2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

이동 에이전트를 이용한 네트워크 침입탐지 시스템

안계순*, 정태명**
성균관대학교 정보공학과
e-mail : ksahn@rtlab.skku.ac.kr

Network Intrusion Detection System Using Mobile Agents

K. S. Ahn*, Tai M. Chung**
*Dept of Information Engineering, Sungkyunkwan University
** Dept of Electric & Computer Engineering, Sungkyunkwan University

요 약

본 논문에서는 이동 에이전트를 이용하여 현재 침입탐지시스템이 가지고 있는 문제점을 해결하고자 한 연구들에 대하여 살펴보고자 한다. 현재 대부분 네트워크 침입탐지시스템의 분산되어 있고, 계층화되어 있는 구조에 의하여 시스템의 유연성이 부족해지고 정보가 단일 모듈에 집중되는 문제점이 발생된다. 이러한 문제점을 해결하고자 자치성 및 이동성을 가진 이동 에이전트 시스템을 도입하는 연구들이 진행되고 있다. 이러한 연구들 중에서 침입의 근원지를 추적하는 연구 및 네트워크에 면역 시스템을 구축하는 연구에 대하여 살펴볼 것이며, 이러한 두 가지의 연구 분야 이외에도 이동 에이전트 시스템을 도입할 수 있는 분야에 대해서도 언급할 것이다.

1. 서론

최근의 네트워크 관련기술의 발전으로 인하여 대규모 네트워크 시스템이 증가하였을 뿐만 아니라 네트워크를 구성하는 요소들도 다양해지고 복잡해졌다. 이러한 네트워크 기술의 발전은 네트워크에 대한 침입을 다양화, 지능화 시켰고, 이러한 침입으로부터 시스템을 안전하게 보호하기 위하여 VPN, 방화벽, 침입탐지시스템 등의 많은 보안 시스템들이 사용되고 있다.

그러한 보안 시스템 중 침입탐지시스템은 1987 년 Dorothy Denning 모델이 제시된 이후에 호스트 기반의 침입탐지시스템을 시작으로 현재에는 다양한 네트워크 기반의 침입탐지시스템이 사용되고 있다[1].

그러나 현재의 침입탐지시스템은 대규모의 네트워크에서 발생하는 모든 이벤트를 처리할 수 있을 정도로 효율적이지 못하다. 또한 다양한 침입을 탐지하기 위한 정책이나 사용자들의 프로파일 정보등의 유지가 어렵고, 네트워크 구조등의 환경 변화에 동적으로 대응하지 못할 뿐만 아니라, 침입탐지시스템 자체가 침입의 대상이 될 경우 이를 탐지하기 어렵다는 문제점을 가지고 있다[2].

이를 해결하기 위한 방법 중 하나로 특정한 목적을 가지고 자치적으로 활동하며 자유롭게 네트워크를 통하여 이동할 수 있는 이동 에이전트 시스템을 도입함으로써 침입탐지시스템이 주위 환경의 변화에 좀 더 동적으로 대응할 수 있고, 침입탐지시스템 자체에 대한 신뢰도를 높이는 방법이 제시되고 있다[2, 3, 4].

따라서, 본 논문에서는 일반적인 네트워크 기반의 침입탐지시스템의 구조에 대하여 살펴 봄으로써 기존의 네트워크 침입탐지시스템에 발생하는 구조상의 문제에 대하여 살펴보고, 이동 에이전트의 특징을 이용하여 이러한 문제점을 어떻게 해결하였는지 현재 연구중인 이동 에이전트를 이용한 네트워크 침입탐지시스템들에 대하여 살펴볼 것이다.

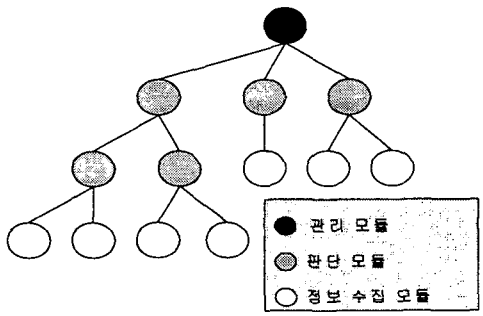
본 논문은 총 5 장으로 구성된다 .2 장에서 일반적인 네트워크 침입탐지시스템의 구조에 대하여 살펴봄으로써 기존의 네트워크 침입탐지시스템의 구조상 문제점을 제기할 것이다. 3 장에서는 이동 에이전트에 대하여 간략히 소개를 할 것이며, 4 장에서는 이동 에이전트 시스템을 이용한 침입탐지시스템에 대한 연구들에 대하여 기술함으로써 앞서 제기된 문제점을 어떻게

해결할 수 있는지를 제시할 것이다. 마지막으로 5 장에서는 결론 및 향후 전망에 대하여 제시할 것이다.

