오용 침입탐지 시스템에서 모바일 에이전트를 이용한 보안규칙 관리에 관한 연구

김 태 경[†] · 이 동 영[††] · 정 태 명[†††]

요 약

이 논문은 모바일 에이전트를 이용해서 보안규칙을 관리하는 방안을 제시하였다. 침입탐지 시스템(IDS : Intrusion Detection System)은 침입탐지 모델을 기반으로 비정상적인 행위 탐지(anomaly detection)와 오용 침입탐지(misuse detection)로 구분할 수 있다. 오용 침입탐지(misuse detection)는 알려진 공격 방법과 시스템의 취약점들을 이용한 공격들은 탐지가 가능하지만, 알려지지 않은 새로운 공격을 탐지하지 못한다는 단점을 가지고 있다. 이에 본 논문에서는, 계속적으로 인터넷 상을 이동하는 모바일 에이전트를 이용해서 안전하게 보안규칙을 관리하는 방안을 오용탐지의 단점을 해결하는 방안으로 제시하였다. 이러한 모바일 에이전트 메커니즘을 이용해서 보안규칙을 관리하는 것은 침입탐지 분야에서는 새로운 시도이며, 모바일 에이전트를 이용해서 보안규칙을 관리하는 방법의 유효성을 증명하기 위해서 기존의 방식과 작업부하 데이터(workload data)를 수식적으로 비교하였고, NS-2(Network Simulator)를 이용하여 시간에 대하여 시뮬레이션을 수행하였다.

A Study of Security Rule Management for Misuse Intrusion Detection Systems using Mobile Agent

Tae-Kyung Kim[†] · Dong-Young Lee[††] · Tai M. Chung[†††]

ABSTRACT

This paper describes intrusion detection rule management using mobile agents. Intrusion detection can be divided into anomaly detection and misuse detection. Misuse detection is best suited for reliably detecting known use patterns. Misuse detection systems can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. Therefore, the introduction of mobile agents to provide computational security by constantly moving around the Internet and propagating rules is presented as a solution to misuse detection. This work presents a new approach for detecting intrusions, in which mobile agent mechanisms are used for security rules propagation. To evaluate the proposed approach, we compared the workload data between a rules propagation method using a mobile agent and a conventional method. Also, we simulated a rules management using NS-2 (Network Simulator) with respect to time.

키워드 : 오용 침입탐지(Misuse Intrusion Detection), 모바일 에이전트(Mobile Agent), 보안규칙(Security Rules)

1. 서 론

컴퓨터 시스템을 보호하기 위한 보안 분야에서의 많은 노력들이 계속적으로 추진되고 있는 가운데, 한편으로는 컴퓨터의 수의 증가와 동시에 여러 가지 공격시도와 침입에 성공하는 공격의 횟수도 증가하고 있다. 이로 인해, 전 세계적으로 보안은 중요한 이슈가 되고 있다. 침입(Intrusion)은 시스템 자원에 대한 무결성(Integrity), 기밀성(Confidentiality) 또는 가용성(Availability)을 침해하는 행위를 말하며, 침입탐지 시스템(IDS : Intrusion Detection System)은 이러한 비인가된 사용자의 침입을 탐지하여 시스템 자원을 효과적으로 보호하는 시스템이다[1-2].

침입을 탐지하는 모델에 따라 오용 침입탐지(misuse detection)와 비정상행위 탐지(anomaly detection) 방법으로 구분할 수 있으며, 오용 침입탐지[3, 4] 기법은 알려진 공격 방법과 시스템의 취약점들을 이용하여 공격하는 행위들을 나타내는 침입 패턴을 정의하여 유지하고, 이 침입 패턴과 일치하거나 유사한 경우의 사건이 발견되는 경우 이를 침입이라 판단하는 방법이다. 비정상행위 탐지[3]는 정상적인 정보시스템의 행위에 대한 참조 모델을 만들어 넣고, 이 참조 모델을 벗어나는 행위를 침입이라 판단하는 방법이다. 현재 개발된 국내·외 대부분의 침입탐지 시스템(IDS)의 43%는 오용 침입탐지 모델을 채용하고 있으며, 7%는 비정상행위 탐지 방식을 그리고 17%는 오용탐지 방식과 비정

† 준 회 원 : 성균관대학교 대학원 정보통신공학부
†† 정 회 원 : 명지전문대학 정보통신과 교수
††† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2003년 3월 11일, 심사완료 : 2003년 8월 22일

상 행위 탐지 방식을 적용하고 있다[5].

오용탐지 방식의 단점은 앞서 언급한 바와 같이 알려진 공격에 대해서 이를 패턴으로 설정하고 이와 일치 하는 행위가 있을 경우 침입으로 한다. 따라서, 새로운 공격 방법이나 시스템의 취약성이 발견되었을시 이에 대한 침입을 판단하기 위한 보안 규칙의 갱신(security rules propagation)이 필요하다. 이에 본 논문에서는 오용 탐지 방식을 채용한 침입탐지 시스템에서 효율적인 규칙 갱신을 위하여 모바일 에이전트(Mobile Agent)를 이용함으로써 보다 침입탐지 시스템의 성능을 향상 시킬 수 있는 방법을 제시하고, 이를 대표적인 네트워크 시뮬레이터인 NS-2를 이용하여 본 논문에서 제시한 방법론을 시뮬레이션 하였다.

