情報保護學會論文誌
第13券 第3號, 2003. 6

퍼지제어를 이용한 관련성 통합탐지

김 용 민*

An Aggregate Detection of Event Correlation using Fuzzy Control

Yong-Min Kim

요 약

침입탐지시스템은 사용된 알고리즘이나 기법의 특성에 따라 여러 탐지영역에 대해서 상이한 탐지결과를 나타내게 된다. 따라서 서로 다른 탐지영역을 갖는 여러 탐지시스템들의 결과를 통합함으로써 탐지영역을 넓힐 수 있는 통합탐지 방법이 필요하다. 또한 통합 시에 발생할 수 있는 수많은 잘못된 보고의 수를 최소화함으로써 보안 관리자의 업무 부담을 줄이고 탐지결과의 정확성을 높일 필요가 있다.

이 논문에서는 시스템 사용행위에 대해서 각 탐지시스템들이 모호한 판정의 결과값을 내어놓는 경우 분석된 탐지시스템의 특성을 퍼지추론을 이용하여 통합탐지 한다. 분석된 탐지 특성은 퍼지제어의 과정에서 적용된 각 탐지시스템에 대한 소속함수와 제어규칙으로 표현한다. 그리고, 모호한 판정 값을 통합하고 잘못된 보고의 숫자를 최소화하였으며, 여러 번의 실험을 통해 결정된 임계값의 적용으로 추론의 적용대상이 최소화되도록 하였다.

ABSTRACT

An intrusion detection system shows different result over overall detection area according to its detection characteristics of inner detection algorithms or techniques. To expand detection areas, we requires an integrated detection which can be archived both by deploying a few detection systems which detect different detection areas and by combining their results. In addition to expand detection areas, we need to decrease the workload of security managers by false alarms and improve the correctness by minimizing false alerts which happen during the process of integration.

In this paper, a method for aggregation detection use fuzzy inference to integrate a vague detection results which imply the characteristics of detection systems. Their analyzed detection characteristics are expressed as fuzzy membership functions and fuzzy rule bases which are applied through the process of fuzzy control. And, it integrate a vague decision results and minimize the number of false alerts by reflecting the characteristics of detection systems. Also it does minimize inference objects by applying thresholds decided through several experiments.

Keyword : *침입탐지시스템(IDS), 관련성(Correlation), 통합탐지(Aggregate Detection) , 퍼지제어(Fuzzy control)*

Ⅰ. 서 론

침입탐지시스템들은 알려진 공격에 대한 패턴이나 상태전이를 이용하는 오용행위 탐지시스템과 시스템의 사용자, 자원, 프로세스 등에 대한 정상행위 프로파일을 기준으로 공격을 판정하는 비정상행위 탐지시스템을 단일 호스트나 지역 및 네트워크 등의 보호하고자 하는 영역에 배치하여 수행한다. 그러나 각 탐지시스템은 적용하는 탐지기술의 특성에 따라 여러 탐지영역에 대해서 정확성(correctness)에 대한 상

* 전남대학교 리눅스시스템 보안연구센터(ymkim@chonnam.ac.kr)

이한 탐지성능을 나타내며 제한적이다. 이러한 점을 극복하기 위해, 알려진 공격 및 비정상행위 공격을 탐지하기 위해 각 탐지영역에서 우수한 성능을 보이는 탐지시스템 결과를 통합하여 탐지영역을 확장하고 전체적인 탐지성능을 높이는 방법이 필요하다. 또한, 각 탐지시스템의 결과에서 발생할 수 있는 많은 잘못된 보고(false alarm)의 수를 최소화하고 탐지결과의 정확성을 높이는 것이 요구된다.

이 논문에서는 각 탐지 영역에 대한 탐지시스템들의 모호한 결과들에 대한 통합탐지를 위해서 퍼지제어(fuzzy control)를 사용하였다. 통합탐지를 위해서 호스트 내의 모든 각 탐지시스템에 대해서 퍼지집합(fuzzy set)을 정의하고 각 소속멤버에 대한 소속함수(membership function)를 정의한다. 또한 퍼지추론(fuzzy inference) 시에 필요한 퍼지 제어규칙(fuzzy control rule set)은 각 탐지시스템의 비정상행위 감사로그를 분석해 작성한다. 발생한 이벤트에 대해서 각 탐지시스템들이 모호한 판정의 결과값을 내어놓는 경우 오프라인으로 생성된 퍼지 제어규칙으로부터 관련된 규칙들을 찾아내고, 관련된 규칙들과 결과값은 퍼지추론을 통해서 각 시스템간의 탐지영역에 대한 탐지특성이 상호 반영된 하나의 결과값을 내어놓게 된다. 관련규칙을 찾는 과정에서 통합이 필요하지 않는 감사데이터들은 필터링하고, 추론의 과정을 통해서 부적절한 감사데이터를 제거함으로써 잘못된 보고의 수도 줄일 수 있다.

이 논문의 구성은 다음과 같다. 관련연구에서 기존의 통합탐지 접근방법 및 통합을 위한 퍼지제어의 특성을 소개하고 퍼지제어 다중시스템 통합탐지시스템의 전체적인 구조와 퍼지의 적용방법에 대해서 기술한다. 그리고 실험결과 및 분석을 통해 기존연구와 비교분석 하며, 마지막으로 결론 및 향후 연구방향에 대해서 서술한다.

II. 관련연구

다수의 탐지시스템이 동시에 공격으로 간주되는 이벤트에 대해서 탐지를 시도한다면 각 탐지시스템의 탐지영역은 중첩될 수 있고 이러한 중첩된 탐지영역은 탐지시스템 간의 상호 관련구간으로서 통합과정에서 탐지시스템 간의 관련정도를 고려하여 반영시켜야 한다. 탐지시스템 사이의 통합을 위해서는 각 탐지시스템이 생성하는 감사데이터로부터 상호 관련성(correlation)을 추출해낼 수 있는 방법론이 요구되며, 현재의 침입탐지 시스템에서 통합탐지의 방법은 명백한 관련성 및 함축적 관련성으로 구분할 수 있다.