2. 네트워크 침입탐지시스템의 구조

초기의 대부분의 침입탐지시스템 - IDES[5, 6], IDIOT[7], NADIR[8], NSM[9] - 은 중앙에 집중된 형태의 구조를 가졌다. 그러나 감시대상이 대규모의 네트워크로 변함에 따라 중앙 집중식의 형태 대신에 분산형태의 침입탐지시스템 - DIDS[10], EMERALD[11], AAFID[12] - 이 등장하게 되었다 [12].

일반적인 분산형태의 네트워크 침입탐지시스템은 [그림 1]과 같은 계층구조를 가진다.



[그림 1] 일반적인 분산형태의 침입 탐지 시스템의 구조

정보 수집 모듈은 네트워크에 분산되어 로그정보를 수집하여 판단 모듈로 보낸다. 일반적으로 정보 수집 모듈과 판단 모듈이 함께 존재할 수도, 따로 떨어져 존재할 수도 있다. 판단 모듈은 여러 정보 수집 모듈로부터 수신된 정보를 이용하여 침입여부를 판단한다. 관리 모듈은 이러한 판단 모듈 및 정보 수집 모듈들을 관리하며 사용자와의 인터페이스를 담당한다.

2.1 분산형태 구조의 장점 및 단점

분산형태의 침입탐지시스템들은 일반적으로 계층적 구조를 가짐으로써 운영상의 여러가지 장점을 가지게 되었다. 대규모 네트워크에 효과적으로 적용을 할 수 있으며, 여러 정보 수집 모듈에서 수집된 정보를 중간 계층의 판단 모듈에서 관리하기 때문에 다중공격도 쉽게 탐지해 낼 수 있다. 또한 각 모듈을 따로 관리할 수 있기 때문에 시스템의 유연성이 높아졌다.

그러나 이러한 구조가 장점만 가지고 있는 것은 아니다. 분산된 모듈들로 인하여 침입탐지시스템의 관리가 어려워 졌으며, 여러 정보 수집 모듈로부터 수집된 정보가 하나의 판단 모듈에 독점되기 때문에 중간 계층이상의 모듈에 이상이 생길 경우 해당 모듈이 탐지하고 있는 영역이 침입탐지시스템의 보호영역에서 벗어날 수 있는 문제점들이 발생하였고, 이로 인하여 또 다른 구조로의 침입탐지시스템의 변화가 필요하게 되었다.

3. 이동 에이전트의 소개

Jeffrey M. Bradwhaw 에 따르면 소프트웨어 에이전트는 다음과 같이 정의할 수 있다[13]. "특정 환경에서 지속적이고, 자치적으로 기능을 수행하는 소프트웨어로써 환경의 변화에 적응할 수 있을 정도로 유연하고 지능적인 방법으로 행동하며. 이상적으로는 에이전트의 경험으로부터 학습이 가능하며 다른 에이전트와의 통신을 통하여 협동이 가능하다."

일반적으로 소프트웨어 에이전트의 필수적인 특징은 자치적이며 지적이라고 표현된다. 즉 에이전트는 특정 목적을 위하여 지속적으로 동작하며 환경의 변화를 판단하고 변화에 적응할 수 있고 이러한 모든 행위는 독립적으로 이루어 질 수 있어야 한다[14].

또한, 소프트웨어 에이전트는 다른 에이전트나 자신이 동작하고 있는 환경과 통신을 할 수 있으며, 에이전트가 발생한 호스트에서 다른 호스트로의 이동이 가능할 수도 있고, 이전의 경험을 통한 학습이 가능할 수도 있는 선택적인 특징을 가진다[14].

즉, 이동 에이전트는 소프트웨어 에이전트의 특별한 형태로써 소프트웨어 에이전트의 기본적인 특징을 만족하며 자신이 발생한 호스트로부터 다른 호스트로 이동할 수 있는 이동성을 가지는 에이전트를 말한다.[14]

이러한 이동 에이전트의 특징에 때문에 일반적인 시스템에 이동 에이전트 시스템을 도입하였을 경우엔 여러 가지 장점이 있을 수 있다. 우선 네트워크의 부하를 줄일 수 있고, 전송 지연시간을 극복할 수 있으며, 시스템이 비동기적이고 자치적으로 동작할 수 있다. 또한 환경의 변화에 동적으로 적응이 가능하고, 신뢰할 수 있는 시스템을 구현할 수 있다[2, 6].