본 논문의 구성을 살펴보면, 2장에서는 관련연구와 모바일 에이전트에 대해서 살펴보고, 3장에서는 모바일 에이전트를 이용한 보안규칙 관리 방안(SRPM : Security Rules Propagation Method using mobile agent)에 대하여 상세설계 기술 및 시뮬레이션을 실시하였다. 그리고 4장에서는 결론 및 향후 연구 과제에 대하여 언급하였다.

2. 관련 연구

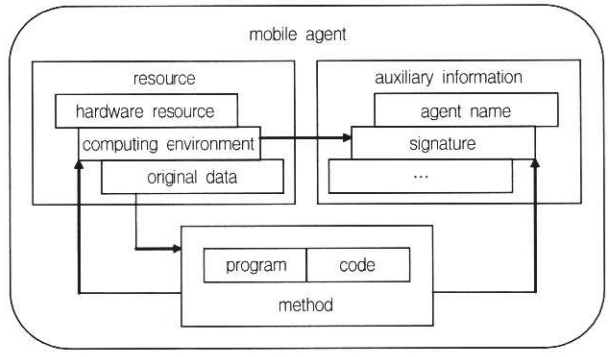
모바일 에이전트의 일반적인 특성 및 모바일 에이전트의 구성에 대해서 살펴보고, 이 분야에서 기존에 수행된 에이전트를 사용하는 침입탐지 시스템에 대하여 조사를 하였다.

2.1 모바일 에이전트

모바일 에이전트는 분산된 네트워크 환경에서 한 노드에서 다른 노드로 자체적으로 이동할 수 있는 독립적인 프로그램의 일종이라 할 수 있다. 전통적인 분산 기술인 Client-Server 모델이나 Code On Demand 모델과 비교해서 다음과 같은 장점을 가지고 있다.

- 사용자의 요구 조건을 충족시키기 위해 존재하는 자원을 능동적으로 사용할 수 있다.
- 네트워크 사용량에 대해서 능동적으로 조절 할 수 있다.
- 네트워크 고장시, 이에 대하여 적절한 조치를 취할 수 있다.
- 모바일 사용자를 지원할 수 있다.
- 상황에 맞는 서비스를 제공할 수 있다.

또한, 모바일 에이전트는 다음과 같은 여러 단계의 라이프 사이클을 가지고 있다. 각 단계들은 생성, 중지, 실행, 서비스 탐색, 새로운 호스트에 도착, 이동, 원래의 호스트로의 귀환, 종료 등으로 구성되어 있다. 그리고 모바일 에이전트는 크게 자원, 기능, 규칙정보 등의 세 부분으로 나누어 볼 수 있다. (그림 1)은 일반적인 모바일 에이전트의 구성을 나타낸 것이다[14].



(그림 1) 모바일 에이전트의 구성

자원(resource)은 하드웨어 자원, 컴퓨팅 환경 그리고 원본 데이터(original data)로 구성되어 있으며, 컴퓨팅 환경은 메소드(method) 모듈의 부호화된 에이전트의 연속된 상태를 의미한다. 메소드 모듈은 실제의 컴퓨팅 코드와 프로그램으로 구성되고, 부가정보(auxiliary information)에서는 에이전트 이름, 서명을 포함한 에이전트의 특성을 나타내는 값들이 명시된다.

2.2 에이전트를 사용한 기존의 IDS의 특성

에이전트 기술은 다양한 분야에서 학술적으로 사용되고 있는데, 특별히 인공지능, 분산시스템, 소프트웨어 공학 분야에 많이 사용되고 있다. 일반적으로 에이전트는 사람대신에 복잡한 작업을 수행할 수 있는 소프트웨어 프로그램으로 정의된다[6]. 자율적인 에이전트의 사용은 분리된 침입탐지 시스템을 구축하는 형태로 몇몇의 연구자들에 의해서 제안되었다[7-9]. 대부분의 자율적인 에이전트의 능력은 응용 도메인의 특정한 정보를 유지하며, 전체 시스템에 대하여 많은 유연성을 제공한다. 에이전트를 사용하는 대표적인 IDS로서는 EMERALD, AAFID 그리고 IA-NSM 등이 있다.

- EMERALD

SRI(Stanford Research Institute)에서 수행하는 EMERALD (Event Monitoring Enabling Response to Autonomous Live Disturbance)는 TCP/IP 데이터 스트림을 통해서 네트워크 공격이 이루어지는 문제에 대해서 연구하는 프로젝트이다. 네트워크 감사 모니터(Network surveillance monitor)는 로컬 지역 네트워크 트래픽을 관찰하고 엔터프라이즈 모니터에게 분석보고서를 제출하는데, 엔터프라이즈 모니터는 이러한 보고서들을 종합적으로 관리한다. EMERALD는 중앙 시스템에 지능적인 기능을 집중하였지만, 다른 에이전트 기술들은 사용하지 않는다[10-12].

- AAFID

AAFID(Autonomous Agents For Intrusion Detection) 프로젝트는 분산된 데이터를 수집하고 분석하는 동작을 수행하는 자율적인 에이전트들인 독립적인 객체에 기반을 두고

있다. 종합적인 분석은 트랜시버(transceiver)와 모니터(monitor)로 호칭되는 상위 계층의 객체에 의해서 각 호스트 별, 각 네트워크 별로 수행된다. AAFID의 구조는 충분한 정보를 획득할 수 있는 곳이라면 에이전트나 트랜시버 혹은 모니터 계층의 어느 곳에서든지 연산이 수행된다[17].

