
퍼지기법을 이용한 침입 탐지 시스템 오류경고메시지 축소 모델 설계

성 경
목원대학교 컴퓨터교육과

Design of False Alerts Reducing Model Using Fuzzy Technique for Intrusion Detection System

Kyung Sung
Dept. of Computer Education, Mokwon University
E-mail : skyys04@mokwon.ac.kr

요 약

정보기술이 발달함에 따라 보안 사고가 증가되면서 시스템에 대한 침입을 방어하기 위한 여러 도구들이 개발되어왔다. 시스템에 대한 불법침입을 탐지하는 침입탐지시스템은 과도한 오류경고메시지 발생으로 인하여 침입 판단의 어려움이 따르고 있다. 본 연구는 오류경고메시지의 축소를 위한 방법으로 네트워크 내부에서 발생하는 긍정오류 탐지를 축소하고, 판단자의 불확실성을 감소시키기 위하여 퍼지기법을 적용한 긍정오류 경고메시지를 축소시킬 수 있는 모델을 설계하여 탐지의 정확성 향상에 활용할 수 있을 것이다.

ABSTRACT

As the development of information technology and thus the growth of security incidents, so implement are coming out for defense the intrusion about the system. However the error detection program has got a difficulty to find out the intrusions because that has become so many false alert messages. In this study is how to reduce the messages for the false alerts which come from the internal of the network and using the Fuzzy techniques for reduce the uncertainty of the judge. Therefore it makes the model which can decrease false alert message for better detection.

키워드

퍼지기법, 네트워크 보안, 침입탐지, 보안 취약성

1. 서 론

네트워크 및 인터넷의 급속한 확산은 순기능과 역기능으로 개인정보 누설, 정보시스템의 비

인가 사용, 전산 자원에 대한 해킹, 중요한 정보의 파괴와 변조 같은 다양한 보안위협에 노출되고 각종 보안 사고가 확산되고 있다.[1] 특히 국내외적으로 정보시스템 및 전산망의 해킹은 다

양한 형태로 나타나고 있으며 고도의 침해 기술을 이용한 주요 정보 유출 및 파괴로 인한 피해 정도가 심각하여 빠르고 정확한 침입차단 및 침입탐지가 요구되고 있다.

침해사고를 예방하고 효과적인 대응방법을 마련하기 위해 침입차단기술, 침입탐지기술 등 여러 가지 정보보호기술들이 개발되고 있다. 이러한 기술 중 네트워크 기반 침입탐지시스템의 대표적인 한계점은[2] 경고메시지 Flooding에 의한 서비스거부 공격, 하나의 공격에 다수의 중복 메시지 발생, 긍정오류(False Positive)로 인한 경고 메시지의 과다 발생 등이 있다. 현재 침입탐지시스템에서의 경고메시지 축소에 관한 연구동향[8]은 서버의 취약성을 이용한 미리 정의된 상황별 평가, 경고메시지 전후 연관관계를 이용한 유사성 평가 방법 등으로 이루어지고 있다. 본 연구에서는 경고메시지의 과다 발생을 해결하기 위하여, 인증된 인트라넷에서의 각 서버별 취약성에 대한 서버 관리자, 인트라넷 보안 관리자, 정보보안 전문가등 판단자들의 취약성에 대한 오답 확률수치를 퍼지기법을 이용하여 취합하고 판단자의 주관적 해석에 의한 불확실성을 제거한 필터링률을 생성 적용하여 각 서버의 취약성에 의해 발생하는 긍정오류 경고메시지를 축소시키고자 한다. 본 연구는 네트워크 기반 침입탐지시스템에서의 서비스거부 공격, 하나의 공격에 다수의 중복 메시지 발생, 긍정오류(False Positive)로 인한 경고메시지의 과다 발생의 문제점과 연구 동향을 제시한 서론에 이어 2장에서는 기존 침입 탐지 시스템의 분석과 퍼지기법의 적용에 대해 알아보고, 3장에서는 경고메시지 축소를 위한 모델의 설계하고 4장에서는 실험결과, 5장에서는 결론을 맺는다.

