분산 침입 탐지 통신 메커니즘의 성능 향상에 관한 연구

*장 정 숙, 전 용 희

*대구가톨릭대학교 공과대학 컴퓨터정보통신공학부

A Study on the Performance Enhancement of Communication Mechanism for Distributed Intrusion Detection

Jang Jung-Sook, Jeon Yong-Hee

*School of Computer and Info. Comm. Engineering,
College of Engineering, Catholic University of Daegu

요 약

분산 침입 탐지시스템은 감시되는 호스트 수에 비례하여 데이터 분석이 다수의 위치에서 수행되는 시스템이다. 따라서, 침입 탐지를 위하여 구성된 컴포넌트 사이의 효율적인 정보 분배가 중요한 문제이며, 통신 메커니즘은 신뢰성, 효율성, 안전성 그리고 확장성이 요구된다. 분산 침입 탐지 시스템의 통신 형태를 나타내는 통신모델 중에서, 높은 확장성때문에 고려되고 있는 모델로 피어 대 피어 통신 모델이 있다. 이 모델은 특정한 형태의 관심 전파와 데이터 전달 방법에 따라 다시 계층적 구조와 직접 연결로 분류할 수 있다. 본 논문에서는, 분산 침입탐지에서 침입 탐지정보를 전달하는 두 가지 방법에 대하여 분석하고, 통신 메커니즘의 성능을 향상시키는 방안을 제시하고자 한다.

I. 서론

침입 탐지에 대한 연구는 중앙 통제형과 단일 프레임워크로부터 분산 침입 탐지 형태로 발전해 왔다. 분산 침입 탐지 시스템은 데이터 분석이 감시되는 호스트 수에 비례하여 다수의 위치에서 수행되는 시스템이다. 분산 침입 탐지 시스템에서는 침입 탐지를 위한 통신 모델과 데이터 모델이 적절하게 선택되어야 한다. 침입 탐지를 위하여 구성된 컴포넌트 사이 효율적인 정보 분배는 분산 침입 탐지 시스템에서의 중요한 문제이며, 신뢰성, 효율성, 안전성 그리고 확장이 가능한 통신 메커니즘을 가지는 통신 모델이 필요하다. 침입 탐지를 위한 분산 통신 모델로는 클라이언트-서버 모델과 피어 대 피어 모델이 있다. 기존의 침입탐지 시스템인 DIDS[1], GrIDS[2], EMERALD[3] 그리고 AAFID[4]는 침입 탐지 정보를 단순한 계층형 혹은 중앙통제형으로 분석한다. 따라서 기존의 침입 탐지 시스템은 계층적인 분석, 데이터의 정련 문제, 계층의 모든 단계에서 부피가 큰 모듈 보유 및 정적인 상호작용 등의 단점을 가진다. 그러므로 분산 침입 탐지 시스템에서 탐지 정보의 분석은 에이전트(agent)화, 탐지 정보의 분석이 계층적이 아닌, 침입의 형태를 특정한 관심(interest)의 개념을 사용하여 지능적인 협력을 하며, 관심과 데이터 전송을 효율적으로 분배하는 전파방법, 침입 탐지 정보를 분배하는 컴포넌트 사이의 동적인 통신, 그리고 탐지 정보의 분석을 위한 모든 계층적 단계에서 초경량 모듈의 사용에 대한 연구가 진행되고 있다.

[5]에서 분산 통신 모델의 비교를 통하여 피어 대 피어(peer-to-peer) 통신 모델기반이 높은 확장성 때문에 고려되고 있는 것으로 분석되었다. 피어 대 피어 통신 모델은 다시 이벤트기반 모델과 푸시기반 모델로 분류된다. 한편, 특정한 형태의 침입 탐지 정보를 전달(delivery)하는 방법에 따라 계층적인 전달(hierarchical delivery)과 직접 전달(direct delivery)이 있다. 본 논문에서는 분산 침입 탐지 관련 정보인 관심과 데이터를 전달하는 두 가지 방법에 대하여 분석하고, 분산 침입 탐지를 위한 통신 메커니즘의 성능을 향상시키는 방안을 분석하고자 한다.

본 논문은 다음과 같은 순서로 구성된다. 먼저 2절에서는 분산 침입 탐지 시스템에 대하여, 3절은 분산 침입 탐지 통신 모델, 4절은 침입 탐지에 대한 통신 메커니즘의 성능 향상 방안을 기술하고, 마지막으로 5절에서는 요약과 향후 계획으로서 끝을 맺는다.