• IA-NSM

IA-NSM(Intelligent Agents for Network Security Management) 프로젝트는 침입탐지에서 지능 에이전트를 기술을 사용하여 전형적인 네트워크 환경에서 내재적인 공격에 대하여 방어하는 레벨을 향상시키는 멀티에이전트 시스템이 유연하게 통합되게 하는 기능을 제공한다[13].

앞에서 살펴본 바와 같이 기존의 에이전트를 이용한 침입탐지 시스템의 경우, 침입탐지를 효율적으로 수행하기 위하여 분산된 환경에 각각의 관리 대상 시스템에 에이전트를 구축하고 이를 중앙기반의 관리 시스템과 연동하여 침입 탐지의 효율을 높이는 연구가 진행되어 왔다. 이에 본 논문에서는 오용 침입탐지 시스템의 단점인 새로운 공격방법에 대한 대처를 신속히 수행할 수 있는 모바일 에이전트를 이용한 보안규칙 관리 방안(SRPM : Security Rules Propagation Method using mobile agent)을 제시하고, 이를 작업부하 데이터(workload data) 및 네트워크 시뮬레이터인 NS-2 (Network Simulator)를 통해서 기존의 방법과 비교를 수행하였다.

3. SRPM의 구조 및 시뮬레이션

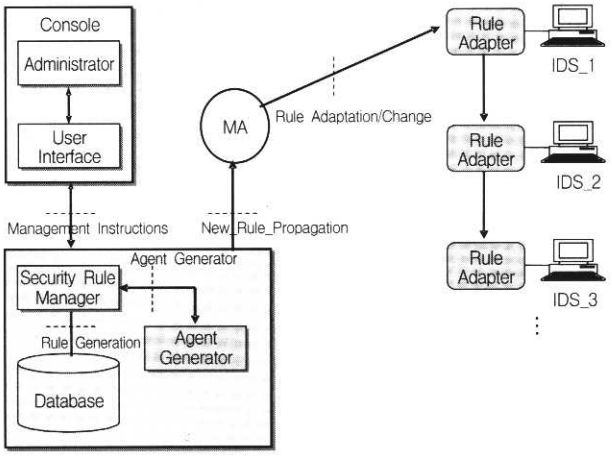
3.1 SRPM의 구조와 동작 메커니즘

본 논문에서는 SRPM을 제시함에 있어 다음과 같은 네트워크 환경을 가정하였다. 우선, 대상범위를 한정된 네트워크의 등록된 IDS가 아닌 인터넷에 존재하는 다수의 IDS시스템을 대상으로 보안규칙을 전파한다는 것과 IDS를 개발한 회사에 관계없이 보안규칙을 전파한다는 것이다. 그래서 본 논문에서는 TTP(Trusted Third Party)라는 공인 인증기관을 통해서 상호 인증하는 구조를 가지고 있으며, 규칙 어댑터라는 모듈을 통하여 새로이 전달되는 보안규칙을 자신의 시스템에 맞게 변경하는 작업을 수행한다.

SRPM에서 제안하는 구조는 크게 사용자가 보안규칙을 입력하고 관리하는 UI(User Interface)와 보안규칙을 저장하는 데이터베이스, 보안규칙을 관리하는 보안관리자(Security Rules Manager) 그리고 모바일 에이전트를 생성하는 에이전트 생성자(Agent Generator) 및 모바일 에이전트와 다른 침입탐지시스템간에 보안규칙 수용여부를 협상하는 규칙 어댑터(Rules Adapter)로 구성된다. 여기서, 모바일 에이전트는 보안규칙을 전파하는 전송자로서 사용되며, 특별히 침입탐지시스템에 설치된 규칙 어댑터와의 상호작용을 통하여 각 시스템에 맞는 보안 규칙을 전달하게 된다. SRPM의 특징을 살펴보면 다음과 같다.

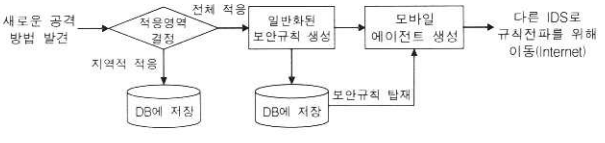
- 분산 시스템 환경에서 보안규칙을 전파하는 시스템
- 보안이 보장되는 모바일 에이전트기반 시스템
- 모바일 에이전트를 인증할 수 있고, IDS와 보안규칙에 대하여 협상이 가능한 시스템
- 기존의 오용탐지 시스템보다 효율성이 좋은 시스템

SRPM의 전체적인 구조는 (그림 2)와 같다.



