한국시뮬레이션학회 논문지
Vol. 17, No. 3, pp. 9-18 (2008. 9)

퍼지로직을 적용한 네트워크 보안 시스템의 성능향상에 관한 연구

서희석[1†]

A Study on performance improvement of network security system applying fuzzy logic

Hee Suk Seo

ABSTRACT

Unlike conventional researches, we are able to i) compare the fuzzy logic based BBA with non-fuzzy BBA for verifying the effective performance of the proposed fuzzy logic application ii) dynamically respond to the intrusion using BBA whereas the previous IDS was responding statically and iii) expect that this would be a cornerstone for more practical application researches (analyzing vulnerability and examining countermeasures, etc.) of security simulation. Several simulation tests performed on the targer network will illustrate our techniques. And this paper applies fuzzy logic to reduce the false negative that is one of the main problems of IDS. Intrusion detection is complicated decision-making process, which generally involves enormous factors about the monitored system. Fuzzy evaluation component model, which is a decision agent in the distributed IDS, can consider various factors based on fuzzy logic when an intrusion behavior is detected. The performance obtained from the coordination of intrusion detection agent with fuzzy logic is compared against the corresponding non fuzzy type intrusion detection agent. The results of these comparisons allow us to evaluate a relevant improvement on the fuzzy logic based BBA.

Key words : Fuzzy logic, Network security system, Simulation, Modeling

요 약

단순히 퍼지만을 사용하여 시스템을 연동하는 경우와 퍼지로직을 같이 사용하여 침입 탐지 에이전트의 시스템 성능향을 향상시키는 경우에 관한 연구로서, 블랙보드 기반의 비퍼지로직을 사용하는 경우와 블랙보드 기반의 퍼지 로직을 사용하는 경우을 비교한다. 또한 BBA를 통해 정적으로 대응하던 시스템을 향상시켜 동적 대응이 가능하게 구성하여 현실적인 시스템이 되도록 구성하였다. 대상 시스템의 성능을 평가하기 위하여 시뮬레이션을 수행하였다. 퍼지 시스템을 사용함으로써 false negative를 줄일 수 있었다. 분산 침입탐지를 위해 포함된 퍼지로직은 다양한 요소를 고려하기 때문에 침입의 성능을 높일 수 있다. 퍼지시스템을 사용하는 경우와 비퍼지 시스템의 성능을 비교함으로써 퍼지 시스템의 성능 향상을 보이며, 이러한 비교를 통해 전체 시스템의 성능 향상을 보인다.

주요어 : 정책기반네트워크, 네트워크 에이전트 연동, 블랙보드구조, 보안시스템

1. 서 론

시뮬레이션이란 문제 해결의 대상이 되는 시스템이 시간에 따라 어떻게 변화하는지를 예측 또는 평가하는 것을 말한다[1,2]. 이것은 시스템을 축소 및 추상화한 모델을 통해 이루어지는데 실제 시스템에서 문제 해결을 하기에는 불가능하거나 위험한 일 또는 경비가 많이 드는 일들을 비교적 쉽게 처리할 수 있으므로 그 중요성이 대두되고 있다. 네트워크의 속도가 급속하게 발전하는 상황에서 많은 양의 데이터를 처리해야 하는 보안 시스템을 직접 사용해 보안 시스템의 성능을 평가하는 것은 많은 비용과 노력을 요구하므로 이를 효과적으로 해결하기 위한 대안이 시뮬레이션 모델을 통해 보안 시스템을 평가하는 것이

* 이 논문은 2007년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2007-331-D00450)

2008년 6월 10일 접수, 2008년 7월 13일 채택

[1)] 한국기술교육대학교 인터넷미디어공학부
주 저 자 : 서희석
교신저자 : 서희석
E-mail; histone@kut.ac.kr

다[3,4]. 시뮬레이션 모델을 통해 구축된 시뮬레이션 환경은 다양한 환경을 조성하고, 시뮬레이션을 반복적으로 수행할 수 있으므로 변화하는 네트워크의 상황에 알맞은 보안 환경을 효과적으로 설정할 수 있다. 시뮬레이션은 위와 같은 가상 실험 환경 조성 이외에도 침입 탐지와 같은 특정 문제의 해결 모듈을 구성하는 데에도 효과적으로 적용된다.

본 연구는 침입탐지의 성능을 향상시키기 위하여 퍼지 로직을 적용하는 방법에 관한 연구이다. 퍼지로직을 적용함으로써 침입에 대한 판단에 있어서 보다 정확한 탐지가 가능하며 이는 관리자들에게 부담으로 작용되는 오작동의 비율을 줄일 수 있는 장점이 존재한다. 침입 탐지 시스템[5], 침입 차단 시스템[6], BBA[7,8]을 중심으로 보안 모델을 구축한 뒤 다양한 네트워크 구성요소 및 침입 모델을 추가함으로써 네트워크 보안 시뮬레이터에 대해서 소개한다.

본 논문에서는 분산 환경에서 침입을 탐지하기 위해 시뮬레이션 환경을 구성하였다. 침입을 판단하기 위해 퍼지[9-11]를 적용하여 여러 에이전트의 다양한 상황을 고려하여 침입을 탐지하도록 하였다. 블랙보드만을 사용하여 경우 침입을 탐지하는 경우와 퍼지를 적용하여 침입을 탐지하는 경우에 대해서 성능을 비교해 본다.

