퍼지를 적용한 계약망 프로토콜 기반의 네트워크 보안 모델의 설계 및 시뮬레이션

이진아*, 조대호**

Modeling and simulation of CNP-applied network security models with application of fuzzy rule-based system

Jin-ah Lee, Tae-ho Cho

Abstract

Attempts to attack hosts in the network have become diverse, due to crackers developments of new creative attacking methods. Under these circumstances the role of intrusion detection system as a security system component gets considerably importance. Therefore, in this paper, we have suggested multiple intrusion detection system based on the contract net protocol which provides the communication among multiple agents. In this architecture, fuzzy rule based system has been applied for agent selection among agents competing for being activated. The simulation models are designed and implemented based on DEVS formalism which is theoretically well grounded means of expressing discrete event simulation models.

Key Words: network security, fuzzy logic, modeling and simulation

* 성균관대학교 전기전자컴퓨터공학부

** 성균관대학교 정보통신공학부

1. 서론

컴퓨터 기술의 발달과 인터넷의 발전은 업무 효율을 향상시키고 생활의 질을 높여주며 국가 경쟁력을 강화시켜 주는 등의 긍정적인 효과를 가져온 반면, 네트워크의 확장으로 외부에서의 시스템 불법 침입, 중요 정보의 유출 및 변경, 훼손, 불법적인 사용, 컴퓨터 바이러스 등의 역기능들이 증가되어 그 피해가 심각한 수준에 이르고 있다[1]. 네트워크에서 발생하는 보안상의 문제점을 해결하기 위하여 현재 침입 탐지 시스템, 침입 차단 시스템, 보안 운영체제 및 인증 시스템 등 여러 보안 시스템들이 사용되고 있으며, 본 연구에서는 침입 탐지 시스템(IDS)을 보안 요소로 도입하였다.

침입 탐지 시스템은 네트워크 시스템이나 컴퓨터상에서 발생하는 이벤트들을 모니터링하고, 자료를 수집한 후 분석하여 침입 발생 여부를 탐지(detection)하고 대응(response)하는 행동을 취하는 자동화된 보안 솔루션이다.

네트워크 기반(network-based) IDS는 시스템 내부에 설치되어 하나의 시스템 내부 사용자들의 활동을 감시하고 공격 시도를 탐지해 내는 호스트 기반(host-based) IDS와는 달리, 네트워크 상의 패킷을 분석하여 전체 네트워크에 대한 침입 탐지가 가능하게 하며, 호스트 기반의 IDS에서는 탐지 불가능한 침입도 탐지할 수 있다. 반면, 네트워크 기반 IDS는 많은 부하가 걸린 세그먼트들을 완전하게 처리할 수 없으며, 최근의 고부하 네트워크 환경에서는 패킷이 탐지되기도 전에 유실될 가능성이 높다는 단점이 있다.

따라서 본 연구에서는 네트워크를 기반으로 하는 다중 침입 탐지 시스템을 도입하였다. 분산 에이전트 기반의 다중 침입 탐지 시스템은 침입 탐지를 다수의 분산 에이전트들이 나누어 수행하므로 시스템의 부하를 감소시키고 침입 탐지의 속도를 향상시키며 발생된 침입에 적당한 에이전트를 선택하여 침입 탐지의 성능을 향상시킬 수 있다. 이러한 다중 에이전트 환경에서 에이전트 사이의 연동에 있어 효율적인 수행 능력을 위해서는 분산된 에이전트들에게 효과적인 작업의 할당이 이루어져야 하며[2], 본 논문에서는 이러한 에이전트 사이의 연동을 위하여 계약망 프로토콜(Contract Net Protocol)을 적용하였다.

계약망 프로토콜은 분산된 에이전트들 중에 입찰(bidding)을 통해 최상의 에이전트를 선택하고 선택된 에이전트는 서비스를 제공하게 된다[3-5].