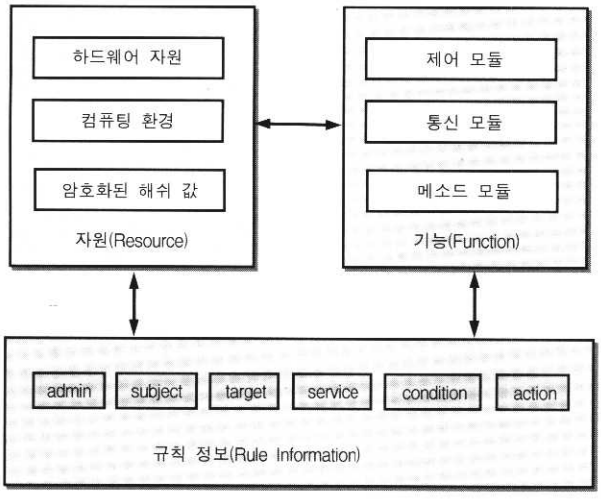
(그림 2) SRPM의 구조

오용 침입탐지 시스템을 관리하는 관리자가 새로운 형태의 공격을 발견했을 경우에 관리자는 UI 화면을 통하여 새로운 공격에 대한 대처 방법에 대한 정보를 입력한다. 입력된 정보는 보안규칙 관리자로 전송되어, 그 시스템에만 적용할 규칙인지 혹은 다른 IDS에도 적용 가능한 규칙인지를 판단하게 된다. 만일, 지역적으로만 적용 가능한 규칙이라면 데이터베이스에 저장되어 보안규칙을 입력한 시스템에서만 사용되고, 다른 시스템에서도 적용 가능한 규칙이라면 새로운 공격에 대한 보안규칙을 생성하여, 데이터베이스에 저장 및 에이전트 생성자로 보내지게 된다. 저장시에는, 새로 생성된 보안 규칙이 기존의 보안 규칙과 충돌하지는 않는지, 다른 보안 규칙에 영향을 주지는 않는지 등의 보안 규칙 무결성 보장을 위한 동작을 수행한다. 또한, 에이전트 생성자는 보안 규칙을 포함하는 모바일 에이전트를 생성하고, 생성된 모바일 에이전트는 인터넷을 통하여 다른 시스템으로 이동하면서 능동적으로 보안규칙을 전달하게 된다. 이를 정리하면 (그림 3)과 같다.



(그림 3) 모바일 에이전트의 생성 과정

SRPM에서 사용되는 모바일 에이전트는 크게 자원, 기능, 규칙정보 등의 세 부분으로 구성되어 있다. (그림 4)는 모바일 에이전트의 구성을 나타낸 것이다. 자원은 하드웨어 자원, 컴퓨팅 환경 그리고 암호화된 해쉬 값으로 구성되어 있으며, 컴퓨팅 환경은 메소드 모듈의 부호화된 에이전트의 연속된 상태를 의미한다. 암호화된 해쉬 값(encrypted hash value)은 에이전트의 무결성을 확인하기 위해 사용된다. 기능(function)은 제어 모듈, 통신 모듈 그리고 메소드 모듈로 구성된다. 제어 모듈은 인증을 포함한 모바일 에이전트의 모든 기능에 대해서 제어를 하고, 통신 모듈은 에이전트가 이동하면서 다른 IDS에 도착 하였을 때에, 그 IDS의 규칙 어댑터와의 통신 채널을 수립하는 기능을 제어하는 역할을 수행한다. 메소드 모듈은 구체적인 컴퓨팅 코드와 프로그램으로 구성된다.

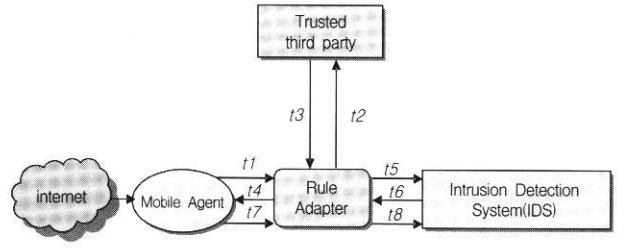


(그림 4) 모바일 에이전트의 구성

규칙정보(rule information)는 관리자(admin), 주제(subject), 대상(target), 조건(condition), 서비스(service), 행동(action)의 여섯 개의 요소로 구성된다. 여기서 관리자는 침입탐지 규칙을 만든 사람을 가리키며, 주제는 어떠한 형태의 공격인지를 나타내며, 대상은 보안 서비스가 필요한 대상을 의미한다. 서비스가 의미하는 것은 침입탐지 규칙에 의해서 영향 받는 서비스가 무엇인지를 나타내고, 조건은 사건에 의해서 만족되어야 하는 항목에 대해서 나열하고, 행동은 조건이 만족되었을 때에 수행되는 작업을 나타낸다.

모바일 에이전트는 분산 시스템 환경에서 새로운 패러다임을 제공하는데, 여기에는 또한, 악의의 에이전트와 악의의 호스트라는 두 종류의 보안 문제가 있다[14, 18]. 악의의 에이전트로부터는 다른 에이전트와 호스트를 보호하여야 하고, 악의의 호스트로부터는 에이전트를 보호해야 된다는 것이다. 본 논문에서 제시한 에이전트의 구조는 이러한 문제를 해결하기 위해서 에이전트 내에 암호화된 해쉬 값을 두어서 에이전트의 무결성을 보장하도록 하였으며, 공개키 기반(Public Key Infrastructure)의 상호인증을 통하여 악의의 호스트와 악의의 에이전트를 방지할 수 있도록 하였다. 또한, 모바일 에이전트의 보안 규칙과 침입탐지 시스템의 보안규칙 사이에 충돌이 발생하면, 모바일 에이전트는 생성되었던 호스트로 반환되어 규칙간의 충돌 사실을 알리게 된다.

(그림 4)와 같이 구성된 모바일 에이전트는 인터넷을 통하여 보안규칙을 다른 IDS에 전파하는데, SRPM의 구체적인 동작 메커니즘은 (그림 5)와 같다.