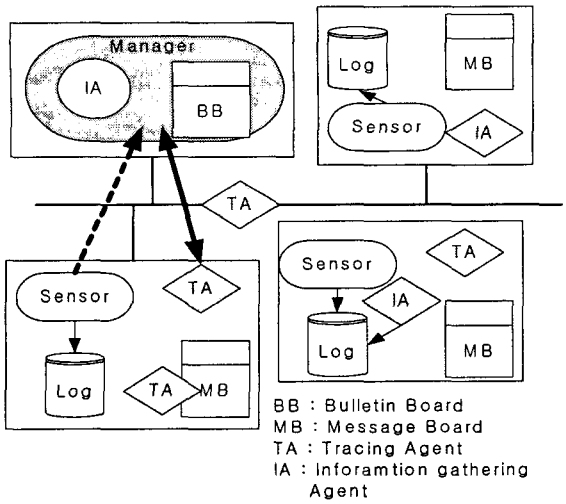
4. 이동 에이전트를 이용한 침입탐지시스템

앞 장에서 언급한 이동 에이전트 시스템을 도입하였을 때 얻을 수 있는 장점은 침입탐지시스템에서도 마찬가지로 적용할 수 있다. 우선 이동 에이전트가 정보 수집 모듈로부터 필요한 정보만을 가지고 직접 이동할 수 있기 때문에 네트워크 부하를 줄일 수 있다. 또한 새로운 네트워크 콤포넌트의 추가나 네트워크의 구성이 바뀔 경우에도 정보 수집 모듈을 이동 에이전트로 구성하여 쉽게 이동 시킬 수 있기 때문에 네트워크의 변화에 동적으로 적응할 수 있다[2]. 마지막으로 판단 모듈 및 관리 모듈이 여러 개의 이동 에이전트 들로 이루어져 있을 경우 하나의 판단 모듈이나 관리 모듈에 이상이 생기더라도 다른 모듈을 이동 시켜 이상이 생긴 모듈을 대체할 수 있기 때문에 신뢰성이 있는 시스템을 구현할 수 있다.

현재 이동 에이전트를 이용한 침입탐지시스템에 대한 연구는 주로 침입의 근원지에 대한 추적에 이용하는 분야 및 네트워크 면역 시스템을 구축하는 분야에서 주로 이루어 지고 있다[2][3].

4.1 침입에 대한 추적 (IDA)

IDA(Intrusion Detection Agents system)는 탐지한 침입의 근원지를 추적하는 데에 이동 에이전트를 이용한 침입탐지시스템이다[3].



[그림 2] IDA의 구조

4.1.1 IDA 의 구조

Manager 는 이동 에이전트로 이루어져 있는 Trace Agent 와 Information-gathering Agent 를 발생시키고 이동시킬 수 있다. 또한 Information-gathering Agent 가 수집한 정보를 관리하는 Bulletin Board 를 관리한다.

Sensor 는 각 탐지 대상 시스템에 존재하며 시스템의 로그 및 패킷 정보를 모니터링하여 의심스러운 정보를 발견하면 Manger 에게 보고한다.

Trace Agent 는 이동 에이전트로 구현되어 침입의 경로를 추적하는 역할을 한다. 추적의 역할 이외에는 Information-gathering Agent 를 발생시키는 일만 하므로 크기를 최소화 하여 추적이 용이하게 하였다.

Information Agent 역시 이동 에이전트로 구현되어 자신을 발생시킨 Trace Agent 가 추적하는 침입에 관련된 정보만을 수집하여 Manager 로 이동하기 때문에 네트워크 트래픽의 발생을 최소화 할 수 있다.

IDA 는 각 에이전트간의 통신이 가능하도록 Bulletin Board 와 Message Board 를 관리한다. Bulletin Board 는 Information –gathering Agent 로부터 수집된 정보를 관리 및 공유하며, Message Board 는 각 Trace Agent 가 현재 자신이 추적중인 정보에 대하여 기록함으로써 하나의 침입을 여러 개의 에이전트가 추적하는 일을 방지한다.

4.1.2 IDA 의 동작원리

각각의 Sensor 는 설치된 시스템에서 로그를 분석하게 되는데 Sensor 가 수상한 정보를 발견하게 되면 발견한 정보의 종류와 함께 Manager 에게 보고하게 된다. Manager 는 Sensor 로부터 보고를 받으면 Trace Agent 를 발생시킨 후 해당 시스템으로 이동시킨다.