명백한 관련성에 의한 접근방식은 공격에 대한 정보를 충분히 보유하고 있다는 가정하에서 진행된다. 공격에 대한 정보는 연속적으로 연관된 감사데이터를 논리적인 링크로 표현한다. 따라서 하나의 공격 혹은 전체적인 공격을 위한 중간단계의 공격은 감사데이터들이 논리적인 링크로 연결된 하나의 그룹으로 표현된다. 또한 그룹간의 논리적인 링크는 전체적인 공격을 달성하기 위한 전이로 생각할 수 있고 전체적으로는 최종 공격을 위한 절차로 생각할 수 있다. 명백한 관련성에 의한 접근방식은 공격행위 정보를 사전에 데이터베이스로 구축해 놓아야한다는 단점이 있지만 알려진 공격에 대한 탐지성능이 뛰어나고 최종 공격을 위한 사전 공격단계에서 탐지가 가능하다는 장점이 있다. 이와 같은 방법에는 개별적인 선행조건과 수행결과에 따른 MIRADOR의 CRIM[1], 알려진 공격의 시나리오에 기반한 LAMBDA[2] 방법이 이에 해당한다.

함축적인 관련성에 의한 접근방식은 감사데이터 내 구성 정보사이의 관련성 정도를 정보로 유지한다. 패킷주소와 같은 감사데이터에서 탐지시스템 사이의 관련성을 찾는 것이다. 현재의 통합탐지 시스템에서 감사데이터 내의 척도(measures)들 간의 관련성을 추출하기 위한 방법으로 분류, 데이터마이닝, 신경망 등과 같은 학습기술들을 이용해 추출해내는 방법이 있다. *IBM/Tivoli*의 TEC[3], DARPA의 EMERALD[4, 5, 6] 이 이와 같은 방법에 해당한다.

침입탐지에 퍼지제어를 이용한 방법[7, 8]이 감사데이터 내 구성요소들 간의 관련성을 근거로 하여 관련성을 찾는 방법이라고 한다면, 현재 탐지영영역에 따른 이종의 침입탐지시스템을 통합하기 위하여 각 탐지시스템의 탐지 값으로부터의 관련성을 이용한 조건부 확률적 방법[9] 및 퍼지제어 적용 방법[10]이 고려된다. 기존의 연구는 관련성 분석을 위한 입력의 대상으로 감사데이터의 구성요소들이라는 명확히 관련성을 도출할 대상이 존재하지만 탐지영역 사이의 특성에 따라 개발된 탐지시스템의 관련성 접근방식은 명확한 관련성의 대상이 존재하지 않고 관련성을 도출할 대상 자체가 탐지 값 내부에 함축되어 있기 때문이다. 결과적으로 탐지영역이 다른 탐지시스템들 사이의 관련성 접근방식은 탐지영역 간의 관련성 정보가 함축된 탐지 값으로부터 함축되어 있는 탐지시스템 간의 관련성 정도를 도출해 줄 수 있는 방법이 필요

하다. 즉, 도출된 각 탐지시스템의 탐지특성들을 반영한 하나의 결과를 만들어줄 수 있는 방법이 요구된다.

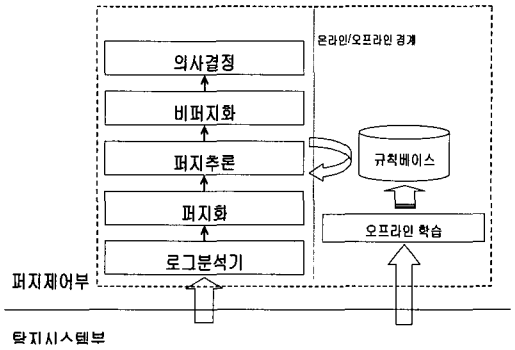
조건부 확률적 방법의 연구에서는 시스템의 동일한 탐지로그 데이터로부터 판단한 각 탐지시스템의 결과 대해 탐지특성을 반영한 탐지결과의 지지율 테이블을 생성하고 실시간에 이를 반영한 결과를 도출하는 방법이다. 그러나 이의 방법에서 지지율 테이블의 갱신 학습시간에 따른 재적용 시간의 지연과 최종 판단시의 최대값을 선택하는 방법에 의해 잘못된 보고의 가능성을 내포하고 있다. 따라서 이러한 요구조건을 만족시킬 수 있는 방법으로 각 탐지시스템의 탐지특성을 이끌어 내는 데는 각 탐지시스템에 대한 퍼지 소속함수를 탐지 값에 적용하고 탐지특성들 간의 통합은 퍼지 추론의 과정에서 퍼지 제어규칙들을 적용하는 수학적으로 검증된 방법을 사용함으로써 실시간의 탐지 및 검증이 가능하도록 정형화할 수 있다.

퍼지제어 시스템은 퍼지화부, 지식베이스, 추론(의사결정)부 그리고 비퍼지화부 등으로 구분할 수 있다. 퍼지화부는 하나의 명확한 값(crisp value)으로 들어오는 입력에 대해서 적절한 퍼지값으로 변경하는 역할을 수행하게 되는데 만일 입력값에 대한 신뢰도가 보장된다면 입력값을 퍼지 단일값으로 변화시킴으로써 추론을 단순화 할 수 있다. 지식베이스는 크게 두 부분으로 나뉘어진다. 한 부분은 입력값에 대해서 제어 시스템의 제어특성을 반영할 수 있는 적절한 퍼지분할 방법과 각 퍼지분할에 대해서 소속함수를 정의해 주는 부분이고 다른 부분은 "if-then" 형식의 언어적 형식으로 표현되는 규칙들의 저장소이다. 이러한 제어 규칙은 입출력 변수가 결정된 후, 제어시스템의 제어특성에 따라 제어규칙을 생성할 수 있다. 추론부는 퍼지제어기에서 언어적인 형태로 기술된 퍼지 제어규칙을 적용하기 위한 논리적인 실행 부분이다. 퍼지규칙으로부터의 논리적인 추론이 가능한 이유는 "if-then" 형식의 퍼지 제어규칙의 조건명제는 퍼지관계로 나타내어질 수 있으며 이로써 논리적인 추론이 가능하다. 비퍼지화부는 퍼지제어의 추론결과로 나타나는 판정을 위한 퍼지집합에서 명확한 결과 값을 만들어내는 부분이다[11].