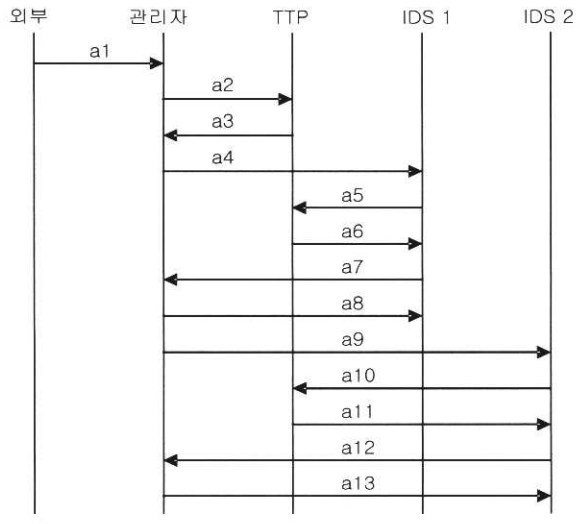
(그림 5) SRPM의 동작 메커니즘

규칙 어댑터(Rules Adapter)는 모바일 에이전트와 IDS 사이에서 중개자 역할을 하는 소프트웨어이다. 새로운 모바일 에이전트가 도착하면 해당 IDS에 필요한 보안규칙인지의 여부 및 모바일 에이전트를 인증하는 기능을 수행한다. 또한, 보안규칙을 자신이 시스템에 맞게 변경하는 기능을 수행한다. TTP는 인증서버로 모바일 에이전트와 서버가 상호 인증할 수 있도록 한다. 모바일 에이전트가 새로운 IDS의 규칙 어댑터에 도착하면(t1), 아래의 과정을 반복한다.

```
[1] If (모바일 에이전트에 대한 인증 수행(t2, t3, t4))
    [1.1] If (규칙 어댑터는 모바일 에이전트의 보안규칙과 IDS의
          보안규칙의 규칙충돌 체크(t5))
          [1.1.1] 충돌시 규칙 갱신을 거부하고, 관리자에게 통보
    [1.2] Else 충돌이 없으면(t6)
          [1.2.1] 규칙에 대한 무결성 체크(t7)
          [1.2.2] IDS의 보안규칙에 추가(t8)
[2] Else 인증 실패시
    [2.1] 새로운 규칙을 삭제하고 관리자에게 통보
[3] 다른 IDS로 이동
```

3.2 SRPM의 보안규칙 전파 메커니즘

(그림 6)과 (그림 7)은 보안규칙 전파의 측면에서 일반적인 IDS와 모바일 에이전트를 사용한 SRPM의 전파 메커니즘을 보여준다. (그림 6)은 관리자가 생성한 보안규칙을 전파하기 위해서 인터넷상에 있는 다른 IDS들과 인증을 수행한 후에, IDS의 요청에 의해서 보안규칙을 전파하는 것을 나타낸 것이다. 관리자는 원격지에 위치하기 때문에 하나의 IDS에 규칙을 전파한 후에 다른 IDS의 보안규칙을 관리하기 위해서는 매번 인증 및 보안규칙 전송요구, 보안규칙의 전송이라는 과정을 반복해야 한다.

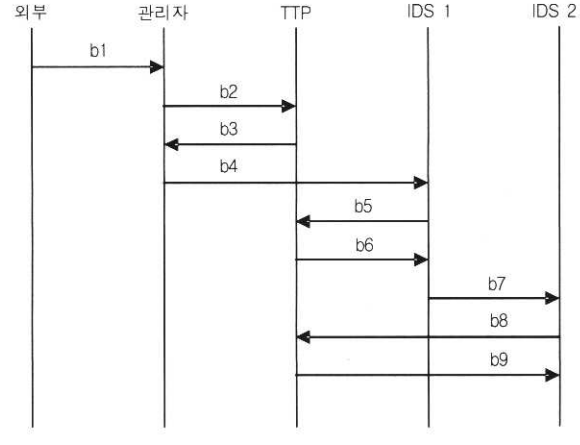


(그림 6) 기존의 IDS 보안규칙 전파

즉, 외부나 보안업체를 통해 침입정보를 입수하면(a1), 아래의 과정을 반복한다.

```
[1] If (정보의 출처인증 수행 (a2, a3))
   [1.1] IDS에게 새로운 보안 정보의 도착 사실을 알림 (a4, a9)
   [1.2] If (IDS는 TTP를 통해 관리자에 대한 인증 수행 (a5, a6,
         a10, a11))
         [1.2.1] 인증시, IDS는 관리자에게 보안규칙의 전송을 요구
                 (a7, a12)
         [1.2.2] 관리자는 IDS에 새로운 보안규칙을 전송 (a8, a13)
   [1.3] Else
         [1.3.1] 인증 실패시, 관리자에게 통보
[2] Else
   [2.1] 인증 실패시, 침입정보를 버림
```

그러나 SRPM의 보안규칙 전파 방식은 기존의 IDS의 방식과는 다른 (그림 7)과 같은 방식으로 이루어진다.



