論文
4-12-10

연동 구조 내의 추론 성능 향상을 위한 RETE 알고리즘의 적용 (An Application of RETE Algorithm for Improving the Inference Performance in the Coordination Architecture)

서희석 (Hee-Suk Seo)[1]

요약

오늘날의 네트워크는 다양한 애플리케이션이 수행되고 있는 많은 수의 서버와 라우터들로 구성되어 있다. 본 논문에서는 침입 탐지 에이전트와 방화벽 에이전트가 계약망 프로토콜(Contract Net Protocol)에 의해서 서로 연동할 수 있는 구조를 디자인하고 구축하였다. 계약망 프로토콜은 분산 시스템과 같은 이기종의 컴퓨터 시스템의 효과적인 연동을 위한 방법으로서 여러 에이전트들이 모여 서로 협력하며 하나의 문제를 해결하게 된다. 계약망 프로토콜 내의 커멘드 콘솔은 매니저로서 침입 탐지를 수행하는 계약자들을 수행시키거나 제어하는 역할을 수행한다. 지식 기반의 네트워크 보안 모델링을 위해서 각 모델은 계층적으로 잘 구성된 DEVS (Discrete EVent system Specification)에 의해서 구성하였다. 본 논문에서는 계약망 프로토콜에 의해서 운용되는 지식 기반의 침입 탐지 에이전트의 추론 주기를 향상시키기 위한 rete 패턴 매칭 알고리즘을 적용하여 시뮬레이션을 수행하였다. 본 연구는 rete 패턴 매칭 알고리즘을 사용하여 계약망 프로토콜의 성능과 특성을 평가해 본다.

Abstract

Today's network consists of a large number of routers and servers running a variety of applications. In this paper, we have designed and constructed the general simulation environment of network security model composed of multiple IDSs agent and a firewall agent which coordinate by CNP (Contract Net Protocol). The CNP, the methodology for efficient integration of computer systems on heterogeneous environment such as distributed systems, is essentially a collection of agents, which cooperate to resolve a problem. Command console in the CNP is a manager who controls the execution of agents or a contractee, who performs intrusion detection. In the knowledge-based network security model, each model of simulation environment is hierarchically designed by DEVS (Discrete EVent system Specification) formalism. The purpose of this simulation is the application of rete pattern-matching algorithm speeding up the inference cycle phases of the intrusion detection expert system. we evaluate the characteristics and performance of CNP architecture with rete pattern-matching algorithm.

Keywords : coordination, knowledge-based system, agent, IDS, modeling.

논문접수 : 2003. 12. 10.
심사완료 : 2003. 12. 16.

1) 정회원 : 성균관대학교 정보통신공학부 박사과정

1. 서론

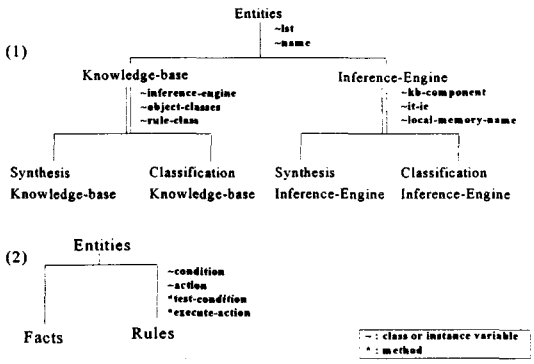
현대 사회는 인터넷 등의 정보통신망의 급속한 반전과 함께 정보가 국가 경쟁력의 원천이 되는 정보화 시대로서 정보화의 정도가 국가의 경제 및 사회의 발전 척도를 나타낸다고 해도 과언이 아니다. 하루가 다르게 정보화가 가속화되고 있으며 정보화 기술 역시 빠르게 진보하고 있다. 그러나 정보화가 급속히 진전됨에 따라 반대급부로 정보에 의한 혹은 정보에 대한 피해가 속출하고 있으며, 해킹 및 바이러스 유포 등의 정보 범죄가 기승을 부리고 있는 실정이다. 아무리 좋은 정보를 가지고 있다 하더라도 정보에 대한 안전한 유통 및 신뢰성, 즉 정보에 대한 보안이 이루어지지 못한다면 정보화의 가치 및 의미를 상실하게 된다. 이러한 보안상의 문제를 해결하기 위해 많은 기관에서 네트워크 보안 요소인 침입탐지 시스템과 침입차단 시스템을 도입하여 운용하고 있다. 침입탐지의 초기에는 외부로부터 보호하고자 하는 시스템마다 단일 호스트 기반인 침입탐지 시스템을 사용하였는데 많은 문제점이 발생되었다. 문제점을 보완하고 탐지에 대한 성능을 향상시키기 위해서 네트워크를 기반으로 한 다중 침입탐지 시스템을 도입하게 되었다. 다중 침입탐지 시스템은 분산 시스템의 이론을 적용한 다중 호스트 침입탐지 시스템으로 네트워크에 분산된 에이전트들에게 작업을 분산시키므로 시스템 부하를 감소시켜 탐지의 속도를 향상시키고 발생된 침입에 알맞은 에이전트를 선택하게 하여 탐지의 성능을 향상시킬 수 있다. 특별히 다중 에이전트의 연구에서 분산 인공지능의 새로운 기술에 대한 연구가 인공지능의 연구에서 중요한 분야가 되고 있으며 본 논문에서는 시스템의 연동을 위해 계약망 프로토콜을 적용할 것이다 [1-3].

