물류서버를 위한 침입 탐지 시스템의 경보데이터 관리+

신문선*, 이종연**, 노기용*
*표준과학연구원
**충북대학교
e-mail:msshin9@nate.com

Management of Alert Data from Intrusion Detection System of EPC-IS

Moon-Sun Shin*, Jong-Yun Lee**, Ki-Yong No*
*Korea Research Institute of Standards and Science
**Chungbuk National University.

요 약

최근 침입 탐지 시스템으로부터 생성되는 대량의 경보데이터에 대한 관리와 경보상관관계 분석 결과를 침입탐지시스템의 능동적인 대응에 활용하고자 하는 연구가 많이 시도되고 있다. 기존의 침입 탐지 시스템은 알려진 공격 형태를 탐지하는 것은 가능하지만 변형된 형태의 공격이나 새로운 형태의 공격의 탐지는 어렵다. 이 논문에서는 침입 탐지시스템의 체계적인 경보데이터관리 및 경보데이터 상관관계 분석을 위하여 데이터마이닝 기법을 적용한 경보 데이터 마이닝 프레임워크를 제안한다.

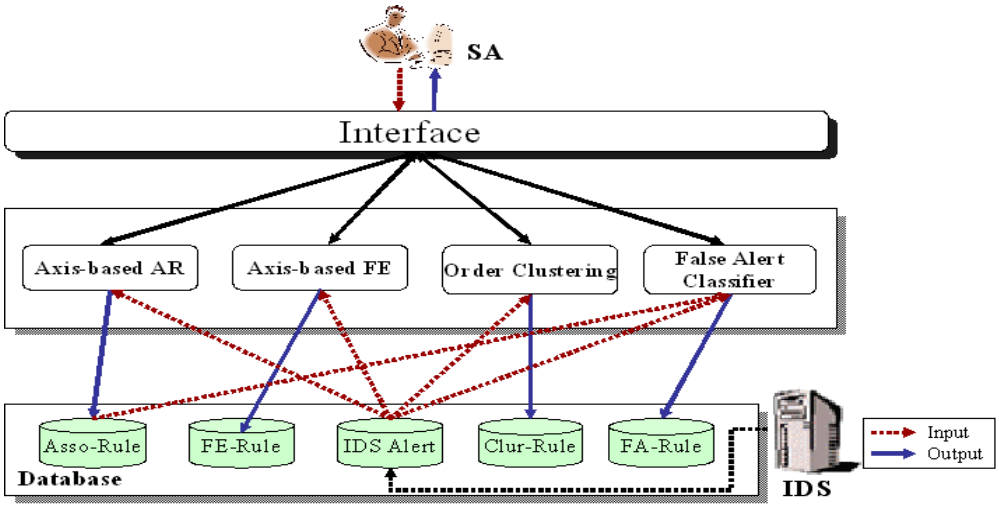
1. 서론

최근 인터넷의 역기능으로 사이버 테러, 인터넷 대란 등의 컴퓨터를 이용한 침입행위가 빈번히 발생하고 있다. 그러나 개방형 네트워크의 특징을 가지고 있는 인터넷의 구조상 침입행위를 차단하는 것이 용이하지 않다. 따라서 침입탐지시스템을 설치하여 각 조직의 자원이나 시스템을 보호하고 있다. 침입탐지시스템은 악의적인 공격으로부터 컴퓨터시스템과 네트워크 시스템을 보호한다. 그러나 이질의 침입 탐지 시스템으로부터 대량의 경보데이터가 중복발생되며 경보의 중복과 과다는 경보데이터 그 자체가 서비스 거부공격으로 오인되는 역기능을 초래하게 된다. 최근 침입 탐지 시스템으로부터 생성되는 대량의 경보데이터에 대한 관리와 경보상관관계 분석 결과를 침입탐지시스템의 능동적인 대응에 활용하고자 하는 연구가 많이 시도되고 있다. 이 논문에서는 침입 탐지시스템의 체계적인 경보데이터관리 및 경보데이터 상관관계 분석을 위하여 데이터마이닝 기법을 적용한 경보 데이터 마이닝 프레임워크를 제안한다. 이 논문에서 제안한 경보 데이터 마이닝 프레임워크는 기존의 경보데이터 상관관계분석에서는 해결하지 못했던 통합적인 경보 상관관계 분석 기능을 수행할 뿐만 아니라 대량의 경보데이터에 대한 필터링을 수행하는 장점을 가진다. 또한 추출된 규칙 및 공격시나리오는 침입탐지시스템의 실시간 대응에 활용될 수 있다.