2. 시스템 모델링

2.1 침입 탐지 모델

그림 1은 각 호스트에 탑재된 침입 탐지 모델의 구성도

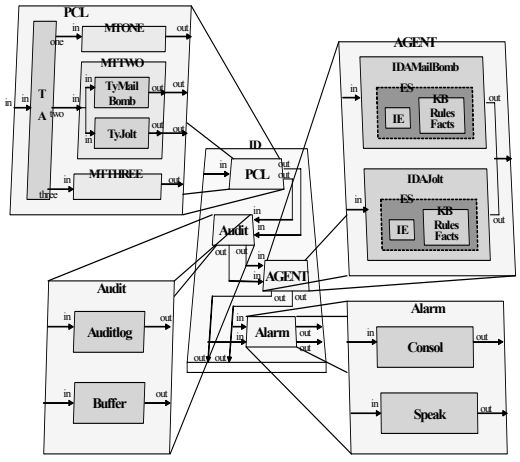

그림 1. 침입 탐지 모델의 구성

이다. 침입 탐지 모델은 크게 PCL, Audit, Alarm과 AGENT 모델로 구성된다. 각 모델의 세부 기능은 아래에서 설명한다.

2.1.1. PCL 모델

PCL 모델은 AGENT 모델에서 사용될 패킷을 분류하고, 필터링하는 역할을 수행하는 모델이다. 침입 탐지 시스템은 많은 양의 데이터를 처리해야 하므로 네트워크에서 수집된 모든 패킷을 검사하는 것은 비효율적이다. 그러므로 침입 탐지에 필요한 정보만을 추출할 필요가 있는데 이러한 역할을 하는 부분이 바로 PCL 모델이다. mailbomb 공격을 예로 들어 PCL 모델의 동작을 설명한다. mailbomb 공격은 메일 서버에 많은 양의 메일을 보내 메일 서버의 동작을 느리게 하거나 전복시키기 위한 DoS 공격의 일종이다. 일반적으로 한 사용자가 다른 사용자에게 전자 메일을 보내기 위해서는 TCP 프로토콜을 사용하고, 25번 포트를 사용한다. 그러므로 PCL 모델의 TyMail-Bomb 모델은 TCP 프로토콜을 사용하고, 25번 포트를 사용하는 패킷만을 통과시키고, 그 이외의 패킷은 소멸시킨다. 이렇게 함으로써 침입 탐지 시스템의 처리량을 줄이게 된다.

2.1.2. Audit 모델

컴퓨팅 환경이나 네트워크 환경에서와 같이 침입 탐지를 위한 처리 환경에서도 정보의 저장은 매우 중요한 역할을 한다. 정보의 저장은 시스템의 상태값, 공격 과정, 공격의 과거 자료들, 크래커들을 구분하기 위한 증거 자료나 다른 여러 곳에 사용될 중요한 정보원으로 활용된다. Audit 모델은 Auditlog 모델과 Buffer 모델로 구성된다. Auditlog 모델의 역할은 다음과 같다. 침입 탐지 시스템은 종종 자신이 사용한 감사 기록 정보나 네트워크에서 수집한 정보를 보관한다. 감사 정보는 일반적으로 보안상의 중요한 가치를 지니므로 안전한 저장소에 저장할 필요가 있다. Auditlog 모델은 이렇게 침입 탐지 시스템의 log 정보를 기억하는 저장소이다. 다음으로 Buffer 모델에 대해서 설명한다. 일반적으로 침입 탐지 시스템은 많은 양의 데이터를 처리해야하고, 이렇게 많은 양의 데이터 처리를 위해서 저장 공간이 필요하게 된다. 침입 탐지 시스템이 대상 시스템의 처리 용량이나 성능과 맞추기 위해서 하드웨어적이나 소프트웨어적으로 구현된 버퍼(or cache) 공간이 필요하다. Buffer 모델은 이렇게 대상 시스템의 많은 트래픽을 잃지 않고 저장하면서 사용하기 위해서 구현된 모델이다.

2.1.3. AGENT 모델

AGENT 모델은 침입 탐지 모델의 핵심 모델로 침입을 판별하기 위해 규칙 기반 전문가 시스템을 내장하도록 하였다. AGENT 모델은 Audit 모델에서 전달받은 패킷을 전문가 시스템에서 사용하는 사실(fact)의 형태로 전환하고, 이 사실을 전문가 시스템에게 넘겨준다. 전문가 시스템은 자신이 갖고 있는 규칙에 이 사실을 적용하여 침입을 판별하게 된다. 전문가 시스템의 지식 기반(Knowledge Base)는 그림 1의 Knowledge Base에 해당하는 모듈로서 침입 탐지에 필요한 다양한 규칙을 가지고 있다. AGENT 모델이 침입을 탐지하게 되면 Alarm 모델에게 이 사실을 알린다.

2.1.4. Alarm 모델

침입 탐지 시스템이 호스트나 네트워크의 상황을 살피면서 침입이나 의심스러운 행위 등을 탐지하게 되면 이러한 침입 상황을 알리는 모듈이 있어야 한다. 이러한 모듈은 많은 침입 탐지 시스템이 갖고 있고, 유용한 역할을 담당하게 된다. Alarm 모델의 역할은 단순한 텍스트 형태의 메시지를 화면에 내보내기도 하고, 특정 사용자에게 자동으로 메일을 보내거나 전화 연결을 시도한다. 또 설정된 특별한 곳으로 팩스를 보내게 할 수도 있으며, 원격지나 현재 사용 중인 컴퓨터의 특정한 프로그램을 실행하도록 좀 더 향상된 기능을 제공하기도 한다. 본 연구진은 화면에 경고를 보내는 consol 모델과 일정한 경보음을 내보내는 speak 모델을 구성하였다.