Ⅲ. 퍼지제어 통합탐지

3.1 퍼지제어 통합탐지시스템

탐지시스템들의 탐지 값에 내포된 탐지시스템 간



〔그림 1〕 퍼지제어 통합탐지 시스템의 구성

의 관련성을 찾아내고 탐지시스템의 탐지 특성을 통합 시에 반영하기 위한 방법으로 퍼지제어를 사용하는 경우 퍼지적용을 위해 몇 가지 절차를 수행해야 되고 이러한 절차의 올바른 수행여부가 퍼지제어의 타당한 요건이 된다. 퍼지제어 통합탐지 시스템은 [그림 1]과 같이 퍼지제어를 위한 감사데이터를 생성하는 탐지시스템부와 퍼지제어를 적용시켜나가는 과정인 퍼지제어부로 나눌 수 있다. 탐지시스템부는 기존의 감사데이터를 생성하는 감사데이터 부분과 오용행위 및 비정상행위 탐지시스템 등으로 구성되어 있다. 오용행위 및 비정상행위 탐지시스템은 호스트 및 네트워크의 감사데이터를 기본 데이터로 사용한다. 그리고 탐지시스템이 생성한 모든 감사데이터가 퍼지화 과정에 들어가기 앞서 임시적으로 저장 관리되는 부분이다.

퍼지제어부는 퍼지제어를 적용시켜가는 과정으로 최종적으로는 퍼지추론과 비퍼지화 단계를 거쳐 탐지시스템 간의 탐지결과를 통합시킨 최종 탐지값을 생성한다. 퍼지제어부는 로그분석기, 퍼지화, 퍼지추론, 비퍼지화, 의사결정 그리고 규칙베이스로 구성된다. 로그분석기는 침입탐지시스템들이 생성한 감사데이터를 읽어서 퍼지추론이 대상이 될 수 있는 최소한의 조건을 만족하는 감사데이터 인지를 선별하는 부분이다. 이러한 작업을 수행하기 위해 감사데이터의 축약과정으로 실험을 통해 생성된 임계값 이하의 값을 갖거나 두 개 이상의 탐지시스템이 공격이 아닌 것으로 판정하는 경우에 해당 감사데이터를 무시하는 것이다. 예를 들면, 오용행위 탐지시스템의 경우 정확도가 높은 특성을 반영해 특정 임계값을 설정해 두고 임계값 이상의 결과가 나오는 경우 이를 퍼지제어부에 넘기지 않고 바로 공격으로 판정해 보고하는 것이다.

퍼지화는 각 탐지시스템으로 부터 비퍼지 값을 퍼지집합으로 변화하고 소속함수를 반영한 퍼지 출력을 수행한다. 퍼지추론은 현재의 입력값이 기존의 소속함수와 일치하지는 않지만 근사값을 구할 수 있도록 하며, 비퍼지화는 퍼지 값을 판단될 수 있는 비퍼지의 출력값으로 변환한다. 의사결정은 퍼지추론을 통해 생성된 최종 결과값을 보고 공격여부를 판정하는 부분이며, 공격판정은 실험을 통한 공격판정의 임계값을 설정해 적용하게 된다. 규칙베이스는 퍼지추론 시에 탐지시스템의 관련성을 반영하는 제어규칙을 담는 규칙 데이터베이스이다.

3.2 탐지결과의 퍼지화

3.2.1 퍼지 입출력 변수와 퍼지집합

퍼지의 개념을 사용하는 목적은 각 탐지시스템들이 출력 값에 내포하고 있는 시스템간의 관련성정도를 퍼지추론을 통해서 통합함으로써 하나의 값으로 표현하는 것이다. 따라서 고유의 탐지영역을 담당하는 각 시스템들을 하나의 퍼지제어 입력변수로 볼 수 있고 각 시스템들의 출력 값의 변화를 퍼지집합으로 정의할 수 있다. 즉, 4개의 탐지시스템이 설치된 경우 Sa, Sb, Sc, Sd를 입력변수로 두고 이들의 추론결과인 Sz를 출력변수로 갖게 된다. [그림 2]는 다중 탐지시스템의 퍼지집합의 예를 보인 것이다.

Sa = {*L, M, H*}	*Sa* : 오용행위 입력변수
Sb = {*L, ML, MZ, MH, H*}	*Sb* : 비정상행위 입력변수
Sc = {*L, ML, MZ, MH, H*}	*Sc* : 비정상행위 입력변수
Sd = {*L, ML, MZ, MH, H*}	*Sd* : 비정상행위 입력변수
Sz = {*L, ML, MZ, MH, H*}	*Sz* : 출력변수

〔그림 2〕 다중 탐지시스템의 퍼지집합

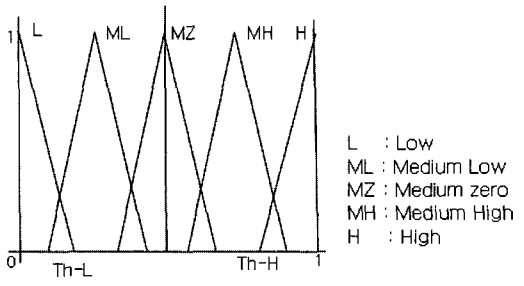
퍼지집합의 멤버는 공격에 대한 가능성을 나타내는데 L은 Low, ML은 Medium Low, MZ은 Medium Zero, MH는 Medium High 그리고 마지막으로 H는 High를 각각 의미한다. Medium은 실제 판정이 모호해지는 부분으로 ML, MZ, MH의 3개의 부분으로 세분화함으로써 실제 최종 출력 값을 내어놓는 퍼지추론시에 모호한 값에 대한 정확성 정도를 높이기 위해서이다. 오용행위 탐지시스템의 경우는 탐지시스템의 특성상 공격과 정상행위에 대한 판정 값이 정형적이기 때문에 퍼지집합을 가능한 단순화 시켜서 3개의 퍼지집합 멤버로 구성한다. 탐지특성에 따른 알고리즘이 적용된 비정상행위 탐지시스템 및 출력변수는 5개의 퍼지집합 멤버로 구성한다.

