데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도 향상에 관한 연구

송중석[O*] 高倉弘喜** 岡部寿男** 권용진***

*경도대학 대학원 정보학연구과 **경도대학 학술정보 미디어 센터 ***한국항공대학교 정보통신공학과
oaktree@net.ist.i.kyoto-u.ac.jp[O*] takakura@media.kyoto-u.ac.jp** okabe@i.kyoto-u.ac.jp** yjkwon@tikwon.hangkong.ac.kr***

A Study on Accuracy Improvement of Intrusion Detection System Based on Data Mining

Jungsuk Song[O*] Hiroki Takakura** Yasuo Okabe** Yong-Jin Kwon***
*Graduate School of Informatics, Kyoto University **Academic Center for Computing and Media Studies, Kyoto University
***Dept. of Info. & Telecom. Eng., Hankuk Aviation University

요 약

공격 방법의 다양화와 지능화에 대응하기 위해 침입탐지시스템(IDS)의 성능도 향상되고 있다. 특히, 데이터 마이닝 기반의 침입탐지시스템은 기존 침입탐지시스템의 많은 문제점을 개선시켰다. 그러나 데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도가 트레이닝 데이터(training data)에 포함된 속성(features)과 선택된 *axis* 및 *reference* 속성에 의해 결정됨에도 불구하고 현재의 데이터 마이닝 기반의 침입탐지시스템은 트레이닝 데이터에 포함된 고유의 속성만을 고려하기 때문에 탐지 정확도를 향상시키는 데는 한계가 있다. 따라서 본 논문에서는 데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도를 향상시키기 위하여 기존 데이터 마이닝 기반의 침입탐지시스템이 고려했던 고유의 속성 외에 침입과 밀접하게 관련되고 *axis* 및 *reference* 속성으로도 사용될 수 있는 새로운 속성을 제안한다.

1. 서론

네트워크 기반 컴퓨터 시스템은 그 역할이 더욱 중요해짐에 따라 많은 공격자들의 공격 대상이 되고 있다. 이러한 컴퓨터 시스템을 보호하기 위해 사용자 인증(User Authentication), 암호화(Encryption) 등의 침입 방지 기술 외에 침입 탐지 기술이 사용되고 있다.

침입 탐지 기술에는 오용탐지(misuse detection)와 비정상행위탐지(anomaly detection)가 있다. IDIOT[1]이나 STAT[2]와 같은 오용탐지 시스템은 알려져 있는 공격 행위로부터 특정 공격 패턴을 추출해내고, 분석 대상에 추출해낸 공격패턴이 존재할 경우 침입으로 판단한다. 반면에 IDES[3]와 같은 비정상행위탐지 시스템은 정상적인 행위의 범위를 정하고 이러한 정상적인 행위를 벗어나는 모든 행위를 비정상행위로 규정하고 탐지한다.

침입탐지시스템의 성능에 있어서 확장성과 융통성도 중요하지만 가장 중요한 요소는 탐지 정확도이다. 특히, 공격 방법이 점점 다양화되고 지능화되어가고 있는 현재 상황에서 기존에 알려진 공격이 아닌 새로운 공격 방법에 대한 탐지는 무엇보다 중요하다. 이러한 목적을 위해 침입탐지시스템의 성능은 계속해서 향상 되었고, 그중에서도 데이터 마이닝에 기반한 침입탐지시스템[4]은 기존 침입탐지시스템의 많은 문제점을 개선시켰다. 특히, 확장성과 융통성의 측면에서 괄목할만한 성장을 가져왔고 또한 새로운 공격 방법에 대한 탐지도 가능해 졌으나 탐지 정확도를 향상시키는 데는 아직 한계가 있다.