2.2 방화벽 모델

방화벽도 한계와 결점을 갖고 있지만 방화벽이 네트워크를 연결하고 그 네트워크를 보호할 수 있게 해주는 효과적인 방식이기 때문에 많이 설치를 하고 있다. 방화벽은 인터넷과 내부 네트워크 사이의 엄격한 접근 제어 수단을 제공하는 방법이다. 그림 2는 시뮬레이션을 위해서 사용될 방화벽 모델의 구성을 보이고 있다. 방화벽 모델은 Controller 모델, Inbound_Filter 모델과 Outbound_Filter 모델로 구성된다. Inbound_Filter 모델과 Outbound_Filter 모델은 Protocol 모델, Address 모델, Port 모델과 Data 모델로 구성된다. Controller 모델은 인터넷이나 내부 네트워크로부터 패킷을 받게 되는데 그 패킷을 방향에 의해서 Inbound_Filter 모델이나 Outbound_Filter 모델로 전달하게 된다. 각 Filter 모델은 받은 패킷을 각각 가지고 있는 보안 정책에 의해서 패킷을 처리하여 다음 모델로 전달하게 된다. Controller 모델은 각 Filter 모델로

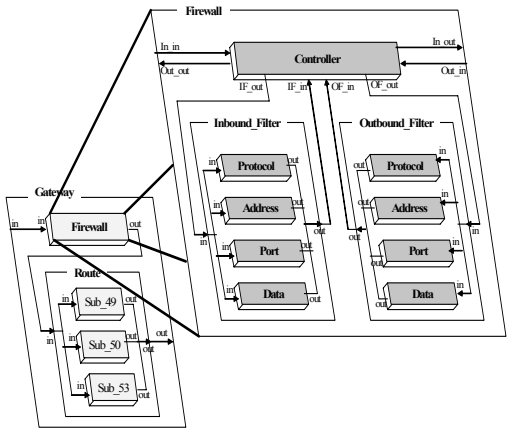

그림 2. 방화벽의 구성

부터 받은 패킷을 보고, 다음 모델로 보내던지 버리게 된다. 예를 들어 mailbomb 공격의 경우 Firewall 모델은 인터넷으로부터 패킷을 받게 된다. 이 패킷을 Controller 모델에게 전달하게 되고, Controller 모델은 이 패킷을 Inbound_Filter 모델에게 전달하게 된다. Inbound_Filter 모델은 IP(Internet Protocol) 주소를 조사하여 자신이 갖고 있는 규칙 테이블 정보에 의하여 패킷을 버릴 것인지 내부 네트워크로 들여보낼 것인지를 판단하게 된다.

2.3 퍼지 시스템 모델

퍼지로직을 사용하여 분산환경에서 침입을 탐지하기 위해서는 다양한 요소들을 고려하여 침입의 행위를 판단하게 된다. 블랙보드 상에 5가지 레벨(Minimal, Cautionary, Noticeable, Serious와 Catastrophic) 중에서 이전의 방법에서는 각각의 에이전트 중에서 최상의 레벨을 갖는 에이전트의 값에 의해 전체 시스템 및 네트워크의 상황이 결정되었다.

즉 A 침입탐지 에이전트가 Noticeable 레벨이 있고 다른 에이전트들은 Cautionary 레벨에 있다면 전체 시스템은 Noticeable 레벨로 평가가 되고 이에 해당되는 정책이 적용되도록 구성되어 있었다.

Cautionary 레벨의 임계값을 31과 40 사이의 값이고, Noticeable 레벨의 임계값은 41에서 50사이로 정하여 사용하고 있었다. 임계값의 변화가 38에서 39로 바뀌는 것은 전체 시스템에 큰 영향을 미치지 않으나 40에서 41로의 전이는 시스템 전체적으로 본다면 매우 중요한 전이가 된다. 단순한 1이라는 값의 변화이지만 시스템 대응 상황

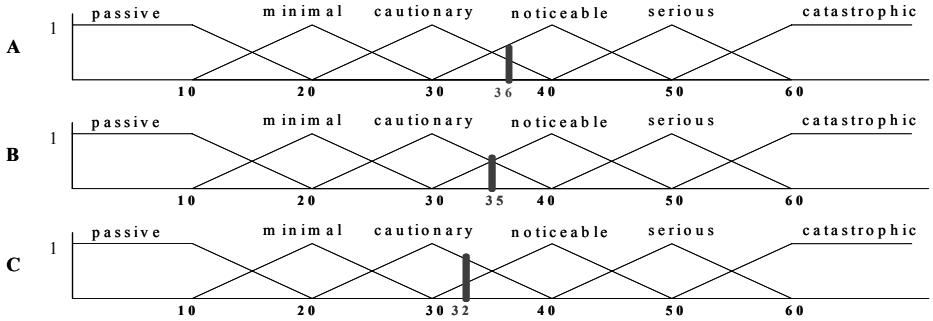

그림 3. 에이전트의 멤버쉽 함수

$$CoA(C) = \frac{Area(C_1)*CoA(C_1)+ Area(C_2)*CoA(C_2)+ Area(C_3)*CoA(C_3)}{Area(C_1) + Area(C_2) + Area(C_3)}$$

그림 4. crisp 값을 얻기 위한 수식

이 바뀔 수 있는 것이다. 따라서 본 연구에서는 이러한 문제를 퍼지로직을 사용하여 해결하고자 한다. 제안된 퍼지 로직의 평가 모델은 4가지 세부 단계로 구성된다.