+ 본 논문은 2008년도 지식경제부 성장동력기술개발 사업의 일환으로 (주)메타비즈의 위탁과제로 수행되었음

2. 관련 연구

침입탐지시스템에서는 침입 혹은 공격에 대하여 경보데이터를 발생시킨다. 따라서 보안 관리자는 침입탐지시스템의 경보를 항상 모니터링 하여야 한다. 그러나 대량의 경보데이터 발생과 오경보의 발생 등은 침입탐지시스템의 성능을 저하시키는 결과를 초래하게 된다. 따라서 경보데이터의 통합 관리와 경보 상관성 분석, 오경보 감소 등을 위해서 경보 데이터를 분석하고, 이를 이용하여 공격의 시퀀스를 추출하고 오경보를 분류하거나 경보데이터 필터링 등을 수행한다. [2]에서는 발견 학습을 이용한 접근방법을 “포트탐지공격(stealthy portscan)”을 탐지



[그림 1] 경보 데이터 마이닝 프레임워크

하기 위해 적용하였다. 비록 발견 학습을 경보 데이터 상관관계 분석에 이용하였지만, 이 방법 또한 경보 데이터 간의 인과 관계를 완벽하게 분석하지 못하였다.

[3]은 경보 데이터의 통합과 상관관계 분석 기법을 제안하였다. 특히, [3]에서 제안된 상관관계 분석 방법은 어떤 타입의 경보가 주어진 경보 유형의 다음에 오는지를 기술하기 위한 결과 메커니즘을 이용하였다. 이것은 오용 탐지 기법과 유사하다.

프랑스의 CERT에서는 경보데이터관리를 위한 데이터베이스 스키마를 설계하고 XML형태의 경보들을 통합하여 클러스터링과 병합과정을 거쳐 상관관계분석을 하고 공격에 대한 광역 진단을 결정하는 프레임워크를 마련하는 프로젝트[4]를 진행하였다.

따라서 이 논문에서는 침입탐지시스템을 위한 데이터 마이닝 기법 기반 경보 상관 관계 분석과 오경보 분류 기능을 지원하는 경보 데이터 마이닝 프레임워크를 제안한다.

3. 경보데이터 마이닝 프레임워크

침입탐지시스템에서 대규모 생성되는 경보데이터의 효율적인 관리를 위해서 기존의 데이터 마이닝 기법을 확장 적용하여 속성기반 연관규칙, 속성기반 빈발에피소드, 순서기반 클러스터링, 그리고 오경보 분류모델 등으로 구성되는 경보 데이터 마이닝 프레임워크를 제안한다. 제안된 경보데이터 마이닝 프레임워크의 구성은 그림 1과 같다.

각 구성요소들을 살펴보면 속성기반 연관규칙 컴포넌트는 경보데이터 속성 간의 연관성을 추출하는 기능을 수행하게 되며 속성기반 빈발에피소드 컴포넌트는 주어진 타임윈도우내에서 경보간 연관성을 탐사한다. 순서기반 클러스터링 컴포넌트는 경보데이터를 클러스터링하여 경보축약을 지원하며 또한 각 클러스터간의 순서를 이용하여 경보 시퀀스를 유추하여 경보 이후의 가능한 경보를 예측하는 기능을 수행한다.