3.2.2 소속함수

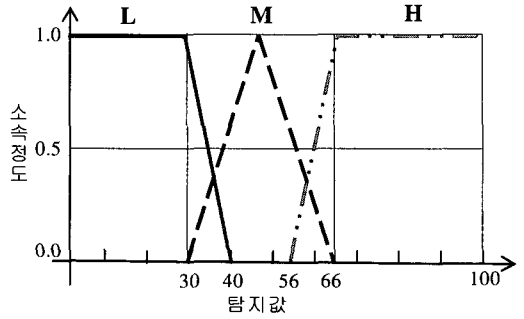
다중 탐지시스템의 입력변수 값은 대부분의 탐지시스템이 탐지의 정도를 [0..1]사이의 폐구간 사이의 값으로 표현하며 삼각숫자 개념의 도입이 가능하다. 즉, 입력변수의 전체집합을 퍼지분할 하고 각 분할에 대해서 적절한 퍼지 소속함수를 부여하는 것이다. 다중 탐지시스템에서 제어대상은 모호한 중간 값들에 대한 제어이므로 퍼지분할 시에 제어의 대상에 포함되지 않는 공격 또는 이상구간과 정상구간을 탐지정도의 상한값과 하한값 형태로 지정해 두고, 실제 탐지 대상인 모호한 범주는 세분화해서 탐지의 정확성을 높일 수 있다.

[그림 3(a)]는 공격범주, 정상범주, 모호한 범주의 퍼지분할에 의해 작성된 퍼지집합이 {L, ML, MZ, MH, H}인 소속함수를 보인다. 여기에서 각 시스템의 탐지특성은 각기 다를 수 있으므로 범주의 크기도 달라 질 수 있다. 정상 판정값인 Th-L(Threshold-Low)과 공격 판정값인 Th-H(Thres- hold-High)는 퍼지제어 시에는 포함되지 않지만 판정의 중요한 요소이다. 각 소속함수의 좌우 경계값은 탐지시스템의 신뢰도를 결정하므로 여러 번의 실험을 통해서 통계적 절차를 거친후 최적의 신뢰도를 적용하여 결정하게 된다. 소속함수의 좌우 경계를 설정하기 위해서 가장 먼저 수행해야 될 작업은 각 퍼지변수의 L과 H에서 소속함수에서의 임계값(Threshold)이라고 부를 수 있는 값을 선정하는 것이다. 이 논문에서의 상한 및 하한의 값을 정하기 위한 방법은 Trapezoidal의 체형적 분법을 이용하였다.

상한 임계값과 하한 임계값이 소속함수에서 갖는 의미는 상한 임계값 이상에서와 하한 임계값 이하의 값에서는 소속함수의 값이 언제나 1 이다. 즉, 하한 임계값 이하의 값은 정상행위이며, 상한 임계값 이상은 공격임을 의미한다. 또한 상한 임계값과 하한 임계값은 퍼지집합의 L과 H의 소속함수에서 소속정도가 1에서 점차 줄어드는 변곡지점이 된다. 판정이 모호한 영역의 세부 영역에 대해서 별도의 가중치를 부여하지 않도록 상한 임계값과 하한 임계값 사이를 3등분하여 ML, MZ, MH에 분할하는 방식을 사용한다. [그림 3(b)]는 오용행위 탐지시스템의 퍼지 소속함수의 예를 보인 것이다. 출력변수에 대한 소속함수



(a) 퍼지 소속함수



(b) 탐지시스템의 퍼지소속함수

〔그림 3〕 탐지시스템의 퍼지 소속함수의 예

를 적용한 퍼지집합의 상한 임계값과 하한 임계값의 작성은 입력변수 퍼지집합에서 상한 및 하한 임계값의 평균을 출력변수 퍼지집합의 상한 및 하한 임계값으로 사용하고 나머지 퍼지집합의 멤버인 ML, MZ 그리고 MH에 대해서는 입력변수에서 사용한 방식을 동일하게 사용하여 작성할 수 있다.

3.3 퍼지제어 규칙

지금까지 연구되어온 퍼지제어 규칙의 규칙유도방법은 전문가들의 경험 및 숙련된 조작을 바탕으로 규칙을 만드는 전문적 지식에 의한 학습방법, 상태변화의 자료로부터 인공 지능의 탐색을 이용하여 원하는 목표점으로 상태를 천이시키는 규칙을 찾아내는 인공지능 학습방법, 역전파 알고리즘등을 적용하여 신경망의 가중치를 학습하고 규칙을 나타내는 소속함수의 파라미터를 찾아내는 신경망에 의한 학습방법, 유전자로 규칙을 모델링하여 교차 및 돌연변이에 의해 변환하여 여러 세대에서 최적의 규칙을 이루는 조합을 구하는 유전 알고리즘에 의한 학습방법이 있다. 이러한 방법 중에서 오차에 대한 분석이 임의적인 단점을 가지지만 간단하고 편리한 전문적 지식에 의한 퍼지제어 규칙을 적용한다.