II. 관련 연구

침입탐지시스템으로 방화벽과 함께 활용되는 네트워크 보안 솔루션을 말한다. 일반적인 침입탐지시스템은 방화벽과 같이 단순히 네트워크를 통한 외부 침입을 차단하는 단계를 넘어 외부 침입에 의해 방화벽이 해킹된 수 침입사실을 탐지해 이에 대해 대응하기 위한 솔루션이다. 이에 반해 IDS는 각종 해킹수법을 이미 자체적으로 내장, 침입행동을 실시간으로 감지, 제어할 수 있는 기능을 제공한다. 침입탐지시스템에 대한 데닝(Denning)[8]은 컴퓨터 시스템 또는 네트워크 상에서 의심스러운 행위를 감시하며, 허가되지 않은 사용자가 불법으로 접속하여 정보를 조작, 오용 및 남용 등의 불법 행위들을 조기에 발견하고 이에 대한 대응을 실시간에 처리할 목적으로 하는 시스템으로 정의 하였다.

COAST[7]에 의한 침입탐지시스템 분류는 원

시 데이터의 근원지에 따라 호스트 기반 방식과 네트워크 기반 방식 시스템으로 구분된다.

2.1 침입탐지시스템 비교 및 한계

◆ 침입탐지시스템 장단점 비교

구분	장점	단점	비고
호스트 기반	-정확한 탐지 -암호화/스위칭 환경에 적합 -하드웨어추가 불필요	-다수 운영체제 지원 필요 -추가적인 시스템 부하 -긍정오류 많음	상용침입탐지시스템 중
네트워크 기반	-트래픽 감시 위치에 설치 -운영체제에 독립적 -구현 및 관리 용이 -긍정오류 적음	-암호화/스위칭 환경에 적합 -기가급 고속 네트워크에서 패킷 손실 발생	60%가 네트워크 방식 사용

표1. 침입탐지시스템 장단점

◆ 침입탐지시스템 한계

- ① 알려진 공격만 탐지 : 네트워크 침입탐지시스템의 가장 심각한 문제는 알려진 공격 이외의 경우에는 속수무책이라는 점이다. 새로운 공격 유형에 대한 공격 패턴이 식별되고 규칙집합 데이터베이스에 추가되어야 공격에 대한 탐지 및 대응이 가능하다.
- ② 관리 오버헤드 : 가장 큰 문제는 침입탐지시스템에서 발생하는 긍정오류(False-Positive)의 수이다. 어떤 전산망에서는 몇 사람이 하루 종일 투입하여 보고된 데이터를 분석하기도 한다. 이러한 상황은 나아지고 있기는 하지만 가까운 미래에도 여전히 문제가 남아 있을 듯 하다.
- ③ 침입탐지시스템 우회가능성 : 네트워크 침입탐지시스템은 진행 중인 잠재적인 공격에 대한 수많은 데이터를 저장해야 한다. 특히, 네트워크 침입탐지시스템의 내부 저장장치 용량을 초과하는 경우가 발생하면, 저장이 가능한 상태로 복구되는 순간까지는 공격이 얼마든지 가능하다.

2.2 퍼지기법의 개념 및 적용방안

◆ 퍼지기법의 적용방안

퍼지이론은 1965년 미국 버클리 대학의 Lofti, A. Zadeh[12]에 의해 처음 소개되었으며 일본 및 유럽에서 활발하게 연구되고 응용하고 있는 학문이다. 퍼지집합으로 나타난 불확실성의 정도를 퍼지정도(fuzziness)라고 하고, 이 퍼지정도를 측정하는 함수를 퍼지정도 척도(measure of fuzziness)라고 한다.

퍼지정도 척도를 나타내는 함수 f 는 다음과 같이 표현된다.[8]

$$f: P(x) \rightarrow R$$

이 때, $P(x)$ 는 전체집합 X 의 모든 부분집합을 모은 멱집합(power set)이다.

퍼지정도 척도가 가져야할 세 개의 공리는 다음과 같다.