본 연구에서는 대상 네트워크에서 침입을 탐지하였을 때, 에이전트들이 입찰을 했을 때, 에이전트를 선택하는 커맨드 콘솔에서 기존의 선택 알고리즘을 이용하여 에이전트를 선택했을 때와 비교하여 퍼지 규칙 기반 시스템(Fuzzy Rule-Based System)을 적용하여 에이전트를 선택했을 때, 어떻게 작업이 할당되는지를 시뮬레이션 하여 비교하고, 최종적으로 퍼지 규칙 기반 시스템을 적용했을 때 침입 탐지의 성능이 얼마나 향상 되었는지를 시뮬레이션 할 것이다. 또한 이산 사건 시뮬레이션을 수행하기 위하여 체계적으로 잘 정립된 이론인 DEVS 형식론을 이용하여 보안 시뮬레이션 환경을 구축한다[6].

2. 배경이론 및 관련 연구

2.1 침입 탐지 시스템(IDS)

침입 탐지 시스템은 외부의 침입에 대해 능동적으로 대처 하는 시스템으로 방화벽의 앞 또는 뒤에서 침입 사실을 탐지해 침입자의 공격에 대응하기 위한 솔루션이다[7,8].

침입 탐지 접근 방법은 크게 오용(misuse) 탐지와 비정상(anomaly) 행위 탐지 방법으로 나눌 수 있다. 오용 탐지 방법은 일반적으로 침입이라고 알려져 있는 행위 또는 비정상적인 행위를 패턴으로 저장해 놓고, 이에 일치 또는 유사한 사용자의 행위가 나타났을 때 이를 탐지하는 것이다. 비정상 행위 탐지 방법은

시스템이나 네트워크에서 일어나는 행위들 중 일반적이지 않고, 발생 빈도가 매우 낮은 행위의 발생을 탐지하는 방법이다. 이러한 탐지 방법은 침입자의 행위가 일반 사용자의 행위와 주목할 만큼 다르다는 가정을 기반으로 한다.

2.2 계약망 프로토콜(Contract Net Protocol)

다중 침입 탐지 시스템은 분산 시스템의 이론을 적용한 시스템으로 네트워크에 분산된 에이전트들에게 작업을 분산시킴으로써 시스템의 부하를 감소시켜 탐지의 속도를 향상시키고 발생된 침입에 적당한 에이전트를 선택하도록 하여 탐지의 성능을 높일 수 있다.

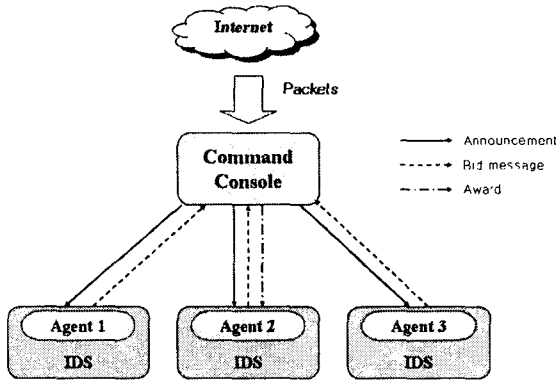
다중 에이전트 시스템에서 에이전트들은 시스템이 보다 나은 목표 달성을 위해 상호작용을 하고, 에이전트들 사이의 상호작용들이 서로 조화될 수 있도록 대화(communication하고 협력(cooperation)하며 타협(negotiation)하는 데에 있어서, 에이전트들이 자원 경쟁을 줄이고 교착상태를 피하며 안전성을 유지할 수 있도록 조정하는 것이 중요하다.

이러한 다중 에이전트 시스템의 조정기법에는 일련의 메시지를 교환하는 프로토콜이 필요한데, 그 중 계약망 프로토콜은 분산된 문제(distributed problem)를 해결하는데 있어 에이전트들 사이의 통신을 하기 위한 도구중 하나로서 제안되었다[4].

계약망 프로토콜은 에이전트들이 계약에 의하여 분산된 문제를 해결하기 위하여 협상하고 통신하는 메커니즘을 제공한다[3]. 커맨드 콘솔은 에이전트들에게 수행될 필요가 있는 작업을 알리고, 에이전트들은 공지된 작업들을 수행하기 위해 bid를 만들어서 보내면 관리자는 에이전트들이 제출한 bid를 평가하여 최상의 에이전트를 선택하여 계약을 체결하게 된다[4,5].