1. 퍼지 규칙의 기본 단계에 대한 계산
2. 매칭 정도에 따른 규칙에 대한 계산
3. 모든 퍼지 규칙에 의해 추론된 결론과의 결합
4. 최종 crisp 값의 결정

그림 3은 각 에이전트가 사용하는 멤버쉽 함수를 보여주고 있다. 퍼지 추론은 빠른 연산을 위해 스케일링 기법을 사용한다. 퍼지 결합을 위해서는 SAM(Standard Additive Model) 모델을 사용한다. SAM 모델에서 퍼지 규칙의 구조는 만다니 모델과 같다. 최종 crisp 값을 얻기 위한 방법은 아래와 같은 수식에 의해서 얻어진다.

2.4 에이전트 연동을 위한 BBA 모델

BBA 모델은 다양한 보안 에이전트들이 서로 정보를 공유하면 네트워크 상에서 정보를 공유하기 위한 방법을 제공하는 모델이다.

본 연구진은 공격의 종류를 네트워크 상에서 진행이 되는 네트워크 공격과 호스트를 대상으로 공격을 진행하는 호스트 공격으로 구분하였다. 이들이 서로 통신하는 방법을 소개한다.

각 에이전트는 두 가지 메시지에 의해서 통신을 수행한다. 하나는 제어 메시지이고, 다른 하나는 데이터 메시지이다. 제어 메시지는 에이전트와 제어기 사이의 통신에 필요한 메시지이고, 데이터 메시지는 에이전트와 블랙보드 간의 데이터 전송에 사용되는 메시지이다.

우선 호스트 공격이 발생한 경우 블랙보드의 상태를 살펴본다. 호스트 공격은 네트워크 상의 호스트 중 하나의 호스트만이 공격을 받고 있는 경우이다. 이러한 경우 공격을 받고 있는 호스트는 블랙보드 상의 Host-Attack에 해당 정보를 게재하게 된다.

블랙보드에 메시지를 게재하기 위해서 해당 에이전트는 BB_update_request 메시지를 제어기에게 보낸다. 이러한 방법을 사용하는 이유는 통신상의 무결성과 에이전트 간의 메시지 전송 충돌을 방지하기 위해서이다. 블랙보드에 메시지를 게재할 수 있다면 제어기는 해당 에이전트에게 BB_update_permit 메시지를 전송한다. 이 메시지를 수신한 에이전트는 블랙보드에 침입에 관련된 정보를 게재(BB_update_action)하고 BB_update_completion 메시지를 제어기에게 보낸다.

제어기는 각 에이전트에게 BB_broadcasting_of_action_request 메시지를 보내고 이 메시지를 수신한각 에이전트는 블랙보드에서 침입 관련 정보를 열람(BB_information_retrieval_action)한다. 정보를 모두 열람한 에이전트는 제어기에게 BB_information_acquisition_completion 메시지를 보내 통신을 마치게 된다. 이러한 과정을 거쳐 공격을 받고 있는 에이전트는 블랙보드 상에서 전이를 하게 된다. 블랙보드의 레벨이 Host-Attack의 Serious 레벨에 이르면 공격 IP(Internet Protocol)에서 에이전트로 전송되는 모든 패킷은 방화벽에 의해서 차단된다.

다음은 네트워크 공격이 발생한 경우 블랙보드의 상태를 살펴본다. 네트워크 공격은 네트워크 상의 여러 호스트들이 공격을 받는 경우이다. 이러한 경우 공격을 받고 있는 호스트는 블랙보드 상의 Network-Attack에 해당 정보를 게재하게 된다. 한 에이전트가 공격을 받게 되면 Host-Attack에서 레벨의 전이를 하게 된다. 이렇게 한 에이전트가 공격 정보를 블랙보드에 게재하고 있는 동안, 다른 에이전트 또한 공격을 받게 된다면 이는 네트워크 공격에 해당한다. Network-Attack의 각 레벨은 다음과 같이 정해졌다. Network-Attack의 Minimal, Cautionary, Noticeable, Serious와 Catastrophic 레벨은 2개 이상의 호스트가 해당 공격을 받는 경우에 해당된다. 예를 들어, Network-Attack의 Cautionary 레벨은 2개 이상의Host-Attack 레벨이 Cautionary 이상일 때를 의미한다. 하나의 호스트가 Cautionary 레벨이고, 하나의 호스트가 공격을 받아 Minimal에서 Cautionary로 전이를 하게 되면, 네트워크 전체는 Network-Attack의 Cautionary 레벨이 된다. 네트워크 공격 시 블랙보드 상의 메시지 전송 방법은 기본적으로 호스트 공격에서의 전송 방법과 동일한 방법으로 메시지를 전송한다.

구성된 시뮬레이션 환경에서는 네트워크 공격을 받는 경우 몇 번의 전이를 거쳐 Network-Attack의 Noticeable 레벨이 되면 공격지에서 전송되는 모든 패킷을 차단하여 네트워크가 공격자로부터 보호되도록 하였다.

공격이 지속되어 Network-Attack의 Serious 레벨에 이르면 네트워크로 유입되는 모든 패킷을 차단하여 네트워크 전체를 보호하였다. 이러한 조치를 통하여 관리자는 네트워크 전체나 일정 호스트에 보안 설정을 다시 할 수 있으며 해당 공격을 막을 수 있다. 이와 같이 블랙보드의 레벨을 세분화하여 관리함으로써 각 레벨에 대한 대처를 용이하게 하고, 침입 탐지의 민감도를 높일 수 있다.

3. 퍼지 시스템의 적용

이전의 시스템과 퍼지 로직을 적용한 두 시스템간의 블랙보드 레벨의 전이의 차이에 대해서 설명한다. 현재 네트워크에 A, B, C 세 개의 에이전트가 있다고 가정한다. 현재 시스템에 있는 에이전트들은 모두 Cautionary 레벨에 있는 것으로 가정한다. 만약 비퍼지시스템에서 공격자의 계속적인 공격이 진행된다면 A 에이전트의 임계값은 38로 전이하게 된다.