〔표 1〕 통합탐지를 위한 퍼지추론의 일반원칙

일반규칙	내용
공격 판정	- 오용행위 탐지시스템의 상한 임계값(H) 이상은 공격 - 비정상행위 탐지시스템 2개 이상이 상한 임계값(H)을 나타내는 경우는 공격
추론 판정	- 오용행위 탐지시스템의 M값 이하는 퍼지 추론의 대상 - 비정상행위 탐지시스템의 경우 각 적용 방법에 따른 탐지시스템에 따라 MH 또는 MZ 이상의 값이 추론의 대상
정상 판정	- 탐지시스템 2개 이상이 ML 값 이하를 나타내는 경우 정상행위 - 공격판정과 추론판정의 경우를 제외한 모든 경우는 정상행위

퍼지제어 규칙의 유도과정은 퍼지 제어규칙이 탐지시스템의 탐지특징을 반영하고 있어야 한다. 즉, 설정의 변경이나 탐지시스템의 탐지 알고리즘 수정을 통한 성능향상을 고려하더라도 더 이상 탐지시스템이 탐지의 성능을 향상시킬 수 없는 수준에서 탐지시스템의 탐지특징을 확인하고 이를 제어규칙의 작성 시에 적용해야 한다. 이러한 탐지시스템의 퍼지제어 규칙을 생성하기 위해서 다음과 같은 탐지시스템에 대한 일반적인 원칙을 적용함으로써 탐지시에 성능에 영향을 미치는 퍼지추론을 위한 제어규칙의 수를 줄일 수 있다. 적용된 탐지시스템에 대한 퍼지추론의 일반적인 원칙은 [표 1]과 같다.

일반적인 원칙에 따른 제어규칙은 다음 단계인 퍼지추론 시에 통합된 결과를 추출하기 위한 규칙으로 사용되며 탐지시스템이 오용행위 탐지시스템 Sa, 비정상행위 탐지시스템 Sb, Sc, Sd로 구성된 경우 다음과 같은 형식의 규칙들을 만들게 된다.

IF (Sa is M) and (Sb is L) and (Sc is MH) and (Sd is H) Then Z is MH
IF (Sa is M) and (Sb is H) and (Sc is MH) and (Sd is MH) Then Z is MH
IF (Sa is M) and (Sb is L) and (Sc is MZ) and (Sd is MZ) Then Z is MZ
IF (Sa is M) and (Sb is MZ) and (Sc is MZ) and (Sd is MZ) Then Z is MZ
IF (Sa is L) and (Sb is MH) and (Sc is L) and (Sd is MH) Then Z is MH
IF (Sa is L) and (Sb is L) and (Sc is MH) and (Sd is MZ) Then Z is MZ
. . .

다중 탐지시스템의 최종결과는 탐지시스템이 나타

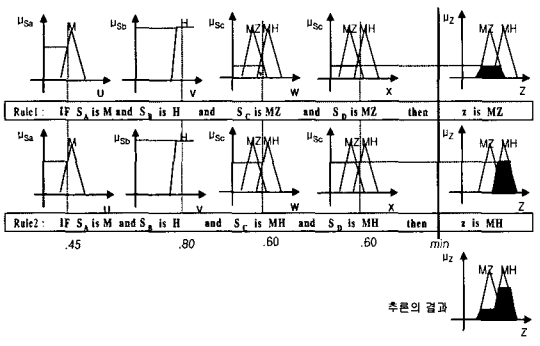
내는 결과가 소속함수의 개수가 아닌 추론의 과정을 통한 결과에 의존함을 보이며, 퍼지 제어규칙의 개수는 입력변수의 개수와 퍼지집합의 개수에 따라서 결정되지만 경험상 제외되는 규칙이 존재해 모든 경우수의 규칙이 필요한 것은 아니다.

3.4 퍼지추론과 비퍼지화

퍼지추론을 위한 추론규칙이 정해지면 퍼지추론의 과정을 거친다. 퍼지추론은 탐지시스템의 특성이 반영된 소속함수들로부터 현재의 입력값이 기존의 소속함수와 완전히 일치하지는 않지만 퍼지추론을 통해서 근사적인 값을 구할 수 있도록 해 준다. 퍼지추론이 시작되기 전에 먼저 추론없이 직접적인 판정이 가능한지 확인하고 판정이 모호한 경우에 대해서 추론의 과정을 거치게 된다. 퍼지추론은 퍼지제어 추론규칙을 기반으로 이루어지고 추론 후에는 비퍼지화를 거쳐 판정이 용이한 형태로 변환한다. 변환된 최종 추론값은 공격에 판정여부에 대한 임계값과의 비교를 통해서 그 결과를 보고하게 된다.

퍼지추론은 퍼지논리를 바탕으로 추리를 전개해나가는 방식이며, 이 논문에서는 직접법의 한 형태인 Mamdani의 Max-Min 추론방식을 사용한다. 그림 4는 Mamdani의 Max-Min 추론방식을 사용한 실제 추론의 예이다. [그림 4]에서 탐지시스템 Sa는 45, Sb는 80, Sc는 60 그리고 Sd는 60의 탐지결과를 보이는 경우 두 개의 규칙에 의해 각각 우측의 결과를 보인다. 입력변수에 대한 각 소속함수의 값은 영역 내에서의 직선의 방정식에 의해서 쉽게 구할 수 있다. 예를 들어 S_A의 경우 45의 입력값에 대해서 아래의 직선의 방정식을 통해서 계산이 가능하다.

$$\mu_{SA} = 1/18x - 5/3 \quad (30 \le x \le 48)$$

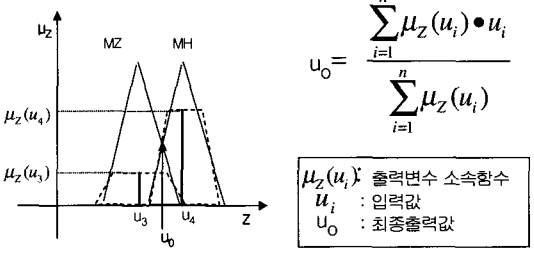


〔그림 4〕 Mamdani의 방법을 이용한 추론의 과정

따라서 45의 입력값은 주어진 구간 내의 직선의 방정식을 이용해 0.83정도의 값을 계산해 낼 수 있다. x의 구간값은 탐지센서 A의 학습에 의한 하한 및 상한 임계값인 30과 66 사이의 모호한 중간(M : medium) 값에 삼각함수를 적용했을 때 소속함수가 0과 1이 되는 30과 48이다.