2.3 계약망 프로토콜을 통한 연동

2.3.1. 계약망 프로토콜의 동작



<그림 1> 계약망 프로토콜의 연동 구조

<그림 1>과 같이 먼저 내부 네트워크로 패킷이 유입되면 커맨드 콘솔은 모든 침입 탐지 에이전트들에게 입찰을 위한 메시지를 브로드캐스트 하게 된다. 이 메시지를 받은 에이전트들은 커맨드 콘솔에게 bid 메시지를 보내게 되고, 이 bid메시지를 가지고 선택 알고리즘에 의해 침입을 탐지할 에이전트가 선택되고 선택된 에이전트에게 award 메시지와 함께 패킷 정보를 담은 데이터를 보내게 되면, 선택된 에이전트는 이 데이터를 가지고 침입을 탐지 하게 된다.

2.3.2 에이전트 선택 알고리즘

커맨드 콘솔에서 어떤 에이전트를 선택할 것인가가 본 연구에서 중요한 부분인데 기존의 연구[9]에서는 각 에이전트가 bid 데이터의 loading 필드의 값이 임계값을 넘지 않은 경우에 bid 메시지를 중앙 콘솔에 보내게 되는데 우선적으로 expertise 필드의 값을 기준으로 정렬하여 가장 큰 값을 갖는 에이전트를 선택한다.

```
Let bidi be bids
Set bid_list = empty set
Let bid_list = ( bid1, bid2,..., bid n ) be a list of bids
for i = 1 to n
  if loading of bidi >= threshold value
    Delete bidi from bid_list
Sort bid_list by expertise in descending order
if the number of bid including the greatest value of expertise >= 2 then
{
  Delete bids from bid_list except bids including the greatest value of expertise
  Sort bid_list including bids of the same expertise by experience in descending order
  if the number of bid including the greatest value of experience >= 2 then
  {
    Delete bids from bid_list except bids including the greatest value of experience
    Sort bid_list including bids of the same experience by loading in ascending order
  }
}
Select agent from bid_list(the first element)
```

<그림 2> 기존 연구의 선택 알고리즘

만약 expertise의 값이 같은 에이전트가 존재하면 그 에이전트 중에 experience 필드의 값을 기준으로 다시 정렬하여 역시 가장 큰 값을 가진 에이전트를 선택한다. 여기서, experience 값마저 같은 에이전트가 존재한다면 마지막으로 loading 필드의 값을 기준으로 정렬하여 가장 작은 값을 가진 에이전트를 선택하게 된다(그림 2).

2.4 DEVS 형식론

DEVS 형식론은 집합 이론에 근거하여, 연속적인 시간상에서 발생하는 이산 사건 시스템을 시뮬레이션하기 위해 정립된 모델링 방법론이다. 이는 모델의 구조와 행동을 시뮬레이션 수행으로부터 추상화시키기 위해 모델을 집합 이론적 방법으로 이용한 것으로, 시스템을 계층적(hierarchical)이고 모듈화(modular)된 형식으로 기술한다[10].

DEVS에서는 기본 모델(basic model)과 결합 모델(coupled model)을 정의한다. 기본 모델은 시간 명세 상태 천이 레벨(timed state transition level)에서 시스템의 동작을 표현하는 모델로서 다음의 항으로 명세할 수 있다.

$M = < X, S, Y, \delta_{int}, \delta_{ext}, \lambda, ta >$

X : 입력 사건 집합

S : 상태들의 집합

Y : 출력 사건 집합

δ_{int} : $S \rightarrow S$ 내부 상태 전이 함수

δ_{ext} : $Q \times X \rightarrow S$ 외부 상태 전이 함수

λ : $S \rightarrow Y$ 출력함수

ta : $S \rightarrow \mathbb{R}^+$ 시간 진행 함수

결합 모델은 시스템 구성 요소간의 상호작용을 표현하기 위한 모델로서 기본 모델이나 결합 모델로 기술된 구성 요소 모델들을 연결하여 만든 모델이다. 이 모델은 다음과 같은 항으로 명세가 가능하다.