따라서 A 에이전트의 블랙보드의 레벨은 호스트 공격의 Noticeable 레벨로 전이하게 된다. 만약 A 에이전트가 계속적인 공격을 받는다면 임계값은 Serious 레벨이 이르게 된다. 결국 나머지 두 에이전트도 Noticeable 레벨로 전이하게 된다.

퍼지시스템에서의 레벨 전이에 대해서 설명한다. 모든 ID 에이전트의 임계값은 30으로 가정한다.(이 값은 비퍼지시스템의 Cautionary 레벨에 해당한다.) A 에이전트의 임계값이 공격에 의해서 38(비퍼지시스템에서 Noticeable 레벨에 해당하는 값)로 바뀌더라도 퍼지로직에 의해서 연산된 레벨 값은 여전히 네트워크 공격의 Cautionary 레벨에 머문다. 만약 A 에이전트가 Serious 레벨로 전이한다면, 즉 임계값이 45에 이른다면 다른 두 에이전트는 Noticeable(임계값 35) 레벨로 전이하게 된다.

이 경우 비퍼지시스템인 경우는 호스트 공격의 Serious 레벨로 전이하나, 퍼지시스템에서는 네트워크 공격의 Noticeable 레벨로 전이하게 된다. 만약 A 에이전트의 임계값이 53, B 에이전트의 임계값이 42, C 에이전트의 임계

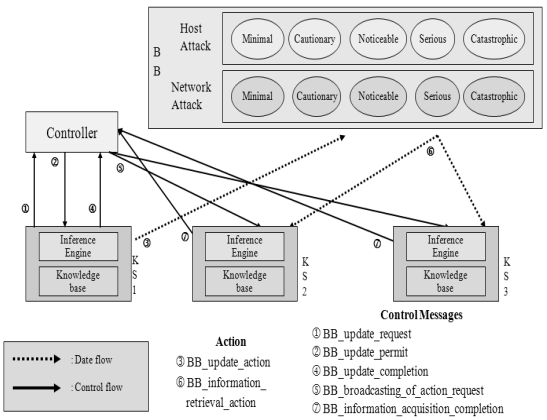

그림 5. BBA 모델

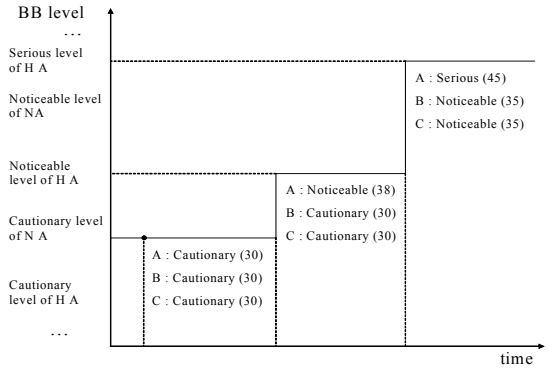

그림 6. 비퍼지 시스템에서 블랙보드 전이

표 1. 비퍼지시스템의 레벨 결정

blackboard level	level selection
Cautionary level of Network Attack	MAX(Cautionary(A), Cautionary(B), Cautionary(C))
Noticeable level of Host Attack	MAX(oticeable(A), Cautionary(B), Cautionary(C))
Serious level of Host Attack	MAX(Serious(A), Noticeable(B), Noticeable(C))

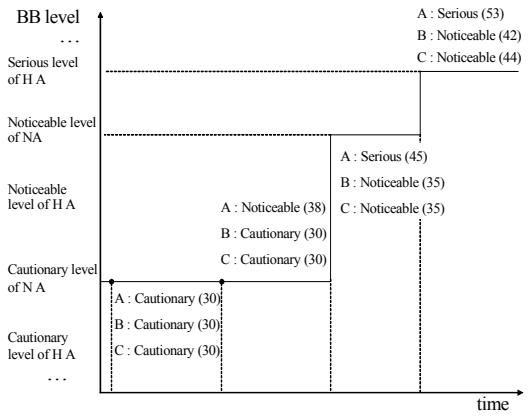

그림 7. 퍼지 시스템에서 블랙보드 전이

표 2. 퍼지 시스템의 규칙

Fuzzy Rules			
A_host	B_host	C_host	BB level
passive	passive	passive	Passive
passive	passive	minimal	Passive
passive	minimal	minimal	Minimal
minimal	minimal	cautionary	Minimal
minimal	cautionary	cautionary	Cautionary
...			
cautionary	cautionary	cautionary	Cautionary
cautionary	cautionary	noticeable	Cautionary
noticeable	noticeable	serious	Noticeable
noticeable	noticeable	serious	Noticeable
serious	serious	noticeable	Serious
serious	serious	catastrophic	Serious
catastrophic	catastrophic	catastrophic	Catastrophic

값이 44에 이른다면 그때서야 블랙보드의 레벨이 호스트 공격의 Serious 레벨로 전이한다.