따라서 본 논문에서는 데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도를 향상시키기 위한 방법을 제안한다. 데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도가 트레이닝 데이터(training data)에 포함된 속성(features)과 선택된 *axis* 및 *reference* 속성에 의해 결정됨에도 불구하고 현재는 트레이닝 데이터에 포함된 고유의 속성만을 고려하고 있기 때문에 탐지 정확도를 향상시키는 데는 한계가 있다[5]. 따라서 본 논문에서는 데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도를 향상시키기 위하여 기존 데이터 마이닝 기반의 침입탐지시스템이 고려했던 고유의 속성 외에 침입과 밀접하게 관련되고 *axis* 및 *reference* 속성으로도 사용될 수 있는 새로운 속성을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 데이터 마이닝 기반의 침입탐지에 대해 알아보고 3장에서는 데이터 마이닝에 기반한 침입탐지시스템의 정확도를 향상시키기 위한 새로운 속성을 제안한다. 마지막으로 4장에서 결론을 맺는다.

2. 데이터 마이닝 기반의 침입탐지

그림 1은 데이터 마이닝에 기반한 침입탐지 모델의 구축과정을 나타낸다[6]. 침입탐지 모델의 구축과정은 다음과 같다. raw(binary) audit data는 ASCII 형식의 패킷으로 바뀌고 전처리 과정을 통하여 ASCII 형식의 패킷으로부터 커넥션 레코드(connection records)가 생성된다. 커넥션 레코드는 source host, source port, service 등의 많은 속성을 포함하고 있다. 커넥션 레코드에 데이터 마이닝, 즉 연관 규칙 생성 알고리즘[7]과 빈발 에피소드 생성 알고리즘[8]을 적용하여 연관 규칙(association rules)과 빈발 순차 패턴(frequent sequential patterns)을 차례로 생성한다. 생성된 빈발 순차 패턴으로부터 속성 생성 알고리즘[6]을 이용하여 새로운 속성을 생성하고, 생성된 속성이 커넥션 레코드에 추가되게 된다. 마지막으로 RIPPER[9]와 같은 분류 프로그램(classification program)을 통하여 새로운 속성이 추가된 커넥션 레코드로부터 탐지 룰(rules)을 만듦으로써 탐지 모델이 구축되게 된다.

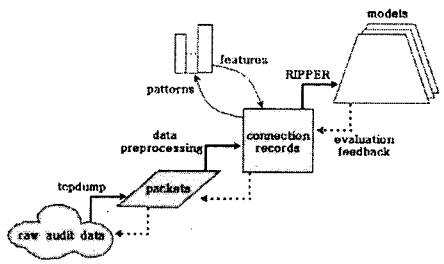

그림 1 데이터 마이닝 기반의 침입탐지모델 구축과정

커넥션 레코드는 source host, source port, destination host, destination port, service, duration, flag(프로토콜에 따라서 정상

또는 에러 상태를 나타냄) 등과 같은 많은 고유의 속성을 가지고 있다. 그림 2는 syn flood 공격에 관한 커넥션 레코드의 예이다. 공격자는 매우 짧은 시간에 victim 호스트로 많은 S0 연결(단지 첫 번째 SYN 패킷만 보냄)을 하나의 포트(80)에 보내기위해 조작된 IP를 사용했음을 알 수 있다.

time	duration	service	src_host	dst_host	flag	···
1.1	0	http	spoofed_1	victim	S0	···
1.1	0	http	spoofed_2	victim	S0	···
1.1	0	http	spoofed_3	victim	S0	···
1.1	0	http	spoofed_4	victim	S0	···
1.1	0	http	spoofed_5	victim	S0	···
···	···	···	···	···	···	···
10.1	2	ftp	A	B	SF	···
13.4	60	telnet	A	D	SF	···
···	···	···	···	···	···	···

그림 2 커넥션 레코드

커넥션 레코드에 연관 규칙 생성 알고리즘[7]을 적용하여 커넥션 레코드의 속성들 사이의 연관 규칙을 생성한다. 연관 규칙 생성 시 가장 중요한 것은 *axis* 와 *reference* 속성[5]의 선택이다. 어떤 속성을 *axis* 와 *reference* 속성으로 선택했느냐에 따라 침입 탐지 모델의 성능이 결정되기 때문이다[5]. 일반적으로는 service 속성을 *axis* 속성으로, destination host 속성을 *reference* 속성으로 사용한다. 왜냐하면 일반적으로 침입은 네트워크에 있는 몇몇 호스트를 침입 대상으로 하고 해당 호스트의 많은 포트(즉, service)에 연결하기 때문이다. 그림 3은 커넥션 레코드에서 service 속성을 *axis* 속성으로 하고 destination host 속성을 *reference* 속성으로 선택해서 생성된 연관 규칙의 예이다.