II. 분산 침입 탐지 시스템

일반적인 침입 탐지 시스템 모델인 CIDF[6]는 이벤트를 생성하는 이벤트 생성기, 생성한 이벤트를 분석하는 이벤트 분석기, 이벤트 생성기와 이벤트 분석기가 생성한 데이터를 저장하는 방법을 정의하고 저장하는 이벤트 데이터베이스 그리고 침입 탐지 분석에 대한 대응을 하는 대응 장치로 구성되어 있다.

분산 침입 탐지 시스템은 데이터의 분석이 모니터 되고 있는 호스트 수에 비례하여 다수의 위치 상에서 수행되는 시스템으로 정의된다[7]. 이 정의에 따르면 단순한 분산 데이터 수집(이벤트 생성기)만을 수행하는 침입 탐지 시스템을 분산 시스템으로 분류하지는 않으며 분석 컴포넌트(이벤트 분석기)가 모니터 되는 호스트 수에 비례하고 위치가 분산되어야 한다. 분산 침입 탐지 시스템에서 다른 컴포넌트들 사이 효과적인 통신메커니즘을 결정하는 요인은 다음과 같다[7].

- 컴포넌트의 수: 컴포넌트의 수에 따라 통신 오버헤드가 증가.
- 컴포넌트의 위치: 호스트 내 통신과 호스트 간 통신으로 컴포넌트 사이 통신의 형태가 컴포넌트의 위치에 따라 구별.
- 데이터의 형태: 감사 추적과 원시 네트워크 트래픽 그리고 축약된 감사 혹은 경보 같은 각기 다른 종류의 침입 탐지 시스템 데이터 형태를 고려.
- 데이터 양: 고려되는 데이터의 양이 많다면 수집 컴포넌트 가까이 분석기 컴포넌트를 위치시키는 것이 효율적.
- 데이터 생성빈도: 데이터의 발생빈도가 높으면 비 연결형 메커니즘보다는 연결형 통신 메커니즘을 사용하는 것이 효율적.
- 데이터 표현 방법: 데이터의 표현 방법에 따라 통신 메커니즘의 선택과 데이터의 크기에 영향.
- 데이터의 민감성: 침입 탐지를 위한 컴포넌트의 모니터는 가장 민감한 데이터에 대하여 접근을 하므로 컴포넌트 사이 데이터교환을 교환하는 메커니즘은 비밀성과 인증같은 보안에 대한 보증을 고려.

분산 침입 탐지 시스템을 위한 통신 메커니즘에서 요구하는 특성은 신뢰성, 보안(인증, 무결성, 부인봉쇄, 비-복제, 서비스 거부공격에 대한 저항), 확장성, 속도 등이 있다.

Ⅲ. 분산 침입 탐지 통신 모델

[5]에서는 분산 통신 모델의 비교를 수행하였으며, 그 결과 피어 대 피어 통신 모델이 분산 침입 탐지에 의한 컴포넌트 사이 탐지 정보의 효율적 분배를 제공하므로, 본 절에서는 이에 대하여 기술한다[8,9].

피어 대 피어 통신 모델에는 그림 1에서 보는 것처럼 중앙 통제형, 계위형, 분산형의 위상 형태가 있다.

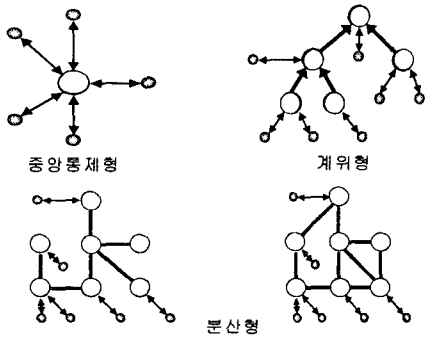


그림 1: 피어 대 피어 통신 위상 형태

피어 대 피이 통신 모델에서 정보 생산자는 정보의 정확한 형태를 이용하기를 광고하고, 관심을 가진 소비자는 이 정보를 구독하고, 그리고 생산자는 정보를 출판한다. 피어 대 피어 통신은 새로운 개념은 아니며 PC의 속도, 처리 능력의 향상으로 피어들 간 서로 이용 가능한 추세이다. 피어 대 피이 통신 모델에는 이벤트 기반[10]과 푸시 기반 통신 모델[8]이 있다. 표 1은 피어 대 피어 통신에서 이 두 가지 모델의 특성을 비교 기술한다.