또 다른 경우의 블랙보드 레벨 전이에 대해서 설명한다. 만약 침입탐지 에이전트 A의 임계값이 36에 이르러

표 3. 퍼지시스템의 레벨 결정
(C:Cautionary, N:Noticeable, S:Serious, Ca:Catastrophic)

Blackboard level	퍼지 매칭 규칙	Combing	비퍼지화
Cautionary level of Network Attack	(A:38, B:30, C:30) (C,C,C) (N,C,C)	$\frac{2*30+8*30}{2+8}$	30
Noticeable level of Network Attack	(A:45, B:35, C:35) (N,C,C) (S,C,C) (N,C,N) (S,C,N) (N,N,C) (S,N,C) (N,N,N) (S,N,N)	$\frac{5*30+5*40+5*40+5*40}{5+5+5+5}$ + $\frac{5*30+5*40+5*40+5*40}{5+5+5+5}$	38
Serious level of Host Attack	(A:53, B:42, C:44) (S,N,N) (Ca,N,N) (S,N,S) (Ca,N,S) (S,S,N) (Ca,S,N) (S,S,S) (Ca,S,S)	$\frac{6*40+4*50+2*50+2*50}{6+4+2+2}$ + $\frac{3*40+3*50+2*50+2*50}{3+35+2+2}$	46

호스트 공격의 Noticeable 레벨에 이르게 된다. 각 에이전트들이 계속 공격을 받아 침입탐지 에이전트 A가 임계값이 38에 이르고, B 에이전트의 임계값이 37에 이르며 C 에이전트는 34에 이른다고 가정한다. 이러한 상황이라면 전체 시스템 상황은 네트워크 공격의 Noticeable 레벨에 이르게 된다.

계속된 공격에 의해 에이전트 A의 임계값이 36(비퍼지 시스템의 경우라면 Noticeable 레벨)으로 변하더라도 퍼지로직의 계산에 의하면 여전히 네트워크 공격의 Cautionary 레벨에 머문다. 에이전트 A가 Noticeable 레벨(임계값이 36이므로)에 있고 에이전트 B가 Noticeable 레벨(임계값이 35이므로)에 있으며, 에이전트 C는 Cautionary 레벨(임계값이 30이므로)에 있다고 하더라도 전체적인 시

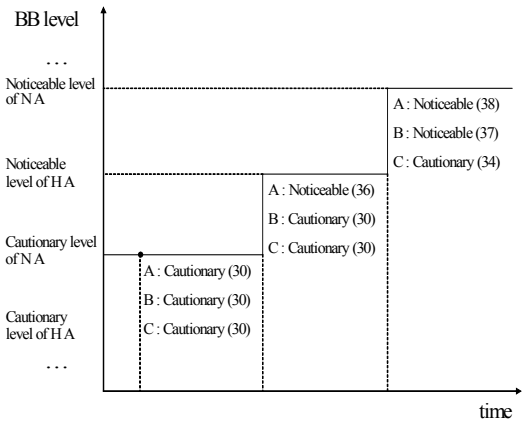

그림 8. 비퍼지 시스템에서 블랙보드 전이

표 4. 비퍼지시스템의 레벨 결정

blackboard level	level selection
Cautionary level of Network Attack	MAX(Cautionary(A), Cautionary(B), Cautionary(C))
Noticeable level of Host Attack	MAX(Noticeable(A), Cautionary(B), Cautionary(C))
Noticeable level of Network Attack	MAX (Noticeable(A), Noticeable(B), Cautionary(C))

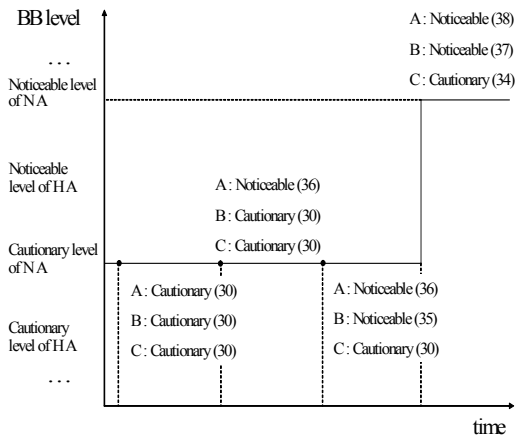

그림 9. 퍼지 시스템에서 블랙보드 전이

스템의 상황은 네트워크 공격의 Cautionary 레벨에 머물게 된다. 만약 A 에이전트의 임계값이 38에 이르고, B 에이전트가 37, C 에이전트가 34에 이르게 된다면, 그때 비로소 시스템의 전체 레벨이 네트워크 공격의 Noticeable 레벨이 이르게 된다. 결국 퍼지 시스템을 적용하게 된다

표 5. 퍼지 시스템의 레벨 결정
(C:Cautionary, N:Noticeable, S:Serious, Ca:Catastrophic)

Blackboard level	퍼지 매칭 규칙	Combing	비퍼지화
Cautionary level of Network Attack	(A:36, B:30, C:30) (C,C,C) (N,C,C)	$\frac{4*30+6*30}{4+6}$	30
Noticeable level of Network Attack	(A:36, B:35, C:30) (C,C,C) (S,C,C) (C,N,C) (N,C,C) (N,N,C)	$\frac{4*30+4*30+5*30+5*40}{4+4+5+5}$	33
Serious level of Host Attack	(A:38, B:37, C:34) (C,C,C) (N,C,C) (C,C,N) (N,C,N) (C,N,C) (N,N,C) (C,N,N) (N,N,N)	$\frac{2*30+2*30+2*30+2*40}{2+2+2+2}$ + $\frac{3*30+3*40+6*40+4*40}{3+3+6+4}$	36

면 오탐의 가능성이 줄어들게 되어 false negative 에러를 줄일 수 있는 장점이 생기게 된다. 퍼지 시스템에 의한 블랙보드 전이는 비퍼지시스템에 비해 더 부드러운 전이가 이루어지게 되기 때문에 결과적으로 탐지의 성능을 높일 수 있게 된다.