계약망 프로토콜은 분산된 에이전트들 중에서 bidding의 과정을 통해서 최상의 에이전트를 선택하고 선택된 에이전트는 서비스를 제공 한다 [5-7]. 이러한 작업의 분산을 통해 각 에이전트들은 효과적으로 주어진 작업을 처리한다. 또한 자신이 처리하지 못하는 작업의 경우는 다른 에이전트에게 의뢰하여 처리하므로 자신이 처리할 수 없는 작업의 처리도 가능하다. 이와 같은 특성을 침입 탐지에 적용하게 되면 신속하고 정확한 탐지가 가능하며 무엇보다도 새로운 침입을 탐지하는 능력을 향상시킬 수 있다.

본 연구진은 침입 탐지 시스템에 전문가 시스템 (Expert System)을 적용하고 그 추론 과정에 있어서 효과적인 알고리즘을 선택하여 향상된 성능의 침입 탐지 시스템의 모델을 설계할 뿐만 아니라 네트워크에 분산된 침입 탐지 에이전트들과 침입 차단 시스템의 연동을 위하여 계약망 프로토콜을 적용한 시스템 환경을 구축할 것이다. 또한 이산 사건 시뮬레이션을 수행하기 위해 체계적으로 잘 정립된 이론인 DEVS 형식론으로 기존의 모델링 기법이 갖는 한계를 극복하여 대규모 시스템에 적합하도록 보안 시스템을 모델링하여 범용 보안 시뮬레이션 환경을 구축할 것이다 [8].

2. 관련 연구

2.1 전문가 시스템



<그림 1> 전문가 시스템의 구성
<Figure 1> Structure of Expert System

<그림 1>은 전문가 시스템의 구성 요소를 보여주고 있다. <그림 1>의 (1)은 전문가 시스템을 구성하는 구성 요소인 지식 베이스 (Knowledge Base)와 추론 기관 (Inference Engine)을 보여 주고 있다. 지식 베이스는 해결하려는 문제의 성격에 따라 Synthesis Knowledge Base와 Classification Knowledge

Base로 구별 될 수 있다. 추론 기관도 해결하고자 하는 문제의 성격에 따라 Synthesis Inference Engine과 Classification Inference Engine으로 구별 될 수 있다. <그림 1>의 (2)는 지식 베이스를 구성하는 사실 (Facts)과 규칙 (Rules)을 보여 주고 있다.

2.2 계약망 프로토콜

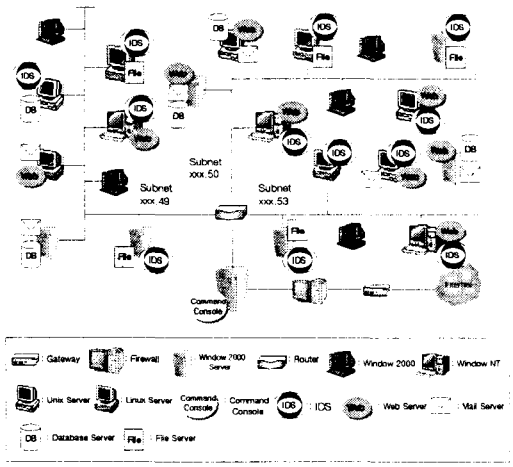
분산 문제 해결 방법은 많은 지식원들의 분산화와 이러한 에이전트들이 서로 느슨하게 연결됨으로써 서로 협력하여 문제를 해결하는 방법을 제안한다. 각 지식원들은 전체 문제를 해결하기 위한 충분한 지식을 갖고 있지 못하므로 서로 협력하여 문제를 해결하게 된다. 지식원들이 서로 분산되어 있다는 의미는 자신들이 다루는 데이터와 제어가 위치적으로나 논리적으로 분산되어 있다는 것을 의미하고 느슨하게 연결되었다는 의미는 서로 통신하는데 많은 시간을 보내기 보다는 각자가 문제를 해결하기 위해서 연산을 하는데 많은 시간을 소비함을 의미한다 [4].