공리1 :

$f(A) = 0$ if $f(A)$ 가 보통집합(crispset)이다

공리2 : 단조성(monotonicity)

$A < B$ 이면 $f(A) \leq f(B)$

두 개의 퍼지집합 A, B에서 A가 B보다 불확실성이 적다면, $f(A)$ 가 $f(B)$ 보다 작아야 한다.

공리3 : 퍼지정도(불확실한 정도)가 최대이면, 퍼지정도 척도 $f(A)$ 가 최대가 되어야 한다.

이상의 공리를 바탕으로 퍼지집합 A의 퍼지정도를 측정할 수 있는 척도 $f(A)$ 를 정의해 보면 다음과 같다.

$$f(A) = - \sum (\mu_A(X) \log_2 \mu_A(X) + [1 - \mu_A(X)] \log_2 [1 - \mu_A(X)])$$

이 척도 $f(A)$ 값을 다음과 같이 정규화(normalize)하여 $F(A)$ 를 얻을 수 있다.

$$F(A) = \frac{f(A)}{|X|}, \quad |X|: \text{cardinality}$$

정규화된 척도는 다음과 같은 관계를 갖는다.

$$0 \leq F(A) \leq 1$$

이 척도는 퍼지정도 척도의 공리 1과 공리 2를 만족한다[5].

본 연구에서는 이러한 퍼지정도의 척도를 적용하여 불확실한 판단자의 주관성을 줄이고자 시도하였다. 전체집합 X를 각각의 자산에 대한 가중치 또는 프로세스에 대한 가중치의 집합으로 보고, 사용자가 부여한 가중치를 집합 X 내의 퍼지집합 A로 보기로 한다. 그러면, 부여가능한 가중치의 집합 X에 대해, 자산에 대한 가중치집합 A는 집합 X의 멱집합이 되고, 집합 A의 원소들을 살펴보면, 0.1 ~ 0.9까지의 값들을 갖는다. 이 값들은 절대적인 값이 아닌, 사용자의 주관에 의해 판단된 값이므로 퍼지집합이고, 일반적으로 조직에 속한 어떠한 자산 또는 프로세스는 그것의 중요도가 아주 큰 경우와 아주 작은 경우는 직관적으로 판단할 수 있다. 따라서 0.1이나 0.9의 경우에는 불확실성이 0.3, 0.5, 0.7의 경우에 비해 상대적으로 적다고 볼 수 있다. 따라서 이 집합은 퍼지정도 척도의 공리2를 만족한다. 공리 1에 대해 만약 집합 A를 보통집합으로 본다면, 집합 A의 원소들은 두 가지의 상태로 나타낼 수 있다. 즉, 중요하다(1)와 중요하지 않다(0)로 구분할 수 있는데, 이 경우 퍼지정도 척도를 도출해 보면 0이 된다. 또한 공리 3에 대해, 집합 A에서 가중치가 0.5인 경우 퍼지정도가 최대라 말할 수 있고, 가중치가 0.1 또는 0.9인 경우 퍼지정도가 최소라고 말할 수 있다. 이 두 경우에 $f(A)$ 를 계산해 보면, 0.5인 경우 1이 도출되고, 0.1 또는 0.9인 경우 0에 가까운 값이 도출된다. 따라서 공리 3도 만족한다. 결과적으로, 집합 A에 대한 퍼지정도 척도는 퍼지정도 척도가 가져야할 세 개의 공리를 만족하므로 이러한 이론을 수준측정 시에 수준측정 결과의 정확성을

보다 더 높이기 위해 사용할 수 있다.

◆ 퍼지기법의 적용방안

본 연구에서는 이러한 퍼지정도의 척도를 적용하여 불확실한 판단자의 주관성을 줄이고자 시도하였다. 전체집합을 서버내의 각 자원에 대한 취약성에 대한 판단자의 오탐 판단값으로 보고, 판단자가 판단한 값을 집합 A로 보고, 부여가능한 가중치의 집합 X에 대해, 자산에 대한 가중치집합 A는 집합 X의 멱집합이 되고, 집합 A의 원소들을 살펴보면, 0.1 ~ 0.9까지의 값들을 갖는다[표2].