4. 시뮬레이션

본 논문에서는 두 가지의 경우에 대해서 시뮬레이션을 수행하였다. 첫 번째 경우는 호스트 공격이 발생한 경우 침입 탐지 시스템이 침입을 탐지하는 경우이고, 다른 경우는 네트워크 공격이 발생한 경우 침입을 탐지하는 경우이다. 시뮬레이션을 수행하기 위한 시뮬레이션 환경은 본 연구진이 개발한 DEVS-ObjC를 사용하였다. DEVS-ObjC는 자체개발한 시스템으로 DEVS를 visual c++ 6.0에서

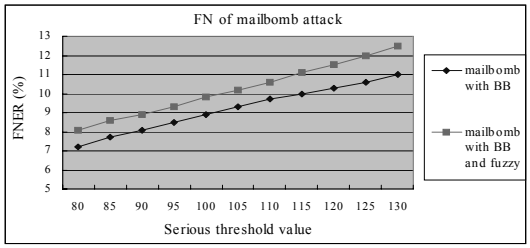

그림 10. MB 공격의 FNER(host)

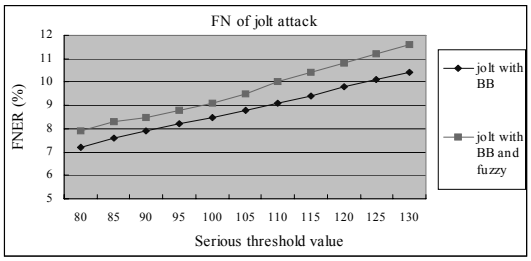

그림 11. Jolt 공격의 탐지시간(host)

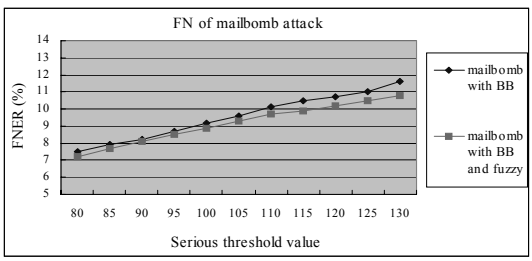

그림 12. MB 공격의 탐지시간(host)

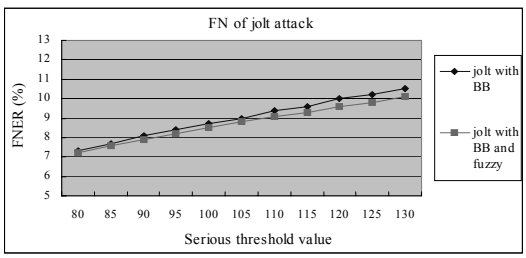

그림 13. Jolt 공격의 탐지시간(network)

사용할 수 있도록 구성한 개발환경이다. 내부 시스템을 공격하기 위해서 mailbomb 공격과 jolt 공격을 사용하였고, 이런 공격을 통해 침입 탐지의 성능을 측정하였다.

시뮬레이션을 위한 성능 지표로는 침입 탐지 시간, false negative error ratio를 선택하였다. 본 연구 결과는

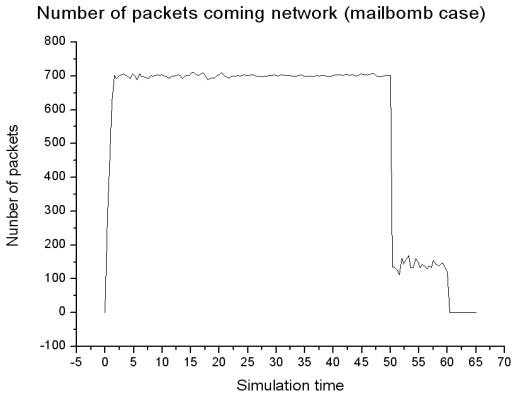

그림 14. Jolt 공격의 탐지시간(host)

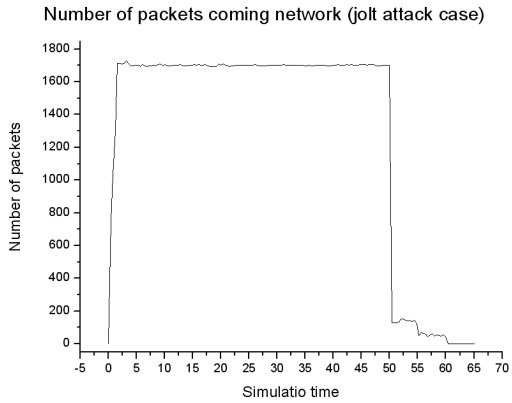

그림 15. Jolt 공격의 탐지시간(host)

BBA만을 사용한 경우와 BBA에 본 연구진이 제한하는 바인 퍼지로직을 적용하였을 경우 침입 탐지의 성능을 비교한다. 성능을 비교하기 위하여 침입탐지 시간과 FNER (false negative error ratio)를 측정한다.

시뮬레이션은 호스트에 대한 공격과 네트워크에 대한 공격을 대상으로 진행하였다. 그림 10, 11는 공격이 한 시스템에 적용되는 호스트에 대한 공격이고, 그림 12, 13은 공격에 네트워크 전체 시스템을 대상으로 진행되는 네트워크 공격이다.

그림 10-13는 mailbomb 공격과 jolt 공격의 PNER을 나타낸다. 보안레벨이 강화됨(임계값이 낮아짐)에 따라 PNER의 비율이 점점 줄어드는 것을 볼 수 있다. 모든 경우에서 보이는 바와 같이 퍼지 로직을 사용한 제안된 시스템의 성능이 더 우수함을 볼 수 있다. 퍼지로직을 사용한 침입 탐지 에이전트의 성능향상을 꾀할 수 있다.