퍼지추론을 끝내고 난 최종결과는 그림 4의 추론의 결과처럼 관리자가 직관적으로 판단할 수 있는 형태가 아니다. 따라서 관리자가 쉽게 판정할 수 있도록 해주는 비퍼지화 과정을 거치게 된다. 이 논문에서는 비퍼지화 방법으로는 무게중심법을 이용하여 비퍼지화 단계를 수행한다.

[그림 5]의 비퍼지화는 그림 4에서 최종 추론단계를 마친 결과를 대상으로 수행되는데 출력변수에 대한 소속함수에서의 값($\mu_z(\mu_i)$)와 입력값(μ_i)를 곱한 값을 출력변수에 대한 소속함수의 값으로 나누어준 값이 최종적인 출력변수가 된다. 여기서 n은 출력변수 퍼지집합의 멤버의 개수이다.



〔그림 5〕 추론결과의 비퍼지화 단계

Ⅳ. 실험 및 분석

4.1 실험 환경

본 논문에서의 실험은 퍼지제어를 이용한 통합탐지를 위하여 SunOS 솔라리스 5.8에서 BSM 감사데이터를 이용하여 호스트기반의 침입탐지시스템에 의해 수행되었다. 호스트 기반의 침입탐지 시스템은 오용행위 탐지시스템(Sa)와 HMM을 이용한 시스템호출(Sb), 파일접근(Sc) 그리고 파일접근 및 시스템호출(Sd) 이상행위 탐지시스템으로 구성하였다.

호스트에서 사용되는 감사데이터의 생성을 위해서 정상행위 생성 프로그램과 공격행위 생성 프로그램을 사용하였으며, 공격행위 생성 프로그램은 크게 4개 타입 총 9개의 공격으로 구성하였다. 정상행위의

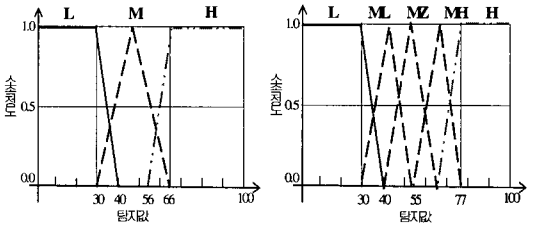
경우는 일반 사용자들이 사용하는 명령어들의 리스트가 포함된 각 사용자의 홈 디렉토리의 히스토리 파일을 읽어 사용빈도가 높은 명령어를 선정하였으며, [표 2]는 실험에 사용된 공격의 형태와 종류, 정상행위 명령어들을 보인 것이다.

〔표 2〕 정상행위와 공격행위

사용행위	내 용
정상행위	ls, pwd, cd, clear, date, df, touch, cal, du, id, ps, who, more, rm
인증공격	su, login
자원공격	fork, mkdir, malloc
권한공격	/etc/passwd deletion
오용공격	buffer overflow, heap overflow, race condition

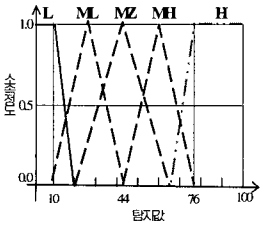
4.2 퍼지제어 통합탐지 성능 및 비교

퍼지제어 통합탐지의 성능을 분석하기 위해서 ROC (Receiver Operating Characteristic) 곡선을 사용한다. ROC 곡선은 X-축으로 미탐율(False Negative)을 Y-축으로 오탐율(False Positive)을 표시함으로써 각 탐지시스템과 통합탐지의 성능을 나타낼 수 있다. 탐지시스템의 성능이 향상될수록 탐지의 영역은 미탐율과 오탐율이 줄어드는 원점에 가까워지게 된다. 일반적인 탐지시스템에서 오용행위 탐지시스템은 미탐율이 높게 나타나며, 비정상행위 시스템의 경우 오탐율이 높게 나타나게 된다. 통합탐지의 수행후 나타난 탐지결과가 ROC 좌표축의 원점으로 접근한다면 탐지성능을 향상시키는 것으로 볼 수 있다.

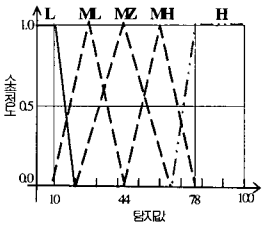


(a) 오용행위 소속함수

(b) 시스템호출 비정상행위 소속함수



(c) File Access 비정상행위 소속함수



(d) 시스템호출-파일접근 비정상행위 소속함수

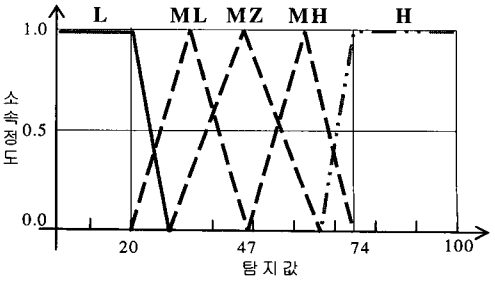
〔그림 6〕 입력변수에 대한 퍼지 소속함수

본 논문에서는 오용행위 탐지시스템 1개와 비정상행위 탐지시스템 3개를 호스트 기반의 탐지시스템으로 사용하여 4개의 퍼지 입력변수와 출력 퍼지변수 1개를 포함한 5개의 퍼지변수를 사용한다. 그리고 각각의 퍼지변수에 대해서 오용행위 탐지시스템(Sa)는 {L, M, H} 그리고 비정상행위 탐지시스템의 입력변수(Sb, Sc, Sd) 및 출력변수(Sz)는 {L, ML, MZ, MH, H}로 퍼지멤버를 구성하여 5개의 퍼지집합으로 구성하였다.