계약망 프로토콜은 분산된 문제를 해결하는데 있어 통신하고 조정하기 위한 도구로서 제안되었다 [5]. 계약망 프로토콜의 사용은 분산 감지 시스템과 분산 전달 시스템을 위해서 시도되었다 [6]. 계약망 프로토콜은 에이전트들이 계약(contract)에 의하여 분산된 문제를 해결하기 위하여 협상하고 통신하는 메커니즘을 제공한다 [7]. 에이전트들은 수행될 필요가 있는 작업을 알리고 다른 에이전트들에 의해 공지된 작업들을 수행하기 위해 bid를 만들고, Command Console은 각 에이전트들이 제출한 bid를 평가하여 계약을 체결하게 된다. 계약망 프로토콜의 적용은 다중 침입 탐지 시스템에 있어서 서로 보완하고 협력하여 탐지의 성능을 향상시키고 정확도를 높일 수 있다.

3. 지식 기반 에이전트 환경

3.1 대상 네트워크의 설계

실시스템 수준의 시뮬레이션 환경 구축에 있어서 대상 네트워크의 설계는 시뮬레이션의 결과가 실시스템에 반영될 수 있는지를 판단하는 기준이 될 수 있다. <그림 2>는 3개의 서브넷을 갖는 대상 네트워크의 구성도이다. 각 네트워크는 49, 50, 53 네트워크로 이루어지고 각 네트워크는 다양한 서버 및 호스트로 구성된다. 내부 네트워크에는 web server, mail server, database server 및 file server를 설치한 호스트들이 있고 각 서브넷 별로 4개의 IDS가 장착되어 있다. 그리고 네트워크 구성요소로서 Router, Gateway, Firewall, Command Console이 구성되어 있다.

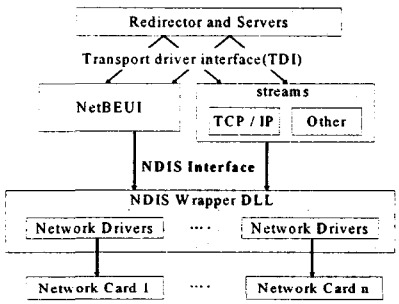


<그림 2> 대상 네트워크 구성도
<Figure 2> Structure of Target Network

각 모델들은 DEVS 기반의 기본 모델과 결합 모델로 구성되어 있으며, 대상 네트워크 모델 이외에 시뮬레이션 수행을 위해 EF (Experimental Frame) 모델을 추가하였다. EF 모델은 Gen 모델과 Trans 모델로 구성된다. Gen 모델은 실제 네트워크에서 capturing한 패킷 데이터를 바탕으로 시뮬레이션을 위한 패킷을 생성하여 대상 네트워크로 보낸다. Trans 모델은 시뮬레이션을 통해 얻은 결과를 분석하고 시뮬레이션을 통제한다.

3.2 패킷 생성 모델

본 연구진이 구성한 시뮬레이션 환경은 실제 보안 시스템의 환경과 가깝도록 구성하기 위해 시뮬레이션의 입력으로 사용되는 패킷을 네트워크에서 수집한 실제 패킷을 사용하였다. 윈도우즈 운영 체제는 네트워크 드라이버 인터페이스 사양 (Network Driver Interface Specification)이라는 인터페이스 환경을 제공한다. 이러한 구조는 네트워크 드라이버를 다양한 전송 프로토콜의 세부 구조로부터 보호하고 여러 프로토콜을 네트워크 드라이버로부터 보호하기 위함이다.

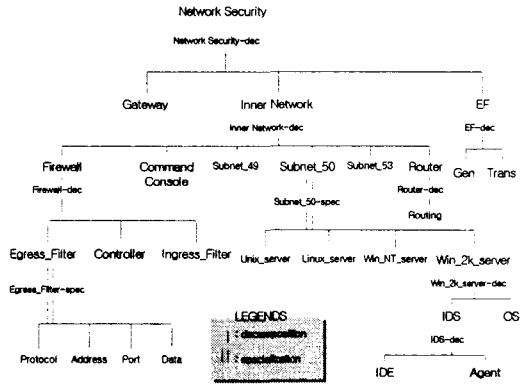


<그림 3> NDIS를 사용한 패킷 수집
<Figure 3> Packet Collection using NDIS

시뮬레이션의 입력으로 사용되는 패킷은 <그림 3>에서와 같이 네트워크에서 수집한 패킷을 사용하게 된다. 네트워크에서 수집된 패킷은 데이터 링크 계층의 데이터로 이 데이터를 대상 네트워크의 Gen 모델이 받게 된다. 패킷 Gen 모델은 네트워크에서 수집된 패킷을 data link, ip와 tcp 계층으로 분류한다. Gen 모델은 각 계층의 헤더 정보를 분석하고, 응용 계층에서 사용할 데이터를 분리하여 시뮬레이션의 입력으로 사용할 수 있는 형태로 만든다.