$N = < X, Y, D, \{M_d \mid d \in D\}, EIC, EOC, IC, Select >$

X : 입력 사건 집합

Y : 출력 사건 집합

D : 구성 요소 이름의 집합

M_d : DEVS 모델의 구성 요소

EIC : 외부 입력 관계

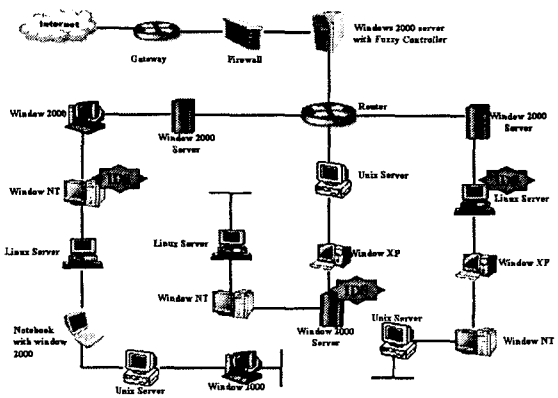
EOC : 외부 출력 관계

IC : 내부 입출력 관계

$Select$: $2^D - \{ \} \rightarrow D$

3. 보안 모델의 설계

3.1 대상 네트워크의 설계



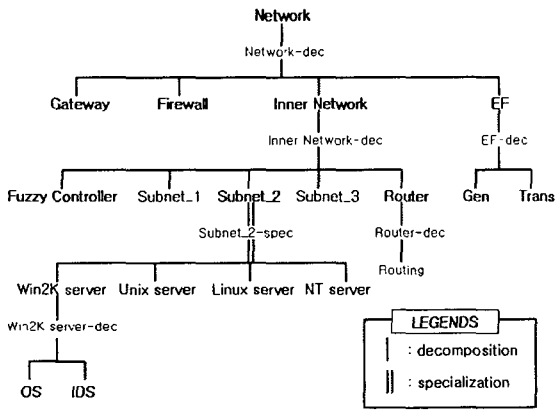
<그림 3> 대상 네트워크 구성도

시뮬레이션의 환경 구축에 있어서 대상 네트워크의 설계는 시뮬레이션의 결과가 실 시스템에 반영될 수 있는지를 판단하는 기준이 될 수 있다.

위의 <그림 3>은 3개의 서브넷을 갖는 대상 네트워크의 구성도이다. 네트워크 구성 요소로 라우터, 게이트웨이, 그리고 방화벽이 있으며, 내부 네트워크에는 각종 어플리케이션 서버들과 호스트들이 있고, 각 서브넷 마다 하나의 IDS가 장착되어 있다.

3.2 대상 네트워크의 SES

<그림 4>는 대상 네트워크의 SES(System Entity Structure)를 나타낸 것이다. 각 모델들은 계층적으로 분할(decomposition) 및 분류(specialization)의 관계를 갖고 있으며, 다음 장에서 하위 모델들의 기능에 대하여 설명하겠다.



<그림 4> 대상 네트워크의 SES

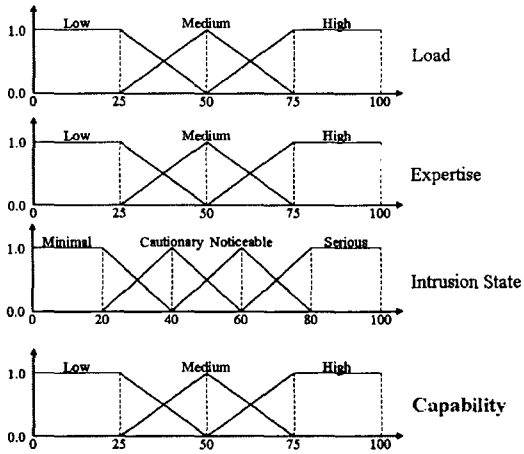
3.3 퍼지 컨트롤러의 설계

3.3.1. 퍼지 컨트롤러의 제안 및 구성

최근에는 웹 서버에 대한 공격보다는 침입 탐지 시스템 자체에 대한 공격이 더 많아졌다. 간단하고 단순한 공격 패킷들을 무수히 많이 보냄으로써, 탐지하고 대응하는 과정을 반복하게 하여, 실제로 중요한 공격에는 대처하지 못하게 하는 것이다. 따라서 대량의 트래픽에서 침입이 발생할 때, 이를 얼마나 효율적으로 탐지할 수 있는가가 침입 탐지 시스템의 성능을 측정하기 위한 중요한 요인이 된다. 이러한 문제를 해결하기 위해서는 다수의 IDS가 트래픽을 공유하도록 하는 것이 중요하다.