Trace Agent 가 대상 시스템에 도착하게 되면, Information-gathering Agent 를 발생 시킨 후 침입을 추적한다. Trace Agent 는 각 시스템에 도착할 때마다 이러한 작업을 반복하고, 더 이상 이동할 시스템이 없을 때에는 다시 Manager 로 복귀한다.

Information-gathering Agent 는 자신을 발생시킨 Trace Agent 가 추적중인 침입에 관련된 정보만을 수집한 후 Manger 로 돌아간다.

4.1.3 IDA 의 장점

IDA 에서는 Trace Agent 와 Information-gathering Agent 를 이동 에이전트를 이용하여 구현하였다. Trace Agent 는 침입의 경로를 추적하는 일 이외에 다른 역할을 하지 않기 때문에 비교적 작게 구현될 수 있어서 쉽게 침입을 추적할 수 있다. 또한 Information-gathering Agent 가 필요한 정보만을 수집하여 Manager 로 이동한다. 따라서 모든 로그정보를 네트워크를 통하여 전송할 필요가 없기 때문에 네트워크 트래픽을 줄일 수 있다.

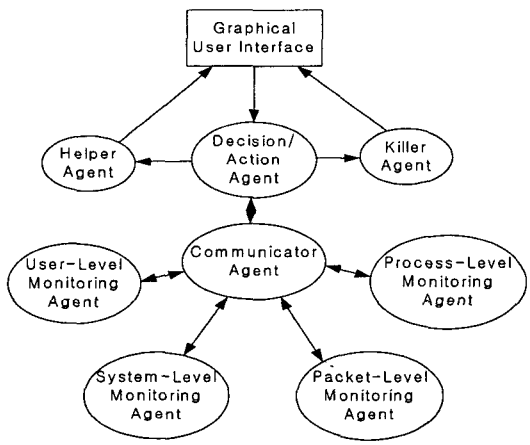
4.2 네트워크 면역 시스템의 구축 (SANTA)

Immunity-based IDS 인 SANTA (Security Agents for Network Traffic Analysis)는 대부분의 모듈을 이동 에이전트로 구현하여 네트워크를 이동할 수 있게 함으로써 마치 생물체의 면역 시스템과 비슷한 구조로 구현하였다[2].

4.2.1 SANTA 의 구조

Monitoring Agent 는 네트워크에 연결된 호스트들을 감시한다. 각 Monitoring Agent 들은 각자의 레벨에 맞게 사용자, 시스템, 네트워크 패킷, 동작중인 프로세스들을 감시하여 비정상 행위가 발생시 이를 Communicator Agents 를 이용하여 Decision/Action Agent 에 보고한다.

Decision/Action Agent 는 Monitoring Agents 로부터 보고된 정보를 이용하여 침입을 판단하고, 그에 대응하기 위하여 Helper Agents 와 Killer Agents 를 발생시킨다. Helper Agent 는 현재의 상태정보를 GUI 를 이용하여 관리자에게 보고하며, Killer Agent 는 침입행위를 하는 프로세스를 종료하는 역할을 한다.



[그림 3] SANTA 의 구조

4.2.2 SANTA 의 동작원리

Monitoring Agent 들은 각자의 레벨에 맞는 정보들을 수집하여 비정상 행위를 탐지한다. 비정상 행위를 탐지하게 되면 이를 Decision/Action Agent 에게 보고하게 된다.

Decision/Action Agent 는 비정상 행위를 보고 받은 후에 Helper Agent 를 이용하여 사용자에게 알린 후, 보고 받은 행위를 판단하여 기준치 이상의 위험요소를 가지고 있을 경우 Killer Agent 를 이용하여 침입을 발생시키는 프로세스나 네트워크 세션을 중지시킨다.

4.2.3 SANTA 의 장점

SANTA 에서는 대부분의 모듈을 이동 에이전트를 이용하여 구현하였다. 이러한 특징 때문에 다수의 Decision/Action Agents 가 다수의 Monitoring Agents 를 관리하는 구조를 가지게 되기 때문에 침입으로부터 하나의 Decision/Action Agent 에 이상이 발생하여 정상적인 동작이 불가능하더라도 다른 Decision/Action Agent 가 이를 대체할 수 있으므로 시스템의 신뢰성을 높일 수 있다.

또한 네트워크 콤포넌트가 추가 되거나 네트워크 구조가 변하더라도 단지 이동 에이전트를 해당 콤포넌트로 이동 시키거나 Monitoring Agents 들을 이동시킴으로써 네트워크의 변화에 침입탐지시스템을 적용시킬 수 있다.