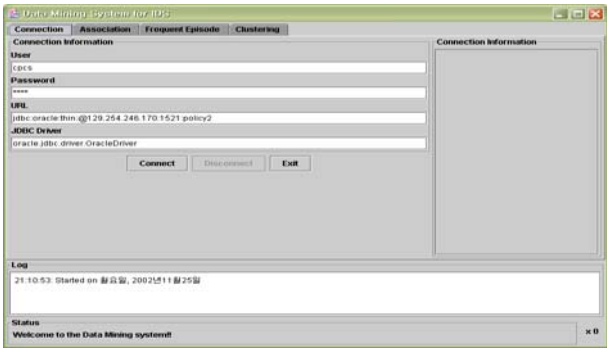
오경보 분류 컴포넌트는 훈련데이터를 이용하여 오경보 분류 모델을 생성하여 테스트 데이터가 주어지면 생성된 결정트리를 이용하여 오경보인지 아닌지를 분류하는 기능을 수행한다. 이는 침입탐지시스템의 앞단 혹은 뒷단에서 오경보 필터링에 활용될 수 있다.

4. 프로토타입 구축

침입탐지시스템에서 네트워크 패킷데이터는 원시 데이터이기 때문에 관계형 데이터베이스에 저장하기 위해서는 데이터 가공이 필수적이다. 따라서 원시 데이터에서 속성을 추출하여 데이터베이스에 저장하기 위해 전처리 프로세서 모듈을 이용하여 아스키 형태로 변환하였다[6]. 먼저 네트워크 패킷 데이터를 수집하여 전처리 프로세서를 거친 후 경보데이터 마이닝 시스템에서 저장된 경보데이터들을 추출하여 오경보 분류, 경보시퀀스 추출, 유사 경보 축약 등의 기능을 수행할 수 있는 프로토타입을 그림 2와 같이 구축하였다.

JDBC 드라이버를 이용하여 데이터베이스에 접속한 후 해당 테이블 리스트를 가져온다. 마이닝 하고자 하는 데이터가 저장된 테이블을 지정할 수 있다. 오라클인 아닌 다른 DBMS의 테이블을 선택하는 것도 가능하도록 하였다. 데이터베이스에 접속 할 UID,

Password, URL, JDBC 드라이버이름을 입력 한 후 데이터베이스에 접속한다. 연과규칙,빈발에피소드, 클러스터링 탭을 선택하여 각각의 마이닝 작업을 수행한다.



[그림 2] 경보데이터 관리시스템 프로토타입

5. 실험

구축된 프로토타입은 경보데이터 관리를 위한 경보데이터 마이닝 프레임워크로 침입탐지시스템으로부터 생성되는 경보데이터를 대상으로 실험을 하였다. 실제 경보데이터를 대상으로 연관 규칙 탐사와 빈발에피소드 탐사를 수행한 결과를 검토하고 적용한 예를 기술한다.

[표 1] 탐사된 연관규칙 의미

Association Rule	Meaning
50<=>21 (supp : 49,conf : 83%,)	Attribute 50(Atid) correlated with attribute 21(dsc_port)
21<=>tcp (supp : 49,conf : 98%,)	Attribute 21(dsc_port) correlated with attribute tcp(protocol)

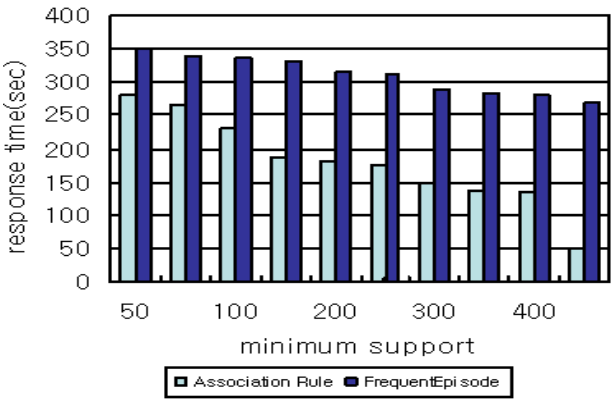
표 1 에서 보이듯이 이러한 룰들은 지지도와 신뢰도에 근거한 신뢰성 정보라고 할 수 있다. 예를 들면 공격아이디가 50은 목적지포트번호 21번과 연관되어 있다는 것을 알 수 있다. 즉 연관규칙 마이너를 통해서 공격아이디속성과 목적지포트번호속성은 서로 밀접한 관계가 있다는 사실을 추출할 수 있다. 빈발에피소드 최종 룰의 의미를 정리하면 표2와 같다.