3.3 대상 네트워크의 SES

<그림 4>는 대상 네트워크의 SES (System Entity Structure)를 나타낸 것이다. 각 모델들은 계층적으로 decomposition 및 specialization 관계를 가지고 있으며 크게 Gateway 모델과 Inner Network 모델 및 EF 모델로 구성되어 있다. Inner Network 모델은 다시 Firewall 모델과 Command Console 모델, Subnet_49 모델, Subnet_50 모델, Subnet_53 모델 및 Router 모델로 구성되고 각 서브넷 모델은 Unix_server 모델, Linux_server 모델, Win_NT_server 모델 및 Win_2k_server 모델로 구성된다. 각 서버 모델은 IDS 모델과 OS 모델로 구성되며 IDS 모델은 다시 IDE 모델과 Agent 모델로 구성된다.



<그림 4> 대상 네트워크의 SES
<Figure 4> SES of Target Network

4. 계약망을 통한 에이전트의 연동

4.1 Command Console 모델

계약망 프로토콜에서 모든 IDS 모델과 Firewall 모델의 에이전트들을 통제하게 되는 Command Console 모델의 모듈과 각 모듈의 기능은 다음과 같다. Messenger 모델은 메시지의 송수신을 관리하는데 Receiver와 Sender로 구성된다. Receiver는 IDS에서 보낸 메시지를 받고 Sender는 Selector나 Commander에서 만들어진 메시지를 해당 IDS나 모든 IDS에게 unicast, multicast, broadcast의 방법으로 보낸다. Selector 모델은 모든 IDS가 보낸 bid로 내부 네트워크를 감시할 IDS를 선택한다. Commander 모델은 내부 네트워크의 상태에 따

라 IDS와 Firewall를 통제하는 메시지를 결정한다.

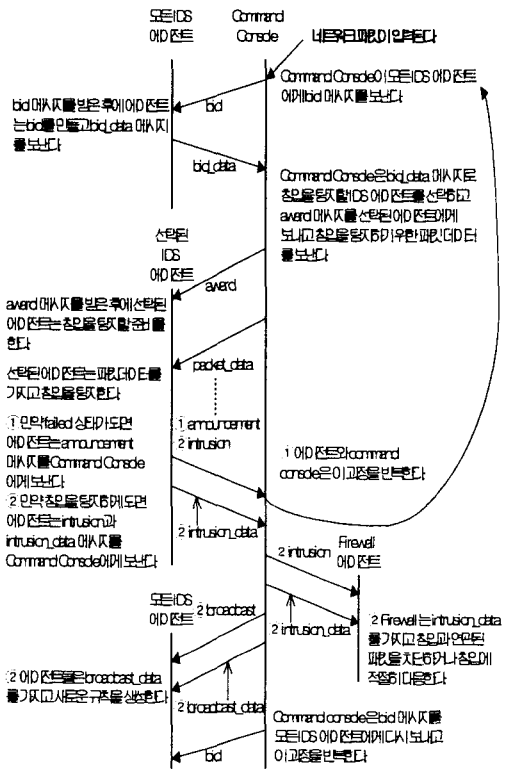
4.2 IDS 모델

Command Console에서 오는 패킷 데이터는 IDE (Intrusion Detection Engine) 모델에서 탐지하게 되고 컨트롤과 관련된 메시지는 IDE 모델을 통과하여 Agent 모델에서 처리하게 된다. 또한 IDE 모델에서 탐지하거나 처리된 메시지를 Agent 모델로 보내 처리하게 된다.

4.3 IDE 모델

Detector 모델은 Pattern_matcher와 Analyzer로 구성되는데 Pattern_matcher는 규칙 베이스 전문가 시스템을 적용하여 입력된 패킷 데이터를 규칙과 패턴 매칭의 과정을 통해 침입을 탐지하게 된다. 무엇보다도 rete 패턴 매칭 알고리즘[9]을 적용하여 전문가 시스템에서 가장 많은 시간을 소비하는 패턴 매칭의 시간을 단축시킬 수 있다. Analyzer는 통계적인 침입 탐지를 수행하는 모듈로 시스템 로그나 시스템 감사에 저장된 자료를 분석하여 침입을 탐지하게 된다. Response_Generator 모델은 Detector 모델에서의 침입 탐지 결과에 따라 IDS가 취할 행동을 결정하고 메시지를 보낸다. Logger 모델은 Detector 모델의 탐지과정에서 발생하는 모든 정보를 로그로 기록한다.