표 1: 피어 대 피어 통신 모델

이벤트 기반 시스템	푸시 시스템
어떤 객체도 이벤트 생산과 소비 가능	특정한 생산자 그리고 소비자
동기적 역할	비동기 역할
느슨한 연결	논리적인 채널
높은 확장성	밀접한 결합
이벤트 광고, 관심 명세 그리고 이벤트 통지	적은 확장성

Ⅳ. 침입탐지 통신 메커니즘의 성능 향상 방안

분산 침입 탐지 시스템을 구성하는 컴포넌트 사이에서 관심과 데이터 전송에 대한 효율적인 정보의 분배를 요점으로, 피어 대 피어 통신 모델의 계위형 위상 구조를 적용한다.

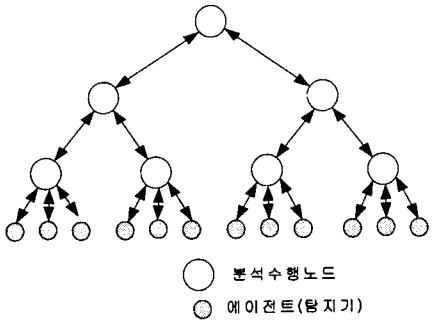
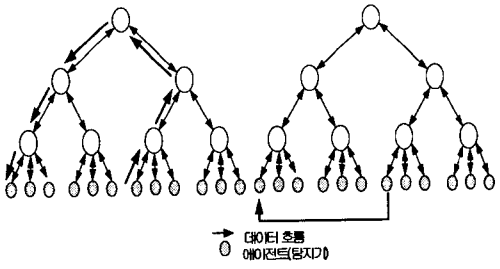


그림 2: 분산 침입 탐지를 위한 계위형 모델

그림 2에서는 분산 침입 탐지를 위한 계위형 모델의 모형을 나타낸다. 그림 3은 관심을 표현하는 에이전트에게 데이터를 전달하는 방법을 보여준다. 특정한 형태의 침입 탐지 정보인 관심과 데이터 전송을 전달(delivery)하는 방법으로 계위적인 전달(hierarchical delivery)(a) 그리고 데이터가 계위를 통하지 않고 에이전트에게 직접 전달(direct delivery(b))되는 방안이 있다. 분산 침입 탐지 시스템에서 관심의 계위적인 전달은 낮은 단계에서 높은 단계로 데이터를 보낸다.

분산 침입 탐지의 통신 메커니즘에 대한 성능을 향상시키는 방안으로 전송 시 모듈의 실패, 확장성, 데이터 협력을 분석하여 통신의 오버헤드를 줄이는 것이 있다.



(a). 계위를 통한 경로 사용 (b). 직접 연결을 사용

그림 3: 탐지 정보를 전달하는 두 가지 방법

그림 3에서 에이전트는 호스트에서 미리 정의된 보안 모니터링 기능을 수행한다. 에이전트 기능은 호스트에 첨부되어 호스트 혹은 네트워크의 보안에 관계한다. 에이전트는 에이전트사이 협력을 제공하며 이벤트 혹은 경보의 요청에 따라 에이전트는 동적인 대응을 한다. 에이전트는 이벤트 혹은 경보로 관심을 표현한다.

데이터 전달방법에서 계위적인 전달과 직접 전달은 모두 다음과 같은 측면에서 장점과 단점을 가지고 있다[7]. 따라서, 본 논문에서는 두 모델의 장점을 살린 통합 모델을 제시하고자 한다.

• 모듈의 실패

더 높은 단계에서 모듈의 이벤트가 침입자에 의해 계위가 훼손되거나 붕괴되거나 혹은 억제된다면 IDS의 탐지 능력에 중요한 영향을 미친다. 만약 에이전트 사이 데이터 전송이 계위 경로를 통하여 전송된다면 이것은 장애 모듈 때문에 억제될 것이다. 다르게 이야기하면 에이전트 사이에서 직접적인 데이터 전송을 한다면 장애모듈의 문제는 해결된다.

• 확장성

여러 개의 도메인을 서로 연결한 대규모 엔터프라이즈에서는, 수천 개의 호스트와 비례하는 에이전트 수가 있다. 서로 직접 데이터를 통신하는 에이전트는 최악의 경우에 수천 개의 연결이 될 수 있다. 만약 같은 목적지 에이전트와 통신할 때 에이전트가 연결을 공유하는 최적화를 고려하더라도, 단일 에이전트의 관심을 서비스하는 다른 호스트가 수백 개의 에이전트를 가진다면 그 수는 엄청날 것이다. 이것은 연결 수 관점에서 확장성의 결여를 가져온다. 하지만 계위적인 데이터 전달 프레임워크를 사용한다면 호스트의 부하 문제는 해결된다.