5. 결론 및 향후 전망

본 논문에서는 현재 침입탐지시스템이 가지고 있는 문제점 중에서 특히 구조적인 특징에 의하여 발생되는 문제점에 대하여 기술하였고, 그 문제를 해결하기 위한 방법으로 이동 에이전트 기술을 도입한 연구들에 대하여 소개하였다.

본 논문에서 소개한 대표적인 두 가지 연구인 이동 에이전트를 이용하여 침입의 근원지를 찾는 연구와 탐지 모듈 및 판단 모듈을 이동 에이전트들로 구성하여 네트워크를 감시하게 함으로써 네트워크에 침입에 대한 면역 시스템을 구축하는 연구에 초점을 맞추어 살펴 보았다[2, 3].

그러나 본 논문에서 기술한 두 가지의 연구분야 이외에도 에이전트의 자치적인 특징 및 학습능력을 이용하여 각 탐지 모듈들이 위치하고 있는 환경에 가장 적합하게 침입탐지에 대한 정책을 수립할 수 있게 하거나 네트워크의 구성이 변하였을 때 스스로 변화된 환경에 가장 알맞도록 탐지 모듈을 배치할 수 있게 하는 연구분야도 생각해 볼 수 있다. 또한 에이전트는 사용자의 일을 대신하여 동작하는 특징을 이용하여 침입탐지시스템의 관리 모듈을 이동 에이전트로 구성하여 사용자에게 관리의 편리성을 주는 연구 분야도 생각할 수 있을 것이다.

마지막으로 필자의 경우엔 현재 개발중인 네트워크 기반의 침입탐지시스템의 관리 모듈에 이동 에이전트 기술을 이용하여 좀 더 유연성이 있고, 신뢰성이 있는 침입탐지시스템을 구현하는 데에 초점을 맞추어 연구할 것이다.

참고문헌

[1] Denning, Dorothy E., "An Intrusion Detection Model," IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, pp.222-232, February 1987

[2] Wayne Jansen, Perter Mell, Tom Karygiannis, Don Marks "Applying Mobile Agents to Intrusion Detection and Response," NIST Interim Report(IR)-6416, October. 1999

[3] M.Asaka, S.Okazawa, A.Taguchi, S.Goto, "A Method of Tracing Intruders by Use of Mobile Agents," INET'99, June 1999.

[4] Dipankar Dasgupta, Hal Brian, "Mobile security agents for network traffic analysis," DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings , Volume: 2 , pp332 –340, 2001

[5] D.E. Denning, D.L. Edwards, R. Jagannathan, T.F. Lunt, P. G. Neumann, "A prototype IDES – a real-time intrusion detection expert system," Technical Report, Computer Science Lab, SRI International, 1987.

[6] T.F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. G. Neumann, H.S. Javitz, A. Valdes, T.D. Garvey, "A real-time intrusion detection expert system (IDES) – Final Technical Report," Technical Report, SRI Computer Science Laboratory, SRI International, Melno Park, CA, February 1992.

[7] M. Crosbie, B. Dole, T. Ellis, I. Irsul, E. Stafford, "IDIOT-Users Guide," COAST Laboratory, Purdue University, ftp://coast.cs.purdue.edu/pub/COAST/papers/IDIOT/IDIOT_Users_Guide.ps, September 1996.

[8] J. Hochberg, K. Jackson, C. Stallins, J.F. McClary, D. Dubois, J. Ford, "NADIR: and automated system for detecting network intrusion and misuse," Computers and Security 12(3) (1993) 235-248

[9] L. Heberlein, G. Dias, K.Levitt, B. Mukherjee, J. Wood, D. Wolber, "A network security monitor," Proceedings of the IEEE Symposium on Research in Security and Privacy, May 1990.

[10] S.R. Snapp, S.Smaha, D.M. Teal, T.Grance, "The DIDS (distributed intrusion detection system) prototype," Proceedings of the USENIX Summer Technical Conference, San Antonio, TX, June 1992.

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

[12] Eugene H. Spafford, Diego Zamboni, "Intrusion detection using autonomous agents", Computer Networks 34, pp.547-570, 2000.

[13] Jaffrey M. Bradshaw, "An Introduction to Software Agents", In Jeffrey M. Bradshaw, editor, Software Agnets, chapter 1. AAAI Press/The MIT Press, 1997.

[14] Danny B. Lange, Mitsuru Oshima, "Programming and Deploying JAVA™ Mobile Agents with Aglet", Addison Wesley, 1998.