4.4 에이전트 간의 연동 과정



<그림 5> 메시지를 교환하는 연동과정
<Figure 5> Collaboration Process of Message Passing

침입을 탐지한 경우에는 선택된 에이전트가 intrusion 메시지를 Command Console에 보내고 intrusion_data 메시지를 보낸다. 이 메시지를 받은 Command Console은 Firewall에게 intrusion과 intrusion_data 메시지를 차례로 보내고 모든 침입 탐지 에이전트에게 broadcast 메시지와 침입에 대한 정보를 broadcast_data 메시지로 보낸다. 그런 다음 다시 bid 메시지를 보내고 위의 에이전트 선택과정을 반복한다. <그림 5>는 IDS, Command Console, Firewall 모델들이 메시지를 교환하는 연동과정을 순차적으로 표현하였다. Command Console은 계약망 프로토콜에서 IDS와 Firewall를 중앙에서 통제하는 중요한 역할을 수행하게 된다. 실제적으로

연동은 Command Console과 IDS 내부의 Agent 모델, Firewall 내부의 Controller 모델사이의 메시지 교환에 의해 이루어진다.

5. Rete 패턴 매칭 알고리즘의 적용

5.1 침입 탐지 전문가 시스템

침입을 탐지하는 전문가 시스템은 규칙의 집합인 지식 베이스, 추론을 수행하는 추론 엔진 그리고 사실을 저장하는 working memory로 구성된다. 추론 방식은 전향 추론 방식을 적용하는데 추론과정은 패턴 매칭, 충돌 해결 그리고 실행의 순서로 이루어진다. 각 규칙의 left-hand side는 규칙에서 if 부분과 일치하는 조건의 결합으로 구성되고 right-hand side 는 규칙에서 then 부분과 일치하는 일련의 행동들로 구성된다. 패턴 매칭은 규칙에서 LHS와 WM에 있는 사실들을 비교한다. 이 과정의 결과 만족된 규칙이 2개 이상인 경우는 충돌 셋이 구성된다. 다음에는 미리 정의된 충돌 해결 전략에 따라 충돌 셋에서 하나의 규칙을 선택하고 마지막으로 그 규칙의 일련의 행동들을 실행하여 WM에 있는 내용을 변화시킨다. WM는 초기상태에서 추론과정을 통해 규칙을 선택하고 최종적으로 침입을 탐지하게 된다.

다음은 침입 탐지 시스템이 추론과정에서 사용할 몇 가지 침입 탐지 규칙에 대한 예를 든 것이다. 규칙들은 DOS와 같이 각 규칙의 모듈별로 탐지가 이루어진다.

```
DOS Rules :

R1 :
if protocol = ip ∧ IPSrcAddr = EXTERNAL_NET ∧ IPDstAddr = HOME_NET ∧
fragbits = "M" ∧ dsize = 408 ∧ state = "passive"
then state = "vulnerable", p_count+=1

R2 :
if protocol = ip ∧ IPSrcAddr = EXTERNAL_NET ∧ IPDstAddr = HOME_NET ∧
fragbits = "M" ∧ dsize = 408 ∧ state = "vulnerable"
then p_count+=1

R3 :
if protocol = ip ∧ IPSrcAddr = EXTERNAL_NET ∧ IPDstAddr = HOME_NET ∧
fragbits = "M" ∧ dsize = 408 ∧ state = "vulnerable" ∧ p_count >= threshold
then state = "intrusion", msg("DOS Jolt attack")
```

```
ICMP Rules :

R15 :
if protocol = icmp ∧ IPSrcAddr = EXTERNAL_NET ∧ IPDstAddr = HOME_NET
∧ data = "|5783 6174 7365 7020 2d20 4210 4e65 7477|" ∧ itype = 8
then state = "intrusion", msg("ICMP PING WhatsupGold Windows)

R16 :
if protocol = icmp ∧ IPSrcAddr = EXTERNAL_NET ∧ IPDstAddr = HOME_NET
∧ dsize > 800
then state = "intrusion", msg("ICMP Large ICMP Packet")

Goal Rule :
if state = "intrusion" then passivate(), p_count = 0
```