본 연구에서는 기존의 에이전트 선택에 있어서 전문성에 따라 한 에이전트로 작업이 편중되는 한계를 갖는 것을 극복하기 위한 퍼지 컨트롤러를 제안하였다.

에이전트 선택을 위한 퍼지 컨트롤러는 퍼지 규칙 기반 시스템(Fuzzy Rule-based System)으로 구성되는데[11], 입찰한 에이전트의 전문성(Expertise)과 침입 상태(Intrusion State), 그리고 부하(Load)를 입력으로 퍼지 추론을 수행하여, 능력(Capability)을 출력한다. 시스템의 입출력에 대한 멤버십 함수(Membership Function)는 <그림 5>와 같다.



<그림 5> 입출력에 대한 멤버십 함수

본 시스템은 총 36개의 퍼지 IF THEN 규칙(그림 6)을 사용하며, 실험에서는 네트워크 IDS의 수를 3개로 한정하고, 동일 시드에서 10,000개의 패킷을 발생시켜, 퍼지 컨트롤러를

적용한 경우와 기존의 선택 알고리즘을 사용하였을 때를 비교하였다.

Rule 13:
IF *Loading=Low* ∧ *Expertise=Medium* ∧ *IS=Cautionary*
THEN *Capability=Low*

Rule 14:
IF *Loading=Medium* ∧ *Expertise=Medium* ∧ *IS=Cautionary*
THEN *Capability=Medium*

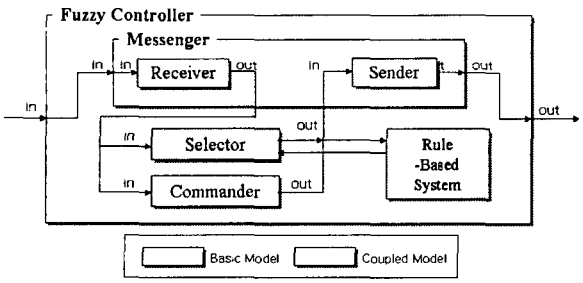
Rule 15:
IF *Loading=High* ∧ *Expertise=Medium* ∧ *IS=Cautionary*
THEN *Capability=Medium*

Rule 16:
IF *Loading=Low* ∧ *Expertise=High* ∧ *IS=Cautionary*
THEN *Capability=Medium*

<그림 6> Fuzzy Rules

3.3.2 퍼지 컨트롤러 모델

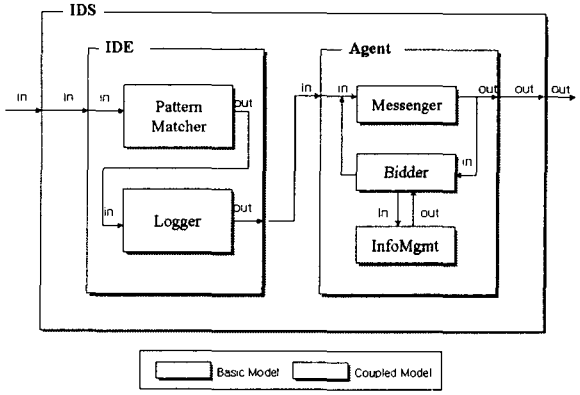
계약망 프로토콜에서 모든 IDS 모델의 에이전트를 통제하게 되는 퍼지 컨트롤러 모델의 구조도는 <그림 7>과 같다.



<그림 7> Fuzzy Controller 모델의 구조도

Messenger 모델은 컨트롤러로 들어오거나 나가는 모든 메시지의 송수신을 관리하는데 크게 Receiver와 Sender로 구성된다. 이는 패킷이 유입되거나 다른 에이전트들로부터 들어오는 메시지를 받고, 생성된 메시지를 다른 에이전트들에게 보내는 역할을 담당한다. Selector 모델은 각각의 에이전트들에게서 받은 Bid를 가지고 퍼지 규칙에 따라서, 최상의 에이전트를 선택하는 역할을 한다. Commander 모델은 IDS를 통제하는 메시지를 결정하게 된다.