수 치	오탐 발생 확률
0.1	오탐 이 10% 정도 발생
0.3	오탐 이 30% 정도 발생
0.5	오탐 이 50% 정도 발생
0.7	오탐 이 70% 정도 발생
0.9	오탐 이 90% 정도 발생

표2. 오탐 발생 확률 수치표

이 값들은 절대적인 값이 아닌, 사용자의 주관에 의해 판단된 값이므로 퍼지집합이고, 일반적으로 조직에 속한 어떠한 자산 또는 프로세스는 그것의 중요도가 아주 큰 경우와 아주 작은 경우는 직관적으로 판단할 수 있다. 따라서 0.1이나 0.9의 경우에는 불확실성이 0.3, 0.5, 0.7의 경우에 비해 상대적으로 적다고 볼 수 있다. 따라서 이 집합은 퍼지정도 척도의 공리2를 만족한다. 공리 1에 대해 만약 집합 A를 보통집합으로 본다면, 집합 A의 원소들은 두 가지의 상태로 나타낼 수 있다. 즉, 오탐이다(1)와 오탐이 아니다(0)로 구분할 수 있는데, 이 경우 퍼지정도 척도를 도출해 보면 0이 된다. 또한 공리 3에 대해, 집합 A에서 가중치가 0.5인 경우 퍼지정도가 최대라 말할 수 있고, 가중치가 0.1 또는 0.9인 경우 퍼지정도가 최소라고 말할 수 있다. 이 두 경우에 $f(A)$ 를 계산해 보면, 0.5인 경우 1이 도출되고, 0.1 또는 0.9인 경우 0에 가까운 값이 도출된다. 따라서 공리 3도 만족한다. 결과적으로, 집합 A에 대한 퍼지정도 척도는 퍼지정도 척도가 가져야할 세 개의 공리를 만족하므로 이러한 이론으로 판단자의 주관적 해석에 의한 불확실성을 줄일 수 있다고 할 수 있다.

III. 긍정오류 축소 모델 설계

방화벽과 가상사설망을 이용 인증된 인터넷 망의 각 서버들에 대한 취약성을 분석 필터링을 생성하는데 보안 관리자 한사람의 주관적 해석에 의한 필터링 생성 및 적용은 서버 관리자나 정보보호 전문가들 다수의 의견이 배제되었기 때문에 오탐에 대한 불확실성이 높다. 이를 해결하기 위한 방법으로 각 서버들의 취약성 분석을 서버 관리자, 보안 관리자, 정보보호 전문

가 등 다수의 판단자의 취약성에 대한 의견을 취합 퍼지정도의 척도를 적용하여 판단자의 불확실성을 감소시킨 필터링룰을 생성 및 적용 할 수 있다.

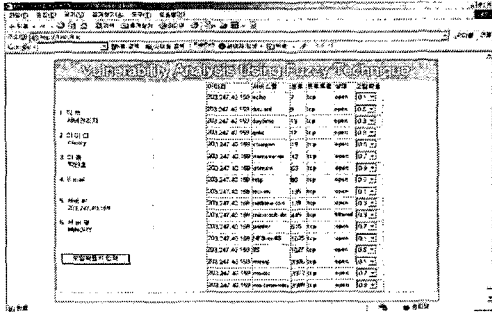


그림1. 오염확률 수치 입력을 위한 취약성 분석틀

퍼지정도를 도출하기 위해 각 판단자들은 [표 2]를 기준으로 [그림1]의 틀을 이용 서버의 취약성에 대해 오염 발생 확률수치를 입력한다.

