서 제시한 평가항목을 가지고 평가항목간의 상호중복성 및 평가자의 주관성 개입을 고려하여 퍼지측도 및 퍼지적분을 이용한 평가방법을 제시하였고, 이는 평가단(혹은 사용단체)의 실정에 맞추어 평가할 수 있는 편리함이 있다는 이점을 인지하여 크기가 주어진 준 노름 퍼지적분법을 제시 하므로서 평가결과치가 구간값으로 나오므로 준노름 퍼지적분을 이용한 평가방법이 합리적이라고 할 수 있다. 또항 평가대상의 실정이나 상황에 따라 평가대상에 맞추어 t-준노름이나 퍼지측도를 적절하게 선택하여 평가하는 방법으로 재시된 준노름 퍼지적분평가 방법은 평가대상에 대한 평가 유연성이 크다고 볼 수 있다. 향후의 연구과제로서 기존에 행해진 평가항목들에 관한 비교연구를 통하여 합리적인 평가기준의 설정 및 평가방법에 대한 연구가 더욱 필요하다고 판단된다.

참 고 문 헌

[1] M. Sugeno, "Theory of Fuzzy

Integrals and Its Applications," Ph. D Dissertation Thesis, Tokyo Institute of Technology, 1974.
[2] K. S .Leung, M. L. Wong, W. Lam, Z. Wang, and K. Xu, "Learning nonlinear multiregression networks based on evolutionary computation," IEEE T. SMC 32, No. 5, pp.630-644, 2002.
[3] Z. Wang, "A new genetic algorithm for nonlinear multiregressions based on generalized Choquet integral," Proc. FUZZ-IEEE2003, pp.819-821.
[4] K. Xu, Z. Wang, and K.S. Leung, "Classification by nonlinear integral projections," IEEE T. Fuzzy Systems, Vol. 16, pp.949-962, 2003
[5] 황승국, "퍼지적분을 이용한 기업평가법", 공업경영학회지, 제 19권, pp.271-280, 1996
[6] 손영선, "퍼지척도 퍼지적분을 이용한 휴먼 인터페이스의 평가," 한국퍼지 및 지능시스템학회 1998 추계학술대회 학술발표논문집, pp. 31-36
[7] 이철영, 임봉택, "퍼지평가의 통합특성에 관하여," 한국항만학회, 제 13권 제 1호, pp.79-85, 1999
[8] 유신근, 이남훈, 심영철, 김홍근, 김기현, "침입탐지시스템 평가 기준에 관한 연구", 정보과학회논문지, 92권, pp.300-302, 1999
[9] 장이채, 퍼지과학의 세계, 교우사, 1997
[10] L. A. Zadeh, "Fuzzy Sets," Information and control, Vol. 8, pp. 338-353, 1965
[11] Suarez Garcia and P. Gil. Alvarez, "Two Families of Fuzzy Integrals," Fuzzy Sets and Systems, Vol. 18, pp. 67-81, 1986.
[12] F. Suarez Garcia and P.Gil Alvarez, "Measures of Fuzziness of Fuzzy Events," Fuzzy Sets and System, Vol. 21, pp. 147-157, 1987.

〈著者紹介〉



김 미 혜 (Mi-Hye Kim) 정회원
1992년 2월: 충북대학교 수학과 졸업
1994년 2월: 충북대학교 수학과 석사
2001년 2월: 충북대학교 수학과 박사
2001년 4월~현재: 충북대학교 전기전자컴퓨터 초빙교수
〈관심분야〉 퍼지적분, 정보보호