또한 각 탐지시스템의 탐지 특성에 따른 상한 및 하한의 임계값과 소속함수의 값은 탐지시스템 수준에서 수 차례의 실험에 따른 통계적 절차를 수행한 후 결정하였다. [그림 6]은 실험에 사용되어진 각 탐지시스템의 상한 및 하한 임계값과 소속함수의 정도를 보인 것이다.

출력변수에 대한 퍼지집합은 4개의 입력변수 퍼지집합을 기준으로 작성되었다. 먼저 출력변수 퍼지집합의 상한 임계값과 하한 임계값의 작성은 입력변수 퍼지집합에서 상한 임계값과 하한 임계값의 평균을 출력변수 퍼지집합의 상한 임계값과 하한 임계값으로 사용하였고 나머지 퍼지집합의 멤버인 ML, MZ 그리고 MH에 대해서는 입력변수에서 사용한 방식을 동일하게 사용하였다. [그림 7]은 최종적으로 생성된 출력변수의 퍼지집합이다.

퍼지제어 규칙은 오용행위 퍼지멤버 3, 비정상행위 퍼지멤버 5로 구성되어 최대 생성개수인 375(3*53)개이며, 이 논문에서는 113 개로 퍼지추론을 위한 제어규칙의 수를 줄일 수 있었다. 퍼지 추론규칙의 숫자는 탐지성능을 좌우하는 요소이므로 탐지규칙의 수는 최소화할 필요가 있다.



〔그림 7〕 출력변수의 퍼지집합

〔표 3〕 퍼지 통합 전/후 탐지시스템의 성능

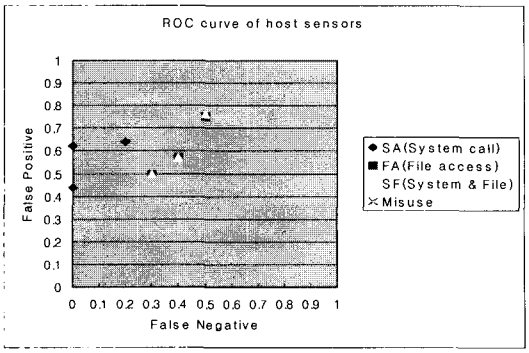
횟수	탐지율	통합전				통합후			
		Sa	Sb	Sc	Sd	Sa	Sb	Sc	Sd
1	FP	0.25	0.62	0.75	0.76	0.2	0.4	0.55	0.5
	FN	0.55	0	0.5	0.5	0.44	0.1	0.4	0.4
2	FP	0.4	0.64	0.57	0.57	0.4	0.45	0.4	0.4
	FN	0.6	0.2	0.4	0.4	0.5	0.2	0.3	0.3
3	FP	0.4	0.44	0.5	0.5	0.35	0.3	0.4	0.5
	FN	0.6	0	0.3	0.3	0.45	0.1	0.2	0.3

* FP: False Positive, FN : False Negative

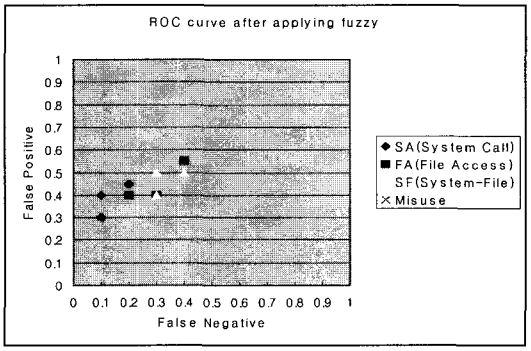
퍼지추론 및 비퍼지화의 작업을 수행한 후의 오탐율 및 미탐율의 결과는 [표 3]에서 보였다. [표 3]의 결과를 보면 오용탐지시스템의 오탐율은 아주 적게 줄어드는 반면 미탐율은 약 10-15% 이상의 성능향상이 이루어졌음을 알 수 있다. 이는 실제 오용탐지시스템이 공격을 탐지하지 못하더라도 비정상행위 탐지시스템과의 퍼지추론을 통해서 공격을 탐지해낼 수 있음을 의미한다. 비정상행위 탐지시스템의 경우 오탐율은 약 20% 미탐율은 약 10% 정도 낮아지는 성능향상이 있었다. 퍼지추론을 이용한 통합탐지의 경우 비정상행위 탐지시스템이 오용탐지시스템보다 더 높은 탐지성능을 나타내는 이유는 퍼지추론이 서로 밀접한 관련성이 있는 비정상행위 탐지시스템간의 관련성을 더 효과적으로 다루기 때문임을 보이고 있다.

[그림 8]의 (a), (b)는 표 3의 결과를 ROC 곡선으로 표현한 것이며, 통합탐지의 결과는 분포형태가 원점의 방향으로 이동되어졌음을 확인할 수 있다. 이것은 다중의 탐지시스템들의 결과로부터 탐지영역 간의 관련성 도출을 위해 퍼지제어를 이용하는 통합탐지 방법이 의미 있음을 설명하고 있다. 또한 퍼지제어 파라미터들의 최적화를 통해서 그 성능을 향상시킬 수 있음을 고려할 때 퍼지제어 통합탐지 시스템의 가능성이 있음을 보여주고 있다.

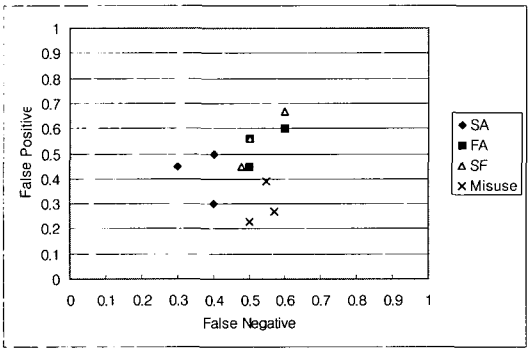
또한, [그림 8(b)]의 결과는 기존의 연구인 (c)의 조건부 확률론적 통합탐지[9]의 결과와 비교하였을 때 탐지값의 특성으로부터 비정상행위의 미탐율 및 오탐율의 탐지결과를 개선하였음을 비교할 수 있다. 이의 결과는 각각 다른 탐지영역의 결과에 대한 조건부 확률적인 통계의 방법에 의해 하나의 탐지시스템의 결과가 다른 탐지시스템의 결과에 영향을 주는 정도를 판단하는 지지율을 이용하는 방법과 비교하여 탐지결과의 퍼지제어를 이용한 통합탐지의 방법



(a) 퍼지 통합 전



(b) 퍼지 통합 후



(c) 조건부 확률적 통합탐지의 결과

〔그림 8〕 퍼지제어 통합전후의 ROC 곡선

이 성능상의 개선을 하였음을 보인다.