(그림 7) SRPM의 보안규칙 전파

SRPM은 외부나 혹은 새로 발견한 침입사건에 대해 정보를 인증하는 동작은 기존의 IDS의 방식과 동일하나, SRPM은 모바일 에이전트가 다른 IDS로 이동해서 보안규칙을 관리한다. 이를 정리하면, 외부나 보안업체를 통해 침입정보를 입수하면(b1), 아래의 과정을 반복한다.

```
[1] If (정보의 출처인증 수행 (b2, b3))
   [1.1] 모바일 에이전트가 다른 IDS로 이동 (b4)
   [1.2] If (모바일 에이전트에 대한 인증 수행 (b5, b6))
         [1.2.1] 모바일 에이전트의 보안규칙을 IDS의 데이터베이스
                 에 저장
   [1.3] Else
         [1.3.1] 인증 실패시, 관리자에게 통보
[2] Else
   [2.1] 인증이 실패하면, 침입정보를 버림
[3] 다른 IDS로 이동 (b7)
```

기존의 IDS는 원격에서 관리자가 직접 매번 보안규칙을 전송해야 되지만, SRPM은 관리자가 한번 보안규칙을 생성하게 되면, 그 보안규칙들이 필요한 IDS에 협상을 통하여 바로 저장된다는 것이 큰 차이점이라 할 수 있다.

3.3 기존 시스템과의 비교

기존의 IDS 방식과 SRPM의 차이점 및 성능을 비교하기 위해서, 아래와 같은 항목들을 작업부하 데이터로 선정하였는데, 이 값들은 각 시스템의 동작에 대하여 성능을 비교하기 위해서 변수로 선정한 것이다. 이 비교를 통하여 보안규칙을 전파하는데 필요한 작업량의 효율성을 알 수 있다.

- i : IDS와 TTP 사이에 통신으로 교환되는 작업부하
- j : 하나의 IDS에서 다른 IDS로 이동하는데 필요한 작업부하
- k : IDS와 모바일 에이전트 사이에 통신으로 교환되는 작업부하
- l : 관리자와 IDS에서 통신으로 교환되는 작업부하
- m : 보안규칙을 분석하는데 필요한 작업부하
- n : IDS를 위한 보안규칙을 생성하기 위한 작업부하
- p : IDS와 모바일 에이전트 사이에 상호인증을 위한 작업부하
- q : 공격을 처음 발견한 관리자가 IDS로 공격에 대한 정보를 입력하는 작업부하

<표 1>은 일반적인 IDS와 SRPM의 작업부하 데이터를 비교한 것이다.

〈표 1〉 SRPM과 IDS의 작업부하 데이터의 비교

행 동	일반적인 IDS	SRPM
패킷 전송	Nq	q
인증 작업	2N (i + p)	2N (i + p)
정보 분석	N (l + m)	l + m
보안규칙 생성	N (l + n)	l + n
보안규칙 전파		k + (N - 1) j

N : IDS의 개수

<표 1>에 대해서 분석해 보면, 일반적인 IDS에서는 새로운 보안규칙을 입력하기 위한 총 데이터 량이 N(2i + 2p + q + 2l + m + n)이고, 여기서 IDS의 개수가 증가할수록 작업부하 데이터 량은 (2i + 2p + q + 2l + m + n)의 배만큼 증가한다. 반면에 SRPM의 총 데이터 량은 q + 2N(i + p) + 2l + m + n + k + (N - 1)j이다. 여기서 N이 증가해도 q + 2l + m + n + k의 값은 고정된 값이므로, IDS의 개수가 증가할수록 작업부하 데이터 량은 (2i + 2p + j)씩 증가하게 된다. 그러므로, IDS의 수가 증가할수록 위에서 설정한 작업부하 데이터는 SRPM에 보안규칙을 추가하는 것이 기존의 IDS에서 보안규칙을 추가하는 것보다 적게 증가한다는 것을 알 수 있다.

3.4 시뮬레이션 결과

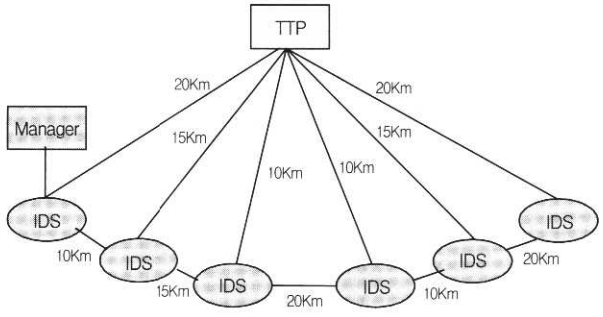
지연시간에 대하여 기존의 방식의 보안규칙 전파 방법과 모바일 에이전트를 이용하여 보안규칙을 전파하는 SRPM 방식을 평가하기 위해서, 네트워크 시뮬레이터인 NS-2를 사용하였다. NS-2는 LBNL(Lawrence Berkeley National Laboratory)에서 개발되었으며, TCP, 라우팅 프로토콜, 멀티캐스트 프로토콜, RTP(Real Time Protocol), SRM(Scalable Reliable Multicast) 등 다양한 인터넷 프로토콜에 대한 시뮬레이션을 수행하기에 적절한 여러 환경을 제공하고 있어 현재 널리 사용되고 있는 네트워크 시뮬레이션 도구이다[15]. 위의 두 가지 방법을 비교하기 위해서 지연시간을 측정하였는데, 이는 [19]에서 조사한 자료처럼 일반적인 사용자가 느끼는 성능 중에서 가장 중요한 것이 지연시간이므로, 본 논문에서는 시간에 대하여 성능비교를 수행하였다.

(그림 8)은 SRPM의 보안규칙 전파 절차에 대하여 나타낸 것이다.