입력된 판단자들의 수치를 취합하여 서버의 취약성에 대한 퍼지정도의 척도를 구해보면, I번째 취약성 항목에 대한 판단집합을

$$S_i = (A_1, A_2, A_3, \dots, A_n)$$

n =판단자의 수, A_j = j 번째 판단자가 i 번째 항목에 대해 입력한 수치 S_i 에 대한 퍼지정도의 척도를 구해보면 위 퍼지정도의 척도식[본논문 관련 연구2.2]에 의해

$f(S_i) = - \sum_{j=1}^n (A_j \log_2 A_j + [1 - A_j] \log_2 [1 - A_j])$ 가 되고 $f(S_i)$ 를 정규화 시키면 정규화된 퍼지정도의 척도

$$F(S_i) = \frac{f(S_i)}{n}, 0 \leq F(S_i) \leq 1 \text{가 된다. 이 } F(S_i) \text{가 판단자의 불확실성의 정도가 된다. 따라서 불확실성의 정도를 감소시킨 판단집합 } US_i \text{는}$$

$$US_i = (A_i - [A_i \times F(S_i)], 1 \leq i \leq n, n = \text{판단자의 수}) \text{가 된다.}$$

따라서 취약성 항목의 오염 여부를 가리기 위한 취합된 값 V_i 는 취약성 항목에 대한 판단집합 US_i 에 대해

$$V_i = \frac{\sum US_i}{n} (V_i : i \text{번째 항목에 대한 취합된 판단값}) \text{이 된다.}$$

V_i 를 경고메시지 필터링룰 생성에 적용하기 위해 위에서 구한 각 취약성 항목에 대한 정규화된 퍼지정도의 척도 $F(S_i)$ 를 취합하면

$$UF = \frac{\sum F(S_i)}{i}, i = \text{항목수} \text{이 된다. } UF \text{는 전체 항목에 대한 불확실성의 정도라 말할 수 있고, [표2]의 90\% 이상 오염확률수치에서 } UF \text{를 제외 시킨 값을 오염을 판단하기 위한 기준으로 활용}$$

구분	내용
ALLOW	경고메시지를 허용한다
DROP	경고메시지를 제거한다
IP	IP Address
PORT	Port Number
PROTOCOL	Protocol Name

표3. 필터링룰 형식

할 수 있다. 오탐판단 기준값을 구하면

$$MDS(MissDetectionStandard) = 0.9 - (0.9 \times UF)$$

가 되고 MDS 를 기준으로 하여 V_i 가 MDS 와 같거나 크면 오탐이라 판단할 수 있고, 작으면 오탐이 아니라고 판단 할 수 있다.

전체적인 취약성 분석 시스템 구성[그림2]은 인터넷 내부 각 서버들의 취약성에 대한 판단자들의 오염수치를 퍼지기법을 이용 취합하여 MDS 를 기준으로 [표3]의 필터링룰 형식에 맞춰 룰을 생성 하고 침입탐지 시스템에서 수집된 경고데이터를 리포팅하기 전에 적용하여 오탐에 의한 경고메시지를 축소시킨다.

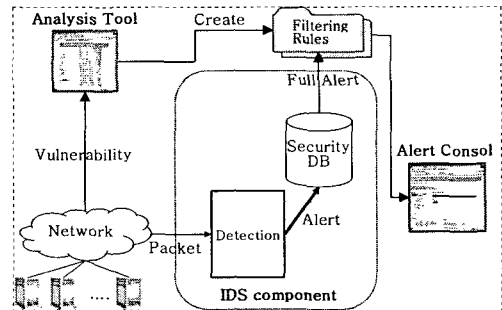


그림2. 취약성 분석 필터링 시스템 구성도

IV. 실험결과

실험을 위해 리눅스 RedHat 8.0(커널 2.4.18-14)에 실시간 트래픽 분석과 IP 네트워크 상에서 패킷 로깅이 가능한 가벼운 침입탐지 시스템으로 유명한 Snort_1.9.1을 이용하며 경고메시지 리포팅을 위하여 Snort센서의 로그를 그래프와 HTML형태로 웹을 통하여 보여주는 ACID 툴을 이용하였다.

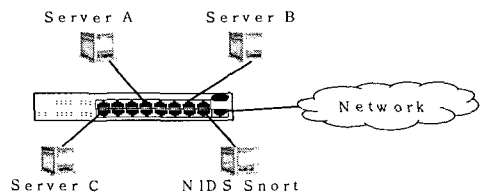


그림3. 실험 환경

[그림3]와 같은 실험 환경에서 3일간 발생한 경고메시지 데이터를 ACID를 통해 리포팅한 실험 전 결과에 비해 서버A, B, C의 취약성 필터링률을 생성 ACID에 적용시킨 결과 경고메시지가 40%정도 축소되었음을 알 수 있다[그림4]. 결과적으로 현재 네트워크망에서 발생하는 다수의 경고메시지는 긍정오류로 인한 오탐임을 알 수 있다. 따라서 경고메시지의 축소를 좀 더 빠른 침입판단을 할 수 있다.