• 데이터 협동

에이전트가 다중 에이전트에게 같은 관심을 서비스한다면, 계위에서 목적지 에이전트로 같은 경로를 통하여 데이터의 단일 복사를 보내고, 계층의 적절한 단계에서 이것을 복제하여, 개별 에이전트들에게 보낼 수 있다. 이런 형태의 데이터 협동(coalescing)은 서비스된 에이전트가 에이전트 사이에서 데이터를 직접 통신하는 경우에 같은 호스트에 소속된다면 단지 가능하여진다.

V. 결론과 향후 계획

본 논문에서는 분산 침입 탐지를 위한 통신 메커니즘의 성능을 향상시키는 방안에 대하여 분석하였다. 침입 탐지를 위하여 구성된 컴포넌트 사이 효율적인 정보 분배를 위하여 신뢰성, 효율성, 안전성 그리고 확장이 가능한 통신 메커니즘이 필요하다. 효율적인 분산 침입 탐지를 위한 분산 통신 메커니즘을 위하여 피어 대 피어 통신 모델을 적용하였다. 분산 침입 탐지의 다른 컴포넌트 사이 효과적인 통신 메커니즘을 결정하는 요인으로는 컴포넌트의 수, 컴포넌트의 위치, 데이터의 형태, 데이터의 양, 데이터의 생성빈도, 데이터의 표현방법 그리고 데이터의 민감성이 있으며, 피어 대 피어 통신 위상에서 계위형 위상을 적용하였다. 관심의 전달을 위해 계위적인 전달과 직접 전달 방법 사이의 모듈의 실패, 확장성, 그리고 데이터 협력 관점에서 장점과 단점을 기술하였다. 결론적으로, 관심의 분류에 의하여 계위적인 전달과 직접 전달 두 메커니즘을 통합하여

사용한다면 관심 전파와 데이터 전송에서 통신의 오버헤드를 줄이고 확장성의 문제를 할 수 있을 것으로 예상된다.

향후 계획으로는 분산 침입 탐지에 대한 피어 대 피어 통신 모델에서 계위형 위상을 적용하여 관심 전파와 데이터 전송에서 계위적인 전달과 직접 전달을 시뮬레이션하여 통신 오버헤드와 확장성을 정량적으로 비교 검증해보는 것이다.

참 고 문 헌

[1] S. Snapp, J. Brentano, and G. Dias et al. DIDS (Distributed Intrusion Detection System) motivation, architecture, and an early prototype. In Proceedings of the 14th National Computer Security Conference, October 1991.

[2] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, and D. Zerkle. GrIDS-a graph based Intrusion detection system for large networks. In Proceedings of the 19th National Information Systems Security Conference, September 1996.

[3] Phillip A. Porras and Peter G. Neumann. EMERALD: event monitoring enabling responses to anomalous live disturbances. In 1997 National Information Systems Security Conference, Oct 1997.

[4] Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, Eugene Spafford, and Diego Zamboni. An architecture for intrusion detection using autonomous agents. In Proceedings of the Fourteenth Annual Computer Security Applications Conference, pages 13 24. IEEE Computer Society, December 1998

[5] 장정숙, 전용희, 장종수, 손승원, "분산 침입 탐지 시스템을 위한 통신 모델", 한국통신학회지, pp.1034-1049. 2002년 8월.

[6] http://www.isi.edu/gost/cidf/

[7] Rajeev Gopalakrishna, Eugene H. Spafford, A Framework for Distributed Intrusion Detection using Interest-Driven Cooperating Agents. Center for Education and Research in Information Assurance and Security, Purdue University.

[8] M. Hauswirth and M. Jazayeri. A component and communication model for push systems. In Proceedings of ESEC/FSE 99 - Joint 7th European Software Engineering Conference (ESEC) and 7th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE-7), Toulouse, France, September 1999

[9]Dipl.-Ing. Manfred Hauswirth. Internet-Scale Push Systems for Information Distribution Architecture, Components, and Communication. Institut fur Informations systeme, August 1999.

[10]A. Carzaniga, D.S. Rosenblum, and A.L. Wolf "Design and Evaluation of a Wide-Area Event Notification Service". ACM Transactions on Computer Systems, 19(3):332-383, Aug 2001.