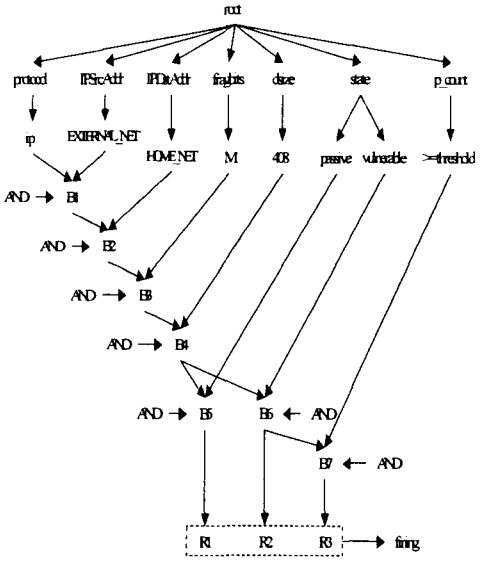
5.2 Rete 패턴 매칭 알고리즘

Rete 알고리즘은 규칙이 선택된 후에 충돌 셋을 다시 계산하기 위해서 요구되는 노력을 감소시키는 것에 의해 전향 추론 시스템(forward-chained rule system)의 속도를 향상시키는 알고리즘이다. Rete 알고리즘을 활용하면 침입 탐지 전문가 시스템의 추론과정에서 가장 많은 시간을 소비하는 패턴 매칭의 시간을 감소시켜 침입 탐지의 성능을 향상시킬 수 있다.

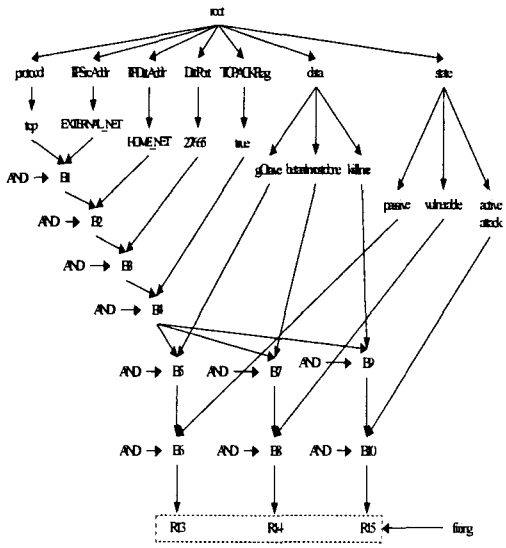
5.3 Rete 네트워크

Rete는 거대한 집합의 패턴을 거대한 집합의 오브젝트에 반복 없이 비교하는 매칭 알고리즘이다 [10]. Rete 알고리즘은 노드 (node)로 구성된 네트워크를 만드는 것에 의해서 구현되는데 root 노드를 제외한 노드들은 패턴을 나타내고 root에서 leaf까지의 경로는 규칙의 LHS를 나타낸다. 지식 베이스로부터 첨가되거나 제거되는 사실들은 노드로 구성된 네트워크에 의해 진행된다. 네트워크에서 가장 아래에 있는 터미널 노드들은 개별적인 규칙을 나타내는데 사실의 집합이 rete 네트워크의 터미널 노드에 이르렀을 때 특정한 규칙의 LHS에 있는 모든 테스트

를 통과한 것이며 이 집합은 activation이 된다. 만약 activation 집합으로부터 하나 이상의 사실을 제거하는 것으로 activation이 무효가 된다면 그 선택된 규칙은 RHS를 실행하게 된다. Rete 네트워크에는 크게 하나의 입력이 있는 노드와 두 개의 입력이 있는 노드가 있다. 하나의 입력이 있는 노드는 개별적인 사실에 대한 테스트를 수행하여 알파 메모리에 저장하고 두 개의 입력이 있는 노드는 사실들 상호간의 테스트를 수행하는 동시에 그룹핑 함수를 수행하여 베타 메모리에 저장한다. 이 시점에서 침입 탐지 전문가 시스템에 적용된 몇 가지 규칙들을 rete 알고리즘을 이용하여 구성한 rete 네트워크는 다음과 같다.



<그림 6> Jolt 공격의 rete 네트워크
<Figure 6> Rete Network of Jolt Attack



<그림 7> Trinoo의 rete 네트워크
<Figure 7> Rete Network of Trinoo Attack

<그림 6>은 DOS Jolt 공격을 탐지하는 규칙을 rete 네트워크로 구성하였다. root 노드로부터 터미널 노드인 규칙까지 알파 노드와 베타 노드를 AND 연산에 의해 그룹핑하여 구성하였으며 패킷 정보가 root 노드에 입력되면 각 패턴에 따라 노드를 이동하고 터미널 노드에 이르게 되면 해당 규칙을 적용하게 된다. <그림 7>은 DDOS Trinoo 공격을 탐지하는 규칙을 Rete 네트워크로 구성하였다.