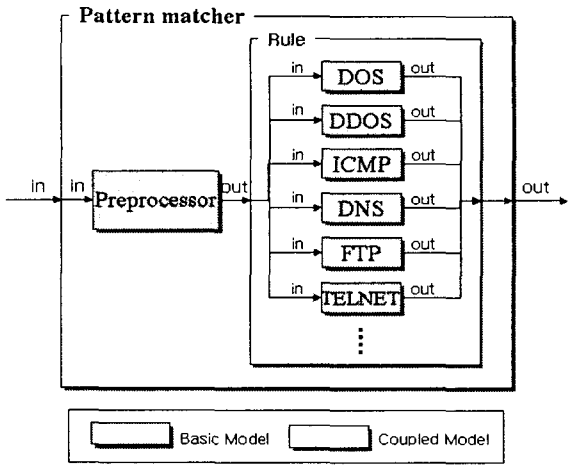
3.3.3 IDS 모델



<그림 8> IDS모델의 구조도

IDS 모델은 크게 침입을 탐지하는 IDE 모델과 메시지 송수신 및 에이전트를 선택하는 Agent 모델의 커플링으로 이루어져 있다.

IDE 모델은 침입 탐지 엔진 부분으로 Pattern Matcher 모델과 Logger 모델로 이루어져있는데, Pattern Matcher 모델(그림 9)에서는 규칙 기반의 전문가 시스템을 이용하여, 입력된 패킷 데이터를 규칙과 패턴의 매칭 과정을 통하여 침입을 탐지하게 된다. 이렇게 침입을 탐지한 결과 및 정보는 Logger 모델에 로그로 기록되게 된다.



<그림 9> Pattern Matcher 모델의 구조도

Agent 모델은 크게 Messenger, Bidder, InfoMgmt 모델로 이루어져 있는데, Messenger 모델은 퍼지 컨트롤러 모델에서처럼 각종 브로드 캐스팅, 멀티 캐스팅, 유니 캐스팅의 방법으로 메시지를 주고받는다. Bidder 모델에서는 에이전트의 정보를 관리하고 있는 InfoMgmt 모델과 통신하여 Bid를 만들어 주면, Messenger 모델을 통하여 다른 에이전트 또는 퍼지 컨트롤러와 통신할 수 있게 된다.

4. 시뮬레이션 결과

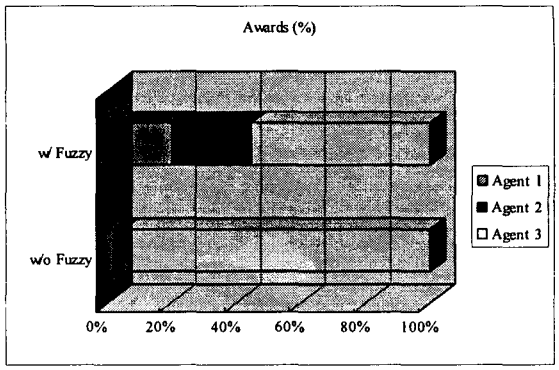
4.1 시뮬레이션 방법 및 성능 지표

본 연구를 위한 시뮬레이션을 두 가지 경우에 대하여 수행하였는데, 한 가지 경우는 기존의 선택 알고리즘을 사용하였을 때의 침입 탐지 결과이고, 다른 한 가지는 퍼지 컨트롤러를 적용하였을 경우에 대한 시뮬레이션 결과이다.

이번 연구에서는 시뮬레이션의 성능 지표를 얻기 위해서 침입 탐지 시간과 침입 오판율을 성능 지표로 설정하였다. 침입 에러 비율은 false positive와 false negative로 구분하는데 false positive 오판율은 침입이 아닌 것을 침입으로 판단하는 경우의 정도를 나타내고, false negative 오판율은 침입인 것을 침입으로 탐지하지 못하는 경우의 정도를 나타낸다.