연관 규칙
($flag = SF$, $service = http$, $src\_bytes = 200$)
($service = icmp\_echo$, $dst\_host = host_B$)
($flag = S0$, $service = http$, $src\_host = host_A$)
($service = user\_app$, $src\_host = host_A$)
···

그림 3 연관 규칙

연관 규칙에 빈발 에피소드 알고리즘[8]을 적용하여 빈발 순차 패턴을 생성한다. 빈발 순차 패턴 생성 시 일반적인 빈발 에피소드 알고리즘과는 달리 먼저 *axis* 속성에 관한 빈발 연관 규칙(frequent associations)을 생성하고 이들 빈발 연관 규칙으로부터 빈발 순차 패턴을 생성한다[5]. 그 결과 속성들 사이의 연관 규칙과 레코드들 사이의 순차패턴을 하나의 룰로 결합하게 된다. 그림 4는 빈발 에피소드 알고리즘으로부터 생성된 침입 패턴의 한 예이다.

빈발 에피소드	의미
(*service=http, flag=S0*), (*service=http, flag=S0*) -> (*service=http, flag=S0*) [0.93, 0.03, 2]	93% of the time, after two *http* connections with *S0* flag are made(to a host *victim*), within 2 seconds from the first of these two, the third similar connection is made, and this pattern occurs in 3% of the data

그림 4 빈발 에피소드

빈발 순차 패턴에 속성 생성 알고리즘[6]을 적용하여 시간적이고 통계적인 속성이 생성되고 생성된 속성은 커넥션 레코드에 추가된다. 이렇게 추가된 속성이 침입 탐지 모델의 탐지 정확도를 높여주는 결과를 가져온다[10]. 왜냐하면 추가되는 속성은 침입 탐지 모델의 탐지 정확도를 결정하는 트레이닝 데이터에 존재하는 고유의 속성을 바탕으로 생성되기 때문이다. 그림 5는 속성 생성 알고리즘으로부터 생성된 속성의 예이다.

service	flag	host_count	srv_count	host_REJ_%	···
ecr_i	SF	1	1	0	···
ecr_i	SF	350	350	0	···
ftp	REJ	231	1	85%	···
http	SF	1	0	0	···
···	···	···	···	···	···

그림 5 속성 생성 알고리즘으로부터 생성된 새로운 속성

새로운 속성이 추가된 커넥션 레코드에 분류 프로그램인 RIPPER[9]를 적용시켜 침입 탐지 룰을 생성 시키게 된다. 침입 탐지 모델은 생성된 침입 탐지 룰을 이용하여 침입 여부를 판단하게 된다. 그림 6은 RIPPER에 의해 생성된 침입 탐지 룰의 예이다.

RIPPER rule	의미
smurf :- service=ecr_i, host_count ≥ 5, host_srv_count ≥ 5	If the service is icmp echo request, and for the past 2 seconds, the number of connections that have the same destination host as the current one is at least 5, and the number of connections that have the same service as the current one is at least, then this is a smurf attack(a DOS attack)
satan :- host_REJ_% ≥ 83%, host_diff_srv_% ≥ 87%	If for the connections in the past 2 seconds that have same the destination host as the current connection, the percentage of rejected connections are at least 83%, and the percentage of different services is at least 87%, then this is a satan attack(a PROBING attack)

그림 6 DOS와 PROBING 공격에 대한 RIPPER 룰

3. 새로운 속성의 추가

앞 절에서도 언급했듯이 데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도는 트레이닝 데이터에 포함된 고유한 속성들의 집합과 선택된 *axis* 및 *reference* 속성[5]에 의해 결정된다. 그러나 현재의 데이터 마이닝에 기반한 침입 탐지는 트레이닝 데이터에 포함된 고유의 속성만을 고려하고 있고 침입과 밀접하게 관련된 속성이 없기 때문에 *axis* 및 *reference* 속성을 선택하는데 한계를 가지고 있다. 따라서 본 논문에서는 데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도를 향상시키기 위해 침입과 밀접하게 관련될 뿐만 아니라 *axis* 및 *reference* 속성으로도 선택할 수 있는 새로운 속성을 제안한다.

제안된 속성은 침입의 정의에 기반을 두고 있다. 침입(Intrusion)이란 시스템 자원의 기밀성(confidentiality), 무결성(integrity), 가용성(availability)을 훼손하는 행위를 말한다[11]. 이러한 침입의 정의로부터 시스템 자원의 기밀성, 무결성, 가용성에 대한 훼손 여부를 판단할 수 있는 속성을 제안한다. 본 논문에서 제안된 속성은 confidentiality, integrity, availability의 세 가지이고 각각은 시스템 자원의 기밀성, 무결성, 가용성의 훼손 여부를 나타낸다. 시스템 자원의 기밀성, 무결성, 가용성이 훼손 됐을 경우에 각 속성은

abnormal 값을 갖고 그렇지 않은 경우에는 normal 값을 갖는다. 시스템 자원의 기밀성, 무결성, 가용성에 대한 훼손 여부를 판단하기 위해 기밀성 모니터 에이전트, 무결성 모니터 에이전트, 가용성 모니터 에이전트를 사용한다. 그림 7은 각 에이전트로부터 생성되는 속성과 속성이 갖는 값을 보여주고 있다.

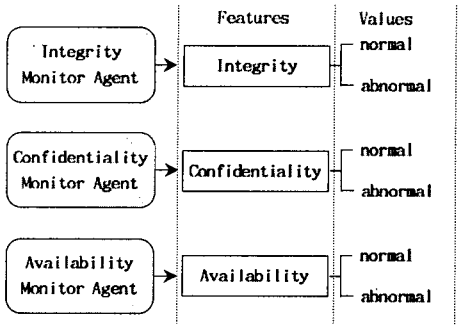

그림 7 제안된 속성과 속성 값

기밀성 모니터 에이전트는 시스템의 정보 제어 정책이 위배되었는지와 보안 정보가 누출되었는지를 감시한다. 기밀성 모니터 에이전트는 오용탐지 기술을 이용하며 Snort와 같은 NIDS 프로그램을 사용하여 시스템 자원의 기밀성에 대한 훼손 여부를 탐지할 수 있다.

무결성 모니터 에이전트는 시스템의 중요 파일의 무결성을 감시한다. 무결성 모니터 에이전트는 중요 파일의 체크섬 등을 계산하여 비정상적으로 중요파일의 내용이 변화되었음을 체크할 수 있는 Tripwire 프로그램을 사용하여 시스템 자원의 무결성에 대한 훼손 여부를 탐지할 수 있다.

가용성 모니터 에이전트는 자원이 비정상적으로 소비되는지를 감시한다. 대부분의 침입이 메모리, 하드 디스크, CPU 등과 같은 자원의 비정상적인 소비를 야기 시키기 때문에 매우 중요하다. 기밀성 모니터 에이전트는 비정상행위탐지 기술을 이용하며 시스템 자원의 정상적인 사용량, 소비 시간 등을 정상행위로 규정하고 이러한 정상정식 행위를 벗어나는 행위를 탐지할 수 있다.

커넥션 레코드에 새로운 속성이 추가되는 과정은 다음과 같다. 먼저, 각 에이전트는 트레이닝 데이터가 수집되는 기간에 시스템 자원의 기밀성, 무결성, 가용성이 훼손된 시간을 기록한다. 다음에 각 에이전트가 기록한 시간과 커넥션 레코드의 타임스탬프를 비교해서 두 값이 동일한 커넥션 레코드에 대해서는 해당 속성의 값을 abnormal로 하고 그렇지 않은 커넥션 레코드에 대해서는 해당 속성의 값을 normal로 한다. 즉, 시스템 자원의 기밀성, 무결성, 가용성이 훼손된 시간과 동일한 타임스탬프를 갖는 커넥션 레코드는 confidentiality, integrity, availability 속성이 abnormal 값을 갖고 동일하지 않은 타임스탬프를 갖는 커넥션 레코드는 confidentiality, integrity, availability 속성이 normal 값을 갖는다. 이렇게 해서 커넥션 레코드에는 고유의 속성 외에 confidentiality, integrity, availability의 세 가지 속성이 추가되고 각 속성은 abnormal 또는 normal 값을 갖는다.

데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도는 트레이닝 데이터에 포함된 속성과 선택된 *axis* 및 *reference* 속성에 의해 결정된다. 그러나 기존의 침입탐지시스템은 트레이닝 데이터에 포함된 고유의 속성만을 고려할 뿐만 아니라 고유의 속성 중에서 선택된 *axis* 및 *reference* 속성은 침입과는 직접적인 관련이 없기 때문에 탐지 정확도를 향상시키는 데는 한계가 있다. 따라서 위와 같은 침입과 밀접하게 관련이 있는, 즉 시스템 자원의 기밀성, 무결성, 가용성의 훼손 여부에 대한 정보를 가지고 있는 새로운 속성이 트레이닝 데이터에 추가됨으로써 데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도를 향상 시킬 수 있다.

4. 결 론

데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도는 트레이닝 데이터에 포함된 고유의 속성과 선택된 *axis* 및 *reference* 속성에 의해 결정된다. 그러나 현재의 데이터 마이닝 기반의 침입탐지시스템에서 고려하고 있는 고유의 속성은 침입과 밀접한 관련이 없기 때문에 탐지 정확도를 향상시키는데 한계가 있다.

본 논문에서는 데이터 마이닝에 기반한 침입탐지시스템의 탐지 정확도를 향상시키기 위하여 침입의 정의에 기반한 새로운 속성을 제안하였다. 제안된 속성은 시스템 자원의 기밀성, 무결성, 가용성의 훼손 여부에 대한 정보를 갖고 있기 때문에 트레이닝 데이터에 포함된 고유의 속성과는 달리 침입과 밀접하게 관련되어 있다. 따라서 제안된 속성이 트레이닝 데이터에 추가됨으로써 데이터 마이닝에 기반한 침입 탐지시스템의 탐지 정확도를 향상시킬 수 있다.

참 고 문 헌

[1] S. Kumar and E. H. Spafford, "A software architecture to support misuse intrusion detection", *In Proceedings of the 18th National Information Secutiry Conference*, pp. 194-204, 1995

[2] K. Ilgun, R. A. Kemmerer, and P. A. Porras, "State transition analysis: A rule-based intrusion detection approach", *IEEE Transactions on Software Engineering*, pp. 181-199, March 1995.

[3] T. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. Neumann, H. Javitz, A. Valdes, and T. Garvey, "A real-time intrusion detection expert system(IDES) - final technical report", *Technical report, Computer Science Laboratory, SRI International, Menlo Park, California*, February 1992

[4] W. Lee and S. J. Stolfo, "Data mining approaches for intrusion detection", *In Proceedings of the 7th USENIX Security Symposium*, San Antonio, TX, January 1998

[5] W. Lee, S. J. Stolfo, and K. W. Mok, "A data mining framework for building intrusion detection modes", *In Proceedings of the 1999 IEEE Symposium on Security and Privacy*, May 1999

[6] W. Lee, S. J. Stolfo, and K. W. Mok, "Mining in a data-flow environment: Experience in intrusion detection", *Submitted for publication*, March 1999

[7] 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

[8] H. Mannila and H. Toivonen, "Discovering frequent episodes in sequences", *In Proceedings of the 1st International Conference on Knowledge Discovery in Databases and Data Mining*, Montreal, Canada, August 1995

[9] W. W. Cohen, "Fast effective rule induction", *In Machine Learning: the 12th International Conference*, Lake Taho, CA, 1995

[10] W. Lee, S. J. Stolfo, and K. W. Mok, "Mining audit data to build intrusion detection modes", *In Proceedings of the 4st International Conference on Knowledge Discovery and Data Mining*, New York, NY, August 1998

[11] J. P. Anderson, "Computer Security Threat Monitoring and Surveillance", *James P. Anderson CO*, Fort Washington, April 1980