6. 시뮬레이션

6.1 성능 지표의 설정

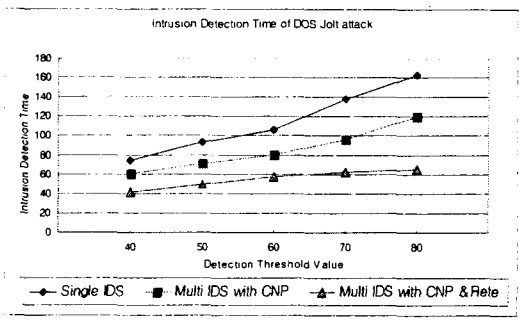
시뮬레이션의 결과를 평가하기 위하여 침입 탐지 시간과 침입 오판율을 성능 지표로 설정하였다. 침입 탐지 시간은 패킷 데이터 상에서 발생하는 침입을 침입 탐지 시스템이 탐지하는데 경과하는 시간을 나타낸다. 침입 오판율은 false-positive와 false-negative로 구분하는데 false-positive 오판율은 침입이 아닌 것을 침입으로 판단하는 경우의 정도를 나타내고

false-negative 오판율은 침입인 것을 침입으로 탐지하지 못하는 경우의 정도를 나타낸다.

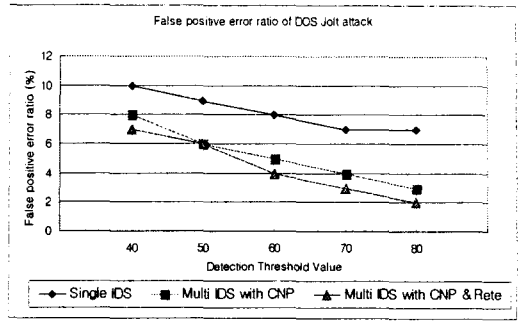
6.2 시뮬레이션 결과 및 분석

본 연구진은 단일 침입 탐지 시스템과 계약망 프로토콜을 적용한 다중 침입 탐지 시스템 및 rete 알고리즘과 계약망 프로토콜을 적용한 다중 침입 탐지 시스템에 대한 시뮬레이션을 수행하였다.

<그림 8>은 DOS Jolt 공격의 탐지를 위한 탐지 임계값이 40, 50, 60, 70, 80으로 증가함에 따라 세 가지 경우의 침입 탐지 시간의 변화를 나타낸다. 여기서 DOS Jolt 공격은 표준에 규정된 길이 이상으로 큰 IP 패킷을 전송함으로써 이 패킷을 수신하는 운영체제에서 이 비정상적인 패킷을 처리하지 못함으로써 서비스거부공격을 유발하도록 하는 방법이다. 시뮬레이션 수행 결과, 계약망 프로토콜을 적용한 다중 침입 탐지 시스템이 단일 침입 탐지 시스템보다 더 빠르게 침입을 탐지했으며 rete 알고리즘을 적용하면 탐지 속도가 더 향상되었다.

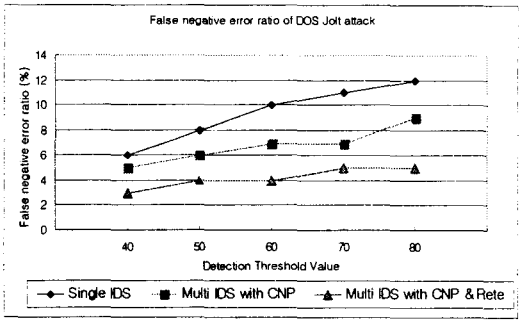


<그림 8> DOS Jolt 공격의 침입 탐지 시간
<Figure 8> Intrusion Detection Time of DoS Jolt Attack



<그림 9> DOS Jolt 공격의 false positive 오판율
<Figure 9> False Positive Error of DoS Jolt Attack

<그림 9>는 침입 탐지의 성능 지표인 false positive 오판율을 탐지 임계값이 증가함에 따라 나타낸 것으로 단일보다 다중 침입 탐지 시스템의 성능이 뛰어나고 Rete 알고리즘을 적용하면 false positive 오판율을 감소시킬 수 있다. 또한 임계값의 증가에 따라 침입이 아닌 것으로 침입으로 판단하는 비율이 낮아진다. <그림 10>은 false negative 오판율을 탐지 임계값이 증가함에 따라 측정한 것으로 단일보다 다중 침입 탐지 시스템의 오판율이 낮았으며 rete 알고리즘을 적용하면 성능이 향상되는 것을 알 수 있다. 그리고 임계값의 증가에 따라 침입을 침입으로 탐지하지 못하는 비율이 높아진다.