실험 전	실험 후
Sensors: 1 Unique Alerts: 68 { 0 categories } Total Number of Alerts: 1315 <ul style="list-style-type: none"> • Source IP addresses: 62 • Dest IP addresses: 3 • Unique IP links: 66 <ul style="list-style-type: none"> • Source Ports: 871 <ul style="list-style-type: none"> ◦ TCP (866) UDP (5) • Dest Ports: 11 <ul style="list-style-type: none"> ◦ TCP (11) UDP (0) 	Sensors: 1 Unique Alerts: 23 { 5 categories } Total Number of Alerts: 653 <ul style="list-style-type: none"> • Source IP addresses: 35 • Dest IP addresses: 4 • Unique IP links: 37 <ul style="list-style-type: none"> • Source Ports: 411 <ul style="list-style-type: none"> ◦ TCP (411) UDP (0) • Dest Ports: 8 <ul style="list-style-type: none"> ◦ TCP (8) UDP (0)

그림4. 실험 결과

V. 결론 및 향후 연구방향

최근 국내외적으로 전산망에서 주요 정보 유출 및 파괴를 막기 위해 침입탐지시스템을 도입을 하고 있다. 그러나 현재의 침입탐지 시스템은 경고메시지의 과다 발생으로 인한 침입판단의 어려움이 존재하고, 이러한 오탐으로 인해 실제적인 침입행위를 탐지하지 못하는 실수를 범할 확률이 높아진다. 이에 본 연구에서는 이러한 오탐 경고메시지를 줄이기 위해 퍼지기법을 이용한 다수의 판단자의 오탐 확률수치를 취합하여 판단자의 주관적 해석에 따른 불확실성을 감소시킨 필터링률을 생성 및 적용하여 긍정오류로 인한 경고메시지를 축소시킬 수 있었다. 본 연구는 향후 침입탐지 시스템의 성능개선에 활용될 수 있으며, 더 나아가서 침입방어 시스템의 가장 큰 요구사항인 탐지의 정확성 향상에도 활용할 수 있다.

향후 연구 과제로 하나의 공격에 다수의 경고메시지가 발생하는데, 이를 축소시키기 위한 유사성분석과 공격유형을 고려한 경고메시지 통합방법에 관한 연구가 필요하다.

[참고문헌]

- [1] 월간 정보 보호 21c 정보 보호 지침서 “기업 정보보호 실천 가이드”
- [2] 이규연, “네트워크 기반 침입탐지 시스템의 경고메시지 축약 구조”, 포항공과대학교, 2002
- [3] 한석재, “리눅스 기반의 실시간 침입탐지 시스템 설계 및 구현”, 한남대학교, 2002
- [4] 최상용, “퍼지기법을 이용한 정보시스템 취약성 평가 도구 설계 및 구현”, 한남대학교, 2003
- [5] 이광형, 오길록 “퍼지이론 및 응용”, 홍릉과학출판사, 1991. 3
- [6] 菅野道夫, “퍼지척도의 퍼지적분” 計測自動學會論文集 8, 1972.
- [7] COAST(Computer Operations, Audit, and Security Technology), <http://www.cerias.purdue.edu/coast/coast.html>
- [8] 허영준, “IDS 기술 동향”, 한국전자통신연구원 보안게이트웨이연구팀, 2002
- [9] Frederic Cuppens, "Managing alerts in a multi-intrusion detection environment", 17th Annual Computer Security Applications Conference, 2001
- [10] Herve Devar and Andreas Wespi, "Aggregation and Correlation of Intrusion Detection Alerts", RAID 2001, Springer-Verlag Berlin Heidelberg, 2001