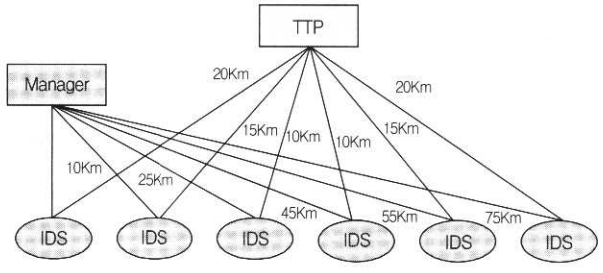
```
While (true) { // attack information arrival
    read incoming_attack_information a ;
    b = create_security_rule (a) ;
    for (i = 0 ; i < N ; i++) { // N : number of IDS
        distance = get_distance (i, i + 1) ;
        p_delay = distance ; / 2.3×10^8
        // propagation delay
         r_size = length of (b) ;
        // size of security rule
         bandwidth = get_bandwidth (i, i + 1) ;
         t_delay = r_size / bandwidth ;
        // transmission delay
         q_delay = get_q_delay (i, i + 1) ;
        // queueing delay
         delay = p_delay + t_delay + q_delay ;
    }
    t = get_time (i, i + 1, bandwidth, delay)
    // compute the elapsed time using NS
}
```

(그림 8) SRPM의 보안규칙 전파 절차

(그림 9)는 SRPM의 성능을 기존의 시스템과 비교평가 하기 위해서 사용한 시뮬레이션 토폴로지를 나타낸 것이다. 이 시뮬레이션에서는 6개의 IDS와 1개의 TTP를 이용한 인증서버가 사용되었으며, 네트워크의 대역폭의 크기는 10Mbps로 하였고, 각각의 IDS와 IDS의 거리는 아래의 그림과 같이 다르게 설정하였으며, 보안규칙 파일의 크기는 4.5kbyte로 하였다.



(a) Conventional IDS

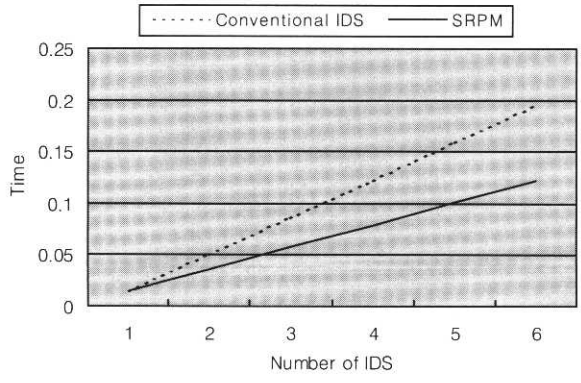


(b) SRPM

(그림 9) 기존의 IDS와 SRPM의 보안규칙 전파

이 시뮬레이션에서는 보안규칙을 전파하는 시간에 대해서 SRPM과 기존의 IDS 시스템과의 비교를 실시하였다. 여기서, 지연(delay)은 다음과 같은 과정을 통하여 계산을 수행하였다[16].

- *Delay = Propagation delay + Transmission delay + Queuing delay*
- *Propagation delay = Distance/* $2.3 \cdot 10^8$*(in a cable)*
- *Transmission delay = Size/Bandwidth*



(그림 10) 기존의 IDS와 SRPM의 보안규칙 전파시간

이 시뮬레이션에서 큐잉 지연(queuing delay)은 고려하지 않았으며, (그림 10)은 보안규칙 전파시간에 대한 결과를 그래프로 표현한 것이다. 그래프에서 알 수 있듯이 보안규칙을 전파해야 될 IDS의 개수가 증가할수록 SRPM의 방법이 기존의 IDS에서 보안규칙을 갱신하는 방법보다 시간적으로 빠르게 보안규칙을 전파할 수 있다는 것을 알 수 있다.

4. 결론 및 향후 계획

오용 탐지 방식은 침입탐지 시스템에서 다른 어떤 방법보다도 많이 사용되는 탐지 방식이다. 그러나 이 방식은 새로운 공격에 대하여 취약하다는 단점이 있다. 이러한 단점을 보완하기 위해서 모바일 에이전트를 이용한 보안규칙 전파 시스템을 제안하였다. 본 논문에서 제안한 방식은 보안규칙 전파 대상을 인터넷 상의 다수의 IDS에 개발회사와 상관없이 보안규칙을 전파하는 것을 기본 전제로 하였다.

모바일 에이전트는 많은 혜택과 보안적인 단점을 가지고 있는데, SRPM에서는 이러한 단점을 보완하기 위해서 TTP 기반의 상호인증과 해쉬 값을 사용하였다. 모바일 에이전트는 다른 침입탐지 시스템을 돌아다니면서, 보안규칙을 빠르게 전파하며, 모바일 에이전트와 IDS와의 협상을 통하여 각각의 IDS에게 최적화 된 보안규칙을 전달한다. 또한, 기존의 IDS와 SRPM의 성능비교에서도 알 수 있듯이, SRPM이 빠른 시간 안에, 적은 네트워크 작업부하 데이터를 사용하여 분산 네트워크 환경에서 효율적으로 보안규칙을 전파하는 것을 알 수 있다.

향후 연구 계획으로는, 다른 보안 시스템들과도 원활하게 보안규칙에 대하여 상호협상을 통하여 일관된 규칙이 반영할 수 되도록 모바일 에이전트의 성능 향상에 대하서 연구를 수행할 것이다.