<그림 10> DOS Jolt 공격의 false negative 오판율
<Figure 10> False Negative Error of DoS Jolt Attack

7. 결론

앞으로 네트워크의 활용은 더욱 증가할 것이며 네트워크에서 교환되는 정보의 가치와 중요성 또한 증가할 것이다. 반면 네트워크를 악용하는 정보 유출이나 침입 사고의 발생 역시 증가할 것이다. 이러한 상황에서 침입 탐지 시스템은 하나의 보안 요소가 될 것이며 그 효용성과 필요성이 평가될 것이다. 본 연구진은 시뮬레이션을 통하여 몇 가지 성능 지표를 설정하고 네트워크 보안을 위한 DEVS 기반의 네트워크 보안 시뮬레이션 환경을 구축하였으며 다중 침입 탐지 시스템과 침입 차단 시스템의 연동을 위해 계약망 프로토콜을 적용하였다. 또한 실질적으로 침입을 탐지하게 되는 침입 탐지 전문가 시스템에 rete 패턴 매칭 알고리즘을 적용하여 성능을 평가하였다. 시뮬레이션을 통하여 단일 침입 탐지 시스템보다는 여러 개의 침입 탐지 시스템이 계약망 프로토콜에 의해 연동하는 다중 침입 탐지 시스템이 효과적으로 침입을 탐지하였으며 더 나아가 침입 차단 시스템과의 연동을 통해 네트워크를 강력하게 보호할 수 있다. 또한 침입 탐지 전문가 시스템의 추론 과정에 Rete 패턴 매칭 알고리즘을 적용하면 계약망 프로토콜을 적용한 다중 침입 탐지 시스템과 침입 차단 시스템의 성능을 월등히 향상시킬 수 있다.

향후 과제로는 다양한 보안 시뮬레이션을 수행할 수 있는 범용 네트워크 보안 시뮬레이션 환경의 구축이 필요하며 침입을 탐지하는 추론 과정에 적용될 효과적인 알고리즘의 구현이 필요할 것이다.

참고 문헌

[1] K. M. Sim, S. K. Shiu, and B. L. Martin, "Simulation of a Multi-agent Protocol for Task Allocation in Cooperative Design," IEEE SMC '99 Conference Proceedings. International Conference on, vol.3, pp. 95-100, 1999.

[2] Shungeng Hu, Li Zhang and Yixin Zhong, "Theories, Technology and Application of Multi-Agent Systems," Computer Science, Vol. 26, No.9, pp. 20-24, 1999.

[3] T. Sandholm, "An Implementation of the Contract Net Protocol based on Marginal Cost Calculations," in 11th National Conference on Artificial Intelligence (AAAI-93), Washington. DC, 1993.

[4] Alan H. Bond and Les Gasser, 「Distributed Artificial Intelligence」, Morgan Kaufmann Publisher Inc., 1998.

[5] Jihoon Yang, Raghu Havaldar, Vasant Honavar, Les Miller and Johny Wong, "Coordination of Distrbuted Knowledge Networks Using Contract Net Protocol," Information Technology Conference, IEEE, pp. 71-74, 1998.

[6] 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.

[7] H. van Dyke Parunak. Manufacturing Experince with the Contract Net. In Research Notes in Artificial Intelligence: Distributed Artificial Intelligence, Vol. 1, pp. 285 - 310, Morgan Kaufmann Publishers, 1987.

[8] H.S. Seo and T.H. Cho, "An application of blackboard architecture for the coordination among the security systems", Simulation Modelling Practice and Theory, Elsevier Science B.V., vol. 11, issues 3-4, pp. 269-284, Jul. 2003.

[9] V. Devedzic, D. Velasevic, "An architecture for real-time inference engines on personal computers", System Sciences, 1992. Proceedings of the Twenty-Fifth Hawaii International Conference on, vol. 1, pp. 619-630, 7-10 Jan. 1992.

[10] C. L. Forgy, "Rete: A fast algorithm for the many pattern/many object pattern match problem", Artificial Intelligence, vol. 19, pp. 17-37, 1982.

서희석

2000.2. 성균관대학교 산업공학과 졸업 (공학사).
2002.2. 성균관대학교 전기전자 및 컴퓨터공학부 졸업 (공학석사).
2002.3.~현재 성균관대학교 정보통신공학부 박사과정 재학 중.