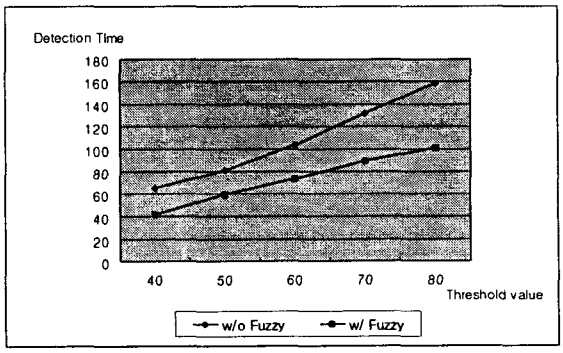
4.2 시뮬레이션 결과 및 분석

먼저, 퍼지 컨트롤러에서 전문성이 서로 다른 3개의 에이전트가 입찰했을 때에, 어떻게 작업을 할당 하는지를 퍼지 규칙 기반 시스템을 적용하였을 때와 그렇지 않았을 때를 비교하여 보면 <그림 10>과 같다.



<그림 10> 전문성이 서로 다른 에이전트가 입찰했을 때의 awards의 비율

퍼지를 적용하게 되면, 에어전트의 전문성이 다르다고 하더라도 한 에이전트에게만 작업이 할당되어서 부하가 더 높아지는 것과 달리, 전문성 뿐 만 아니라 다른 요소들도 고려하여 다른 에이전트들로도 골고루 부하가 분산되어서 더 나은 로드 밸런싱 기능을 수행함을 볼 수 있다.

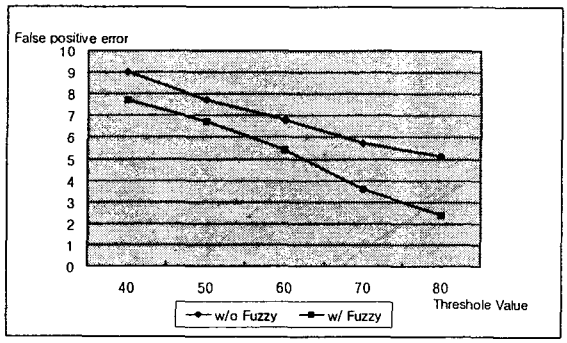


<그림 11> mailbomb 공격의 탐지 시간

<그림 11>은 최종적으로 침입을 탐지 하는데 에 있어서 mailbomb 공격의 탐지를 위한 임계값이 40, 50, 60, 70, 80 으로 증가함에 따라, 계약망 프로토콜을 적용한 다중 침입 탐지 시스템에서 퍼지를 적용하지 않았을 때보다 퍼지를 적용하였을 때, 더 빠르게 침입을

탐지 하는 것을 보여 준다.

여기서 mailbomb 공격이란 DoS 공격의 한 종류로써 많은 수의 메일을 메일 서버에 보냄으로써 메일 서버가 정상적인 메일을 처리하지 못하도록 방해하는 공격이다.



<그림 12> mailbomb 공격의 false positive 오판율

<그림 12>는 침입 탐지의 성능 지표인 false positive 오판율을 탐지 임계값이 증가함에 따라 나타낸 것으로, 퍼지를 적용하지 않았을 때보다 퍼지를 적용했을 때가 침입 탐지 시스템의 성능이 더 뛰어나며, false positive 오판율을 감소시킬 수 있다. 또한 임계값이 증가함에 따라 침입이 아닌 것을 침입으로 판단하는 비율도 낮아지게 되는 것을 볼 수 있다.

5. 결론 및 향후과제

네트워크 상에서의 침입 시도는 해가 갈수록 증가되고 다변화되고 있으며, 악의적인 사용자들에 의한 독창적이고 새로운 침입 방식의 개발은 침입 탐지에 대한 어려움을 증가시키고 있다.

이러한 상황에서 침입 탐지 시스템은 보안 시스템으로서의 역할을 잘 해내야 할 뿐더러, 그 필요성과 효용성이 잘 평가되어야만 할 것이다.