참 고 문 헌

[1] R. G. Bace, Intrusion Detection, Macmillan Technical Publishing, 2000.

[2] B. Mukherjee, T. L. Heberlein and K. N. Levitt, Network Intrusion Detection, IEEE Network, May/June, 1994.

[3] R. Jagannathan, T. Lunt, D. Anderson, C. Dodd, F. Gilham, C. Jalali, H. Javitz, P. Neumann, A. Tamaru and A. Valdes, System Design Document : Next-Generation Intrusion Detection Expert System (NIDES), Technical Report A007/A008/A009/A011/A012/A014, SRI International, March, 1993.

[4] S. Kumar and E. Spafford, "A Pattern Matching Model for Misuse Intrusion Detection," Proceedings of the Seventeenth National Computer Security Conference, Oct., 1994.

[5] Information Security 21c, The history and kinds of intrusion detection system, http://www.securityinformation.com, July, 2001.

[6] H. S. Nwana, Software Agents : an Overview. Knowledge Engineering Review, 1996.

[7] M. Crosbie and G. H. Spafford, Defending a Computer System using Autonomous Agents. Technical Report No.95-022, Dept. of Comp. Sciences, Purdue University, March, 1996.

[8] M. Crosbie and E. H. Spafford, "Active Defense of a Computer System using Autonomous Agents," Technical Report CSD-TR-95-008, Department of Computer Sciences, Purdue University, 1995.

[9] Balasubramaniyan, Jai, J. O. Garcia-Fernandez, E. H. Spafford and D. Zamboni, An Architecture for Intrusion Detection using Autonomous Agents. Department of Computer Sciences, Purdue University, Coast TR 98-05, 1998.

[10] G. G. Helmer, J. S. K. Wong, V. Honavar and L. Miller, Intelligent agents for intrusion detection. In Proceedings, IEEE Information Technology Conference, Syracuse, NY, pp.121-124, September, 1998.

[11] A. Porras and P. G. Neumann, EMERALD : Event Monitoring Enabling Responses to Anomalous Live Disturbances. In Proceedings of the National Information Systems Security Conference, Oct., 1997.

[12] A. Porras and A. Valdes, "Live Traffic Analysis of TCP/IP Gateways," in Networks and Distributed Systems Security Symposium, March, 1998.

[13] K. Boudaoud, H. Labiod, R. Boutaba, Z. Guessoum, Network security management with intelligent agents, Network Operations and Management Symposium, 2000, NOMS 2000.

[14] L. Qi, L. Yu, "Mobile agent-based security model for distributed system," Systems, Man and Cybernetics, 2001, IEEE International Conference, 2001.

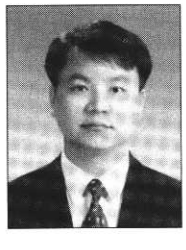
[15] NS, http://www-mash.cs.berkeley.edu/ns.

[16] L. Peterson and B. Davie, Computer Networks : A Systems Approach. Morgan Kaufman, 2nd Edition, 2000.

[17] W. Jansen, P. Mell, T. Karygiannis, D. Marks, Applying Mobile Agents to Intrusion Detection and Response, October, 1999.

[18] S. Greenberg, C. Byington, T. Holding, G. Harper, "Mobile Agents and Security," IEEE Communications Magazine, July, 1998.

[19] NSF CISE Grand Challenge in e-Science Workshop Report, http://www.evl.uic.edu/activity/NSF/index.html, Jan., 2002.



김 태 경

e-mail : tkkim@rtlab.skku.ac.kr

1997년 단국대학교 수학교육(학사)

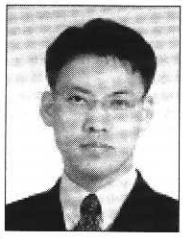
2001년 성균관대학교 정보통신공학(석사)

1996년~1997년 기아정보시스템 사원

1997년~2001년 서울신학대학교 종합전산실 주임대리

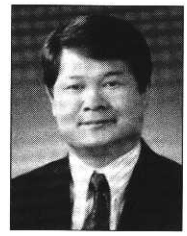
현재 성균관대학교 정보통신공학부 박사과정 수료

관심분야 : 그리드 네트워크, 네트워크 보안, Mobile Agents



이 동 영

e-mail : dylee@rtlab.skku.ac.kr
1993년 동아대학교 전자공학(학사)
1998년 성균관대학교 정보공학(석사)
2002년 성균관대학교 컴퓨터공학(박사)
1993년~1997년 기아자동차 중앙기술연구소 연구원
1999년~2002년 성균관대학교 정보통신과 강사
현재 명지전문대학 정보통신과 조교수
관심분야 : 네트워크 보안, 시스템보안, 네트워크 관리



정 태 명

e-mail : tmchung@ece.skku.ac.kr
1981년 연세대학교 전기공학(학사)
1984년 University of Illinois Chicago, 전자계산학과 학사
1987년 University of Illinois Chicago, 컴퓨터공학과 석사
1995년 Purdue University, 컴퓨터공학 박사
1985년~1987년 Waldner and Co., System Engineer
1987년~1990년 Bolt Bernek and Newman Labs., Staff Scientist
현재 성균관대학교 정보통신공학부 부교수
관심분야 : 실시간 시스템, 네트워크 관리, 시스템 보안, 네트워크 보안, 전자상거래