V. 결 론

본 논문에서는 각 탐지영역에 따른 탐지시스템의 탐지한계를 극복하기 위한 방법으로 탐지시스템의 결과들 간의 관련성을 퍼지제어를 이용하여 통합탐지 하는 방법에 대해서 연구하였다. 퍼지제어 통합탐지 시스템은 각 탐지시스템의 결과를 분석하는 로그

분석기, 그리고 퍼지화 과정을 수행하는 퍼지제어부 그리고 퍼지제어를 적용하는 과정에서 필요한 제어 규칙과 각 탐지시스템의 소속함수로 구성된다. 탐지 시스템의 탐지 결과는 정확한 탐지영역의 결과, 오탐지 영역에 대한 결과 그리고 미탐지 영역에 대한 결과가 중첩되거나 누락 및 추가된 형태로 볼 수 있다. 통합탐지를 위해서 각 탐지시스템에 대한 퍼지집합의 멤버를 정의하였으며, 탐지특성에 따른 퍼지 소속함수를 작성하였고 각 탐지시스템 간의 상호 관련성의 정도를 반영하기 위한 제어규칙을 생성하였다.

통합탐지를 위해 퍼지추론의 단계에서 퍼지추론이 필요없는 탐지시스템으로 부터의 결과에 대한 축약을 수행하였으며, 모호한 탐지값에 대한 퍼지규칙을 적용함으로써 잘못된 보고의 숫자를 최소화하였다. 즉, 통합을 하지 않는 경우에 각 개별 탐지시스템들이 발생시키는 수많은 잘못된 보고를 퍼지추론의 과정을 통해 최소화 시켰다. 이러한 결과는 조건부 확률적인 통계적 방법에 비해 탐지결과의 성능에 향상이 있음을 보였고 퍼지제어 규칙의 갱신으로서 탐지시스템 사이의 지지율 테이블을 갱신하는 데에 실시간의 탐지방법을 적용할 수 있음을 보였다.

제안한 퍼지제어 통합탐지 시스템은 기존의 통합탐지 시스템들의 관련성 추출방법과는 달리 다양하게 운용중인 이종의 침입탐지시스템의 탐지값 자체에 포함된 탐지 영역간의 관련성을 이용하여 통합탐지하였다. 제어규칙의 생성이나 퍼지추론을 위한 파라미터의 결정 시에 전문가의 직관에 의한 방법에 많이 의존하고 있으나 향후 연구에서는 자동적인 제어규칙의 생성이나 추가/삭제 그리고 좀 더 과학적인 파라미터의 결정방법에 대한 연구가 필요하다.

참 고 문 헌

[1] F. Cuppens, and A. Miège, "Alert Correlation in a Cooperative Intrusion Detection Framework," *IEEE Symposium on Security and Privacy*, May 2002.

[2] F. Cuppens and R. Ortalo, "LAMBDA : A Language to Model a Database for detection of Attacks," *Proc. of the 3rd International Workshop on the Recent Advances in Intrusion Detection(RAID '2000)*, Toulouse, France, Oct. 2000.

[3] C. Christian, D. Mark *etal.* "Towards a Taxonomy of Intrusion Detection Systems and Attacks," *Research Report RZ 3366, IBM Research, Zurich Research Lab.*, Sept. 2001.

[4] P. A. Porras and P. G. Neumann, "EMERALD: Event Monitoring Enabling Responses To Anomalous Live Disturbances," *Proc. of the 20th National Information Systems Security Conference*, pp. 1~13, 1997.

[5] A. Valdes and K. Skinner, "An Approach to Sensor Correlation," *3rd International Workshop on the Recent Advances in Intrusion Detection*, Oct. 2000.

[6] A. Valdes and K. Skinner, "Probabilistic Alert Correlation," *4th International Symposium on the Recent Advances in Intrusion Detection*, pp.54~68, Oct. 2001.

[7] J. Gomez and D. Dasgupta, "Evolving Fuzzy Classifiers for Intrusion Detection," *Proc. of IEEE Workshop on Information Assurance*, 2002.

[8] M. Manic and B. Wilamowski, "Fuzzy Preference Approach for Computer Network Attack Detection," *International Joint Conference on Neural Networks (IJCNN'01)*, pp.1345~1349, July, 2001.

[9] 김용민, 김민수, 김홍근, 노봉남, "이종의 침입탐지센서 관련성을 이용한 통합탐지의 민감도 향상 기법," 정보보호학회논문지, 12(4), pp.29~40, 2002.

[10] 김상찬, 김용민, 김민수, 노봉남 "퍼지제어를 이용한 다중 탐지시스템의 통합탐지 방법," 정보과학회 가을 학술발표논문집(I), 29(2), pp.532~534. 2002.

[11] 이광형, 오길록, "*퍼지이론 및 응용 - 1,2권*," 홍릉과학출판사, 서울, 1991.

〈著者紹介〉

김 용 민 (Yong-Min Kim) 정회원

1989년 : 전남대학교 전산통계학과 졸업
1991년 : 전남대학교 전산통계학과(이학석사)
2002년 : 전남대학교 전산통계학과(이학박사)
2003년 6월~현재 : 전남대학교 리눅스시스템 보안연구센터 Post-doc.
<관심분야> 시스템 및 네트워크 보안, 정보보안, 퍼지 이론, 네트워크 관리 등