본 연구진은 시뮬레이션을 위하여 몇 가지 성능 지표를 설정하고 네트워크 보안을 위한 DEVS 기반의 네트워크 보안 시뮬레이션 환경을 구축하였으며, 다중 침입 탐지 시스템의 연동을 위하여 계약망 프로토콜을 적용하였다. 또한, 계약망 프로토콜의 적용 과정에 있어서 퍼지 규칙 기반 시스템을 사용하여, 에이전트들 사이에 작업의 분산이 잘 이루어지도록 하였으며, 따라서 기존보다 더 나은 로드 밸런싱 기능을 수행하는 것을 확인하였으며, 오판율(False rate)이 낮아지고, 침입 탐지 시간도 빨라지는 등 성능을 향상시킬 수 있었다.

향후 과제로는 다양한 보안 시뮬레이션을 수행할 수 있는 범용 네트워크 보안 시뮬레이션 환경의 구축이 필요하며, 침입을 탐지하는 과정에 적합한 알고리즘의 개발과 더 큰 네트워크 상에서의 침입 탐지를 위하여 고 수준의 프로토콜의 개발 또한 필요할 것이다.

참고문헌

[1] 한국정보보호학회, "차세대 네트워크 보안 기술," 한국정보보호진흥원, 2002.

[2] K. M. Sim, S. K. Shiu, and B. L. Martin, "Simulation of a Multi-agent Protocol for Task Allocation in Cooperative Design," Proc. of IEEE SMC '99 Int'l Conf., vol. 3, pp. 95-100, 1999.

[3] *J. Yang et al.* "Coordination of Distrbuted Knowledge Networks Using Contract Net Protocol," Information Technology Conf., IEEE, pp. 71-74, 1998.

[4] R. Smith, "The Contract Net Protocol: High-level Communication and Control in a distributed problem solver," IEEE Transactions on Computers, vol. C-29, no. 12, pp. 1104-1113, December. 1980.

[5] H. D. Parunak, "Manufacturing Experience with the Contract Net," In Research Notes in Artificial Intelligence: Distributed

Artificial Intelligence, vol. 1, pp. 285-310, Morgan Kaufmann 1987.
[6] H.S.Seo and T.H.Cho, "An application of blackboard architecture for the coordination among the security systems", simulation Modeling Practice and Theory, Elsevier Science B.V., vol.11, issues 3-4, pp. 269-284, Jul. 2003
[7] R. Base, "Intrusion Detection," Macmillan Technical Publishing, 2000.
[8] E. Amoroso, "Intrusion Detection : An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response," Intrusion.Net Books, 1999.
[9] K. J. Suh, and T. H. Cho, "Application of Contract Net Protocol to the Design and Simulation of Network Security Model," Int'l Conf. of Korea Intelligent Information System Society, pp. 197-206, 2003.
[10] B. P. Zeigler, H. Praehofer, and T. G. Kim, "Theory of Modeling and Simulation", 2nd Ed., Academic Press, 2000.
[11] J. Yen and R. Langari, "Fuzzy Logic ; Intelligence, Control, and Information", Prentice Hall, 1999.

주 작 성 자 : 이 진 아
논문투고일 : 2004. 10. 11
논문심사일 : 2004. 10. 19(1차), 2004. 10. 19(2차), 2004. 10. 20(3차)
심사판정일 : 2004. 10. 20

● 저자소개 ●

이진아

2002 성균관대학교 전기전자 및 컴퓨터공학부 학사

2004 성균관대학교 전기전자 및 컴퓨터공학과 석사과정

관심분야 : 네트워크 보안, 모델링 및 시뮬레이션, 인공지능

조대호

1983 성균관대학교 전자공학과 학사

1987 University of Alabama 전자공학과 석사

1993 University of Arizona 전자 및 컴퓨터공학 박사

1993~1995 경남대학교 전자계산학과 전임강사

1995~1999 성균관대학교 전기전자 및 컴퓨터공학부 조교수

1999~2002 성균관대학교 전기전자 및 컴퓨터공학부 부교수

2002~현재 성균관대학교 정보통신공학부 부교수

관심분야 : 모델링 및 시뮬레이션, 네트워크 보안, 지능 제어, ERP