그림 14, 15는 mailbomb 공격과 jolt 공격이 수행됨에

따라 네트워크에 유입되는 패킷을 양을 나타낸다. 본 연구에서 설정한 정책은 아래와 같다.

- 시스템 전체의 레벨이 호스트 공격의 Serious 레벨에 이른다면 해당 공격 시스템으로 유입되는 모든 패킷은 차단된다.
- 시스템 전체의 레벨이 네트워크 공격의 Serious 레벨에 도달한다면 해당 서브넷으로 유입되는 모든 패킷은 차단된다.
- 시스템 전체의 레벨이 호스트 공격의 Catastrophic 레벨에 이른다면 네트워크 전체로 유입되는 모든 패킷은 차단된다.

그림 14, 15와 같이 공격이 진행되에 따라서 정책이 적용되고, 결과적으로 패킷의 양이 점점 줄어들고 있다.

5. 결론 및 향후 연구계획

현재 인터넷상에서 진행되고 있는 공격들은 과거에 비하여 더 심각하고, 기술적으로 더 복잡해 졌다. 그래서 침입을 탐지하기 위해 하나의 침입 탐지 시스템을 사용하는 것은 효과적이지 못하다. 다수의 침입 탐지 시스템을 사용하여 서로 정보를 공유하며 침입을 탐지하는 것이 침입 탐지의 성능을 높이는 좋은 방법이다. 정보를 공유하기 위해서 블랙보드구조를 사용하는 시스템은 새로운 침입 탐지 에이전트를 추가하거나, 블랙보드의 레벨의 수를 쉽게 증가시킬 수 있어 확장이 용이하다. 블랙보드 레벨의 세분화를 통해 에이전트들 간의 정보 교환을 충분히 함으로 침입 탐지의 성능을 높일 수 있다. 침입 탐지 시스템간의 연동뿐 아니라 침입 탐지 시스템과 침입 차단 시스템의 연동은 네트워크를 안전하게 보호하는 방법을 제공한다.

본 연구는 침입탐지의 성능을 향상시키기 위하여 퍼지로직을 적용하는 방법에 관한 연구이다. 퍼지로직을 적용함으로써 침입에 대한 판단에 있어서 보다 정확한 탐지가 가능하며 이는 관리자들에게 부담으로 작용되는 오작동의 비율을 줄일 수 있는 장점이 존재한다. 침입 탐지 시스템, 침입 차단 시스템, BBA을 중심으로 보안 모델을 구축한 뒤 다양한 네트워크 구성요소 및 침입 모델을 추가함으로써 네트워크 보안 시뮬레이터에 대해서 소개하였다. 본 논문에서는 분산 환경에서 침입을 탐지하기 위해 시뮬레이션 환경을 구성하였다. 침입을 판단하기 위해 퍼지를 적용하여 여러 에이전트의 다양한 상황을 고려하여 침입을 탐지하도록 하였다. 블랙보드만을 사용하여 경우 침입을 탐지하는 경우와 퍼지를 적용하여 침입을 탐지하는 경우에 대해서 성능을 비교해 봄으로써 퍼지 로직을 사용하는 경우의 성능이 더 우수함으로 보였다.

참 고 문 헌

1. B. P. Zeigler, H. Praehofer, and T.G. Kim, Theory of Modeling and Simulation, Academic Press, 2000.
2. T. H. Cho, and B. P. Zeigler, “Simulation of Intelligent Hierarchical Flexible Manufacturing : Batch Job Routing in Operation Overlapping,” IEEE Transactions on Systems, Man and Cybernetics-PART A : System and Humans, Vol. 27, No. 1, pp. 116-126, Jan. 1997.
3. H. S. Seo, and T. H. Cho, “Modeling and Simulation for Detecting a Distributed Denial of Service Attack,” Lecture Notes on Artificial Intelligence, Springer Verlag, LNAI 2557, pp. 179-190, Dec. 2002.
4. T. H. Cho, and H. J. Kim, “DEVS Simulation of Distributed Intrusion Detection System,” Transactions of the Society for Computer Simulation International, Vol. 18, No. 3, pp. 133-146, Sep. 2001.
5. M. Biship, Computer Security, Addison-Wesley, 2003.
6. S. Malki, Network Security Principles and Practices, Cisco Press, 2003.
7. G. M. P. O'Hare and N. R. Jennings, Foundation of Distributed Artificial Intelligence, John Wiley & Sons Inc., 1996.
8. G. Van Zeir, J. P. Kruth, J. Detand, “A Conceptual Framework for Interactive and Blackboard Based CAPP,” International Journal of Production Research, Vol. 36(6), pp. 1453-1473, 1998.
9. J. E. Dickerson, J. Juslin, O. Koukousoula, and J. A. Dickerson, “Fuzzy intrusion detection,” In IFSA World Congress and 20th NAFIPS International Conference, pp. 1506-1510, 2001.
10. A. Orfila, J. Carbo, A. Ribagorda, “Fuzzy logic on decision model for IDS,” The 12th IEEE International Conference on Fuzzy Systems, Vol. 2, pp. 1237-1242, May 2003.
11. Z. Jian, D. Yong, G. Jian, “Intrusion detection system based on fuzzy default logic,” The 12th IEEE International Conference on Fuzzy Systems, Vol. 2, pp. 25-28, May 2003.

서 희 석 (histone@kut.ac.kr)

2000 성균관대학교 산업공학과 학사
2002 성균관대학교 전기전자및컴퓨터공학부 공학석사
2005 성균관대학교 전기전자및컴퓨터공학부 공학박사
2005～현재 한국기술교육대학교 조교수

관심분야 : 네트워크 보안, 모델링&시뮬레이션, USN, 악성코드