[표 2] 빈발에피소드 규칙

Frequent Episode Rule	Meaning
5001:210.155.167.10:21:tcp ⇒ 5007:210.155.167.10.21:tcp (fre : 10, conf : 9%, time : 10sec)	If 5001(Ftp Buffer Ovrflow) occur, then 5007(Anonymous FTP) occur together.

표 2에서처럼 빈발 에피소드 마이너를 실행시킨 경우도 최종 규칙을 살펴보면 5001공격 다음에 5007 공격이 일어난다는 것을 알 수 있다.

또한 프로토타입의 성능 분석을 위해 속성기반 연관규칙과 속성기반 빈발에피소드 수행 시 최소 지지도 변경에 따른 수행 시간에 대한 실험 결과를 보여준다. 실험에서 사용된 경보데이터는 32000개의 레코드이며 최소지지도를 20%, 15%, 10%, 5% 씩 줄여가면서 실험을 하였다.



[그림 3] 최소 지지도 변경에 따른 수행시간

그림 3 은 32000개의 데이터집합에 연관규칙과 빈발에피소드의 최소지지도를 줄여 가면서 실행시간을 측정한 결과를 보여준다. 그 결과 연관규칙에서는 지지도가 작을수록 데이터베이스에서 생성되는 후보항목 수가 많아지므로 그만큼 수행시간도 오래 걸린다.

6. 결론

유비쿼터스 환경에서 안전한 물류 서비스를 위해서는 침입탐지시스템, 방화벽, 침입방지시스템 등의 보안솔류션의 설치가 필수적이다. 이러한 침입탐지시스템으로부터의 대량의 경보데이터 발생은 경보의 중복 발생 및 경보 과다로 인한 침입탐지시스템의 성능을 저하시키는 원인이 된다.

따라서 이 논문에서는 경보 데이터 통합관리 및 경보상관관계 분석을 위한 경보 데이터마이닝 프레임워크를 제안하였다. 아울러 제안된 프레임워크의 프로토타입을 구현하여 데이터 마이닝기법 기반 경보데이터 통합관리 및 경보상관관계분석에 적용하고 실험 평가하였다. 경보 데이터의 체계적인 통합 관리와 경보 상관관계 분석을 위해 경보데이터들이 데

이터베이스에 저장되어야하므로 전처리 과정을 통해 경보데이터를 저장하고 경보데이터 마이닝 태스크를 수행할 수 있도록 경보데이터 스키마를 설계하고, 데이터마이닝기법 기반 경보데이터 통합 관리 프레임워크 구축하였다. 기존의 데이터마이닝기법의 알고리즘을 경보데이터의 특성에 맞게 확장 설계하였다. 설계된 알고리즘은 경보데이터의 특성을 고려하여 관심있는 항목에 대한 지식탐사를 가능하게 하였으며 경보들중 오경보를 감소시키는 기능도 수행하는 장점을 가진다. 향후 침입탐지시스템의 시그네쳐나 규칙에 추가할 수 있도록 하는 에이젼트 개발에 대한 연구가 계속되어야할 것이다.

참고문헌

[1] Moon Sun Shin, HoSung Moon, KeunHo Ryu, JinOh Kim and KiYoung Kim, "Applying Data Mining Techniques to Analyze Alert Data", APWeb2003, LNCS 2642 pp.193-200, SpringerVerlag.

[2] A. Valdes and K. Skinner, "Probabilistic alert correlation", In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001), pages 5468, 2001.

[3] P. Ning and Y. Cui., "An intrusion alert correlator based on prerequisites of intrusions", Technical Report TR-2002-01, Department of Computer Science, North Carolina State Univ., Jan. 2002.

[4] D. Curry and H. Debar, "Intrusion detection message exchange format data model and extensible markup language document type definition", Internet Draft, draft-ietf-idwg-idmef-xml-03.txt, Feb. 2001.

[5] R. Agrawal, T. Imielinski, and A. Swami. "Mining association rules between sets of items in large databases" In Proceedings of the ACM SIGMOD Conference on Management of Data, pp. 207-216, 1993.

[6] 신문선, 류근호, “침입탐지시스템의 성능향상을 위한 오경보 분류 모델 구현”, 정보과학회논문지:데이터베이스 2007년 12월