이상탐지(Anomaly Detection) 및 오용탐지(Misuse Detection) 분석의 정확도 향상을 위한 개선된 데이터마이닝 방법 연구

최윤정[O] 박승수
이화여자대학교 컴퓨터학과
cris@ewhain.net, sspark@ewha.ac.kr

Reinforcement Mining Method for Anomaly Detection and Misuse Detection using Post-processing and Training Method

Yun-Jeong Choi[O] Seung-Soo Park
Dept. of Computer Science & Engineering, Ewha Womans University

요 약

네트워크상에서 발생하는 다양한 형태의 대량의 데이터를 정확하고 효율적으로 분석하기 위해 설계되고 있는 마이닝 시스템들은 목표지향적으로 훈련데이터들을 어떻게 구축하여 다룰 것인지에 대한 문제보다는 대부분 얼마나 많은 데이터마이닝 기법을 지원하고 이를 적용할 수 있는지 등의 기법에 초점을 두고 있다. 따라서, 점점 더 에이전트화, 분산화, 자동화 및 은닉화 되는 최근의 보안공격기법을 정확하게 탐지하기 위한 방법은 미흡한 실정이다. 본 연구에서는 유비쿼터스 환경 내에서 발생가능한 문제 중 복잡하고 지능화된 침입패턴의 탐지를 위해 데이터마이닝 기법과 결함허용방법을 이용하는 개선된 학습알고리즘과 후처리 방법에 의한 RTPID(Refinement Training and Post-processing for Intrusion Detection)시스템을 제안한다. 본 논문에서의 RTPID 시스템은 active learning과 post-processing을 이용하여, 네트워크 내에서 발생 가능한 침입형태들을 정확하고 효율적으로 다루어 분석하고 있다. 이는 기법에만 초점을 맞춘 기존의 데이터마이닝 분석을 개선하고 있으며, 특히 제안된 분석 프로세스를 진행하는 동안 능동학습방법의 장점을 수용하여 학습효과는 높이며 비용을 감소시킬 수 있는 자가학습방법(self learning)방법의 효과를 기대할 수 있다. 이는 관리자의 개입을 최소화 하는 학습방법이면서 동시에 False Positive와 False Negative 의 오류를 매우 효율적으로 개선하는 방법으로 기대된다. 본 논문의 제안 방법은 분석도구나 시스템에 의존하지 않기 때문에, 유사한 문제를 안고 있는 여러 분야의 네트웍 환경에 적용될 수 있다.

1. 서 론

인터넷 인프라의 급속한 보급과 함께 유비쿼터스나 E-business 는 무서운 속도로 성장하고 있다. 그러나 이들의 성장과 함께 위협적인 공격과 그 피해도 크게 증가하고 있는 상황이다. 또한, 정보시스템에 대한 불법적인 활용 시도 즉, 네트워크 및 시스템의 오용 사례가 급속도로 증가하고 있다. 이러한 오용행위들은 초기 시스템에 대한 단순한 의도에서 시작했던 것과는 다른 형태와 구체적인 목적을 띄고 있어서 그 분석의 중요성이 부각되고 있다. 점점 지능화 되어가는 침입패턴들의 탐사문제와, 정치, 경제, 사회적인 이해관계와 연결되어 불법적으로 범죄화되는 양상을 보이고 있고, 이러한 행위에 의한 피해가 크게 증가하고 있는 상황이다.

최근 침입탐지시스템(Intrusion Detection System)에 데이터마이닝 기법을 적용하여 능동적인 침입탐지시스템을 구축하고자 하는 연구들이 활발하다. 대표적인 예로서 대량의 감사데이터를 효율적으로 분석하거나 자동화된 침입탐지모델을 구축하는 연구가 있으며, 이를 위해서는 정상적인 프로파일이나 비정상적인 공격기법의 시나리오를 구축하고, 이를 실험 및 검증이 가능한 많은 양의 시스템과 네트워크 감사데이터를 통해 정확하고 효율적으로 분석해야 하는 일이 뒤따른다. 네트워크상에서 발생하는 다양한 형태의 대량의 데이터를 정확하고 효율적으로 분석하기 위해 설계되고 있는 마이닝 시스템들은 분석목표지향적으로 훈련데이터들을 어떻게 구축하여 다룰 것인지에 대한 문제보다는 대부분 얼마나 많은 데이터마이닝 기법을 지원하고 이를 적용할 수 있는지 등의 기법에 초점을 두고 있다. 따라서, 에이전트화, 분산화, 자동화 및 은닉화 되고 있는 최근의 보안공격기법을 탐지하거나 차단하기 위한 방법은 미흡한 실정이다. 따라서, 이 논문에서는 지능화된 침입패턴의 탐지를 위해 데이터마이닝 기법과 결함허용방법을 이용하는 개선된 학습알고리즘과 후처리방법에 의한 RTPID(Refinement Training and Post-processing for Intrusion Detection) 시스템을 제안한다. 본 논문에서의 RTPID 시스템은 능동학습(Active Learning)과 향상된 후처리분석(Post-processing) 을 이용하며. 네트워크 내에서 발생가능한 침입형태들을 정확하고 효율적으로 다루어 분석하고 있다[1]. 이는 기법에만 초점을 맞춘 기존의 데이터마이닝

분석을 개선하고 있으며, 특히 제안된 분석 프로세스를 진행하는 동안 능동학습방법의 장점을 수용하여 학습 효과는 높이며 분석비용을 감소시킬 수 있는 자가학습 방법(self learning)방법의 효과를 기대할 수 있다. 이는 관리자의 개입을 최소화 하는 방법이면서 동시에 False Positive와 False Negative 의 오류를 매우 효율적으로 개선하는 방법으로 기대된다. 본 논문은 다음과 같이 구성된다. 2장에서는 침입탐지시스템의 구성요소와 여러 유형의 침입방안에 대한 내용을 정리하고, 3장에서는 이상탐지와 오용탐지의 성능을 높일 수 있는 개선된 데이터마이닝 방법을 제안한다. 4장에서는 이를 바탕으로 한 내용을 정리하며 결론을 맺는다.

2. 관련연구

2.1 침입탐지 방법

침입탐지시스템(IDS)은 분석 기법에 따라 이미 알려진 침입행위에 대한 정보를 이용하여 공격을 탐지해내는 오용탐지(Misuse Detection: action-based method)와 사용자의 정상행위를 기반으로 정상적인 행동패턴에 어긋나는 경우를 침입으로 탐지하는 이상탐지 혹은 비정상행위탐지(Anomaly Detection: profile-based method)으로 나눌 수 있다[2,4]. 또한 이용하는 데이터 소스의 기반에 따라 호스트 기반과 네트워크 기반 방식으로 나눌 수 있다. 이들 시스템을 평가하는 기준들로는 기능성(Capability), 편의성(Usability), 성능의 우수성(Performance), 관리성(Manageability), 연동성(Interoperability), 확장성(Scalability), 안정성(Robustness)등으로 규정되며[3]. 이중 무엇보다도 성능에 대한 중요성이 강조되는 상황이다.

침입탐지시스템에서 가장 일반적인 형태는 네트워크 기반의 오용탐지시스템이며, 많은 기관들은 오용행위들에 있어서 빠른 시간내에 탐지하고 복구하기 위해 침입탐지시스템을 도입하고 있다.

오용탐지는 이미 알려진 형태의 공격 순서를 시그너쳐(Signature)화하여 이 순서 혹은 특징을 따르는 상황을 공격이라고 판단한다. 알려진 공격방식 및 사이트별 보안정책과 같은 것을 규칙(rule-base)으로 구성하고 전문가 시스템을 활용하여 침입을 탐지한다. 이는 일반적으로 알려진 공격에 대한 탐지능력만을 가지게 되므로 실제 침입이 아닌경우 침입이라고 판정하는(false positive) 오류가 비교적 적은데 반하여, 공격정보를 계속 수집해야 하며 알려진 공격형태를 벗어나면 탐지할 수 없다는 한계가 있다. 따라서 전문가의 뛰어난 분석력이 요구된다.

또 다른 유형의 하나인 이상 탐지는 오랜 기간 축적된 정상적인 데이터를 수집하여 학습시킴으로써 정상적인 형태의 사용에 대한 프로파일을 완성한 후 이와 다른 형태의 패턴을 가진 데이터를 탐지하는 방식이다. 기존에 알려지지 침입을 탐지할 수 있고 실제의 침입을 침입이 아니라고 판정하는(false negative) 오류를 줄일 가능성이 높기 때문에, 위의 두가지 탐지기법을 하이브리드방식으로 적용하는 연구가 활발하다. 그러나, 정상범위의 데이터 프로파일링을 통한 비정상행위 탐지기법에 대한 활발한 연구가 진행되고 있지만, 정상범위의 모든 데이터를 수집할 수 없다는 한계가 드러나며, 정상패턴과 공격패턴을 구분짓는데 있어서 많은 어려움이 존재하기도 한다[7]. 주로 사용자의 계정, 시스템파일 및 디렉토리 사용에 따른 변화들을 분석의 근거로 삼는다.

2.2 기존의 데이터마이닝에 의한 분석

데이터마이닝 기법들 중에서 가장 많이 쓰이고 있는 유용한 기법 두가지를 간략히 정리한다.

1) 연관규칙(Association Rule)

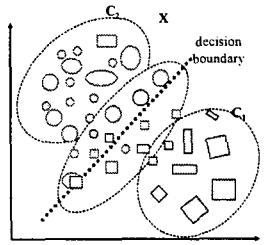
연관규칙은 항목집합으로 표현된 트랜잭션에서 각 항목간의 연관성을 반영하는 규칙으로서, 미리 주어진 최소 지지도와 신뢰도 값을 만족하는 항목집합들의 모든 집합들인 빈발항목집합을 찾아내어 연관규칙을 생성한다[5]. 대량의 데이터로부터 적당한 특성이나 패턴 탐사를 위한 속성간의 연관성을 추출하며, 주로 감사 데이터(audit data)의 분석에 유용하여 많이 쓰인다.

2) 분류(Classification)

분류란 데이터들을 미리 정해진 항목에 올바로 할당하는 것으로서, 각 항목에 대한 훈련데이터들의 학습을 통하여 분류규칙과 입력데이터를 비교하는 작업으로서 효율적인 정보관리 및 검색등에 유용하다. 대부분의 문제들은 분류분석이 필수적인 만큼 분류분석의 성능향상을 위해 많은 연구가 진행되어 왔다. 기존의 분류성능 향상을 위한 연구들은 대부분 분류모델 자체를 개선시키는데 주력해왔으며 통계적인 방법으로 그 범위가 제한된다.

3. RTPID(Refinement Training and Post-processing for Intrusion Detection) 방법에 의한 분석

본 논문의 제안방법은 오분류의 가능성이 높은 비정상 및 오용데이터들의 개선된 분류분석을 통해 침입탐지 시스템의 정확률을 높인다[1]. <그림 1>에서 알 수 있듯이 데이터의 복잡도 및 불확실성이 높으면 분류경계상의 위치가 명확하지 않으며, 이는 오분류율(false positive, false negative)을 높이게 되고 그대로 분류결과의 신뢰도에 영향을 미치게 된다. 제안방법은 학습문서집합을 구성하는 방법과 분류 후 최종항목으로 지정하는 방법의 두 분야로 나뉘며, 이에 따라 학습과 후처리 프로세스를 설계하였다. 일부 데이터마이닝에서는 신경망이나 유전

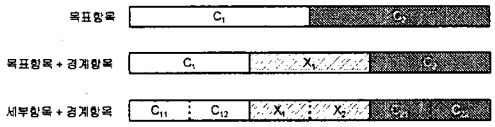


<그림 1> 불확실성이 높아 분류경계에 인접한 데이터들의 복잡도

자 알고리즘 같은 특정기법들에만 초점을 두고 있으나 다양한 지식탐사를 위한 개념적인 정보추출의 방법론이자 일련의 과정으로 이해해야 한다는 점을 강조한 것이다. 어떤 문제를 다루는데 정해진 기법이나 규칙이 정해져 있는 것이 아니라 데이터에 따라 혹은 다루어야 할 문제의 성격에 따라 다양한 기법들이 적용될 수 있어야 하기 때문이다. 데이터마이닝을 통해 얻어진 정보는 평가를 통해 다시 마이닝 초기단계에 반영되고 재분석이 되면서 얻게될 결과의 신뢰성을 높여가게 된다. 따라서 지침이 되는 가이드라인이제시되어야하며 마이닝된 결과를 어떻게 활용할 것인가를 판단하는 인적요소의 역할 또한 중요하다[1].

1)학습 : 목표항목 설정 및 정의

<그림 1>의 경계선 부근에서 겹쳐서 나타나고 있는 데이터들은 쓰인 분류기준이 애매하므로 확실히 어떠한 범주에 할당되는지 판단하기 어려운 성질을 지닌다.

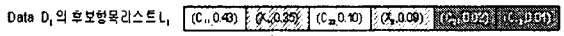


<그림2> 경계항목과 세부항목으로 정의한 학습문서 집합구성방법

제안방법에서의 목표항목 C={침입패턴, 침입에 가까운 패턴, X, 정상에 가까운 패턴, 정상패턴}으로 설정하며, 각각에 해당하는 데이터로 학습시킨다. 이때 X 는 구분하기 어려운 데이터, 즉 침입의 형태이나 정상패턴, 혹은 정상적인 형태이나 침입패턴인 데이터를 따로 모아 정의한다. 이는 기존의 C={침입, 정상}의 자료만으로 학습시킨 결과와는 매우 다르며, 보다 세분화된 분류규칙을 얻게된다.

2)후처리분석

위에서 정의한 목표항목들로 학습을 수행하고, 1 차 분류 알고리즘을 적용하여 전체 후보항목리스트 L 을 얻는다. 데이터 D_i 에 대한 후보항목리스트인 L_i 는 분류가능한 범주와 점수치(score)를 쌍으로 하는 순위 리스트이다. <그림 3>과 같은 후보항목리스트의 점수치는 적용한 분류모델에 따라 상대적 혹은 절대적 수치값으로 얻어진다.



<그림 3> 후보항목리스트(candidate category list)의 예

결국 데이터 D_i 의 후보항목 리스트 L_i 는 데이터와 범주들간의 유사도(Similarity)를 나타내는 것이다. 범주 할당작업은 분류수행 결과인 범주와 범주별 점수치쌍인 랭킹정보(ranking list)를 분석하는 것이다.

for n=0 to N (= number of target category) {

Calculate distance of category between P, c_{nk}

$$Dist(P, c_n) = \sum RD(P, c_{nk}) * w_m \quad (1)$$

}

assign D_i to more closer side c_n

<그림4> 후보항목리스트(candidate category list)의 수치분석을 위한 할당규칙

후보항목리스트의 분석에는 수치적 근거사항과 항목간 거리차가 입력이 된다. 앞서 판단된 사례들이 분류 수행을 위한 학습패턴으로 동작하고, 이 입력을 이용하여 2차 분류를 수행하면 후보항목의 패턴을 조건항으로 갖는 규칙이 생성된다. 즉, 2차분류의 규칙 을 통해 1차분류에서 발견하지 못했던 침입이나 정상오류를 확장된 기준으로 다시 한번 걸러내는 것이 가능하게 되며, 개선된 방법으로서 정확도가 향상된 패턴분류의 역할을 하게 된다. 이로서 전문가는 1차,2차분류의 결과의 비교를 통해 학습단계에 적절히 피드백하는 것이다.

4. 결론 및 향후연구

침입탐지시스템의 성능에 있어서 가장 중요한 요소는 탐지의 정확도이다. 특히 공격방법이 점점 다양화되고 지능화 되어가고 있는 상황에서 탐지력을 향상시키기 위한 연구는 매우 중요하다. 기존 데이터마이닝에 기반한 침입탐지시스템은 우수한 분석기법을 적용한다는 면에서는 의미가 있으나, 대부분의 경우 분석알고리즘 또는 기법선정에만 관심을 두고 있기 때문에 정확도면에서는 아직 한계가 있다. 우수한 훈련데이터와 강인하고 능동적인 학습과정 없이는 신뢰할만한 정확도를 얻기 힘들다는 것을 간과해서는 안 될 것이다. 본 논문에서의 제안방법은 학습데이터의 설정 및 훈련방법을 개선함으로써 오분류율이 높은 침입상태를 보다 정확히 발견해냄으로써 False Positive 및 False Negative 오류를 최소화하여 정확도 향상에 기여한다.

본 논문의 제안방법은 분석도구나 시스템에 의존하지 않기 때문에, 유사한 문제를 안고 있는 여러 분야의 네트워크 환경에 적용될 수 있을 것이다.

참고문헌

[1] 최윤정, 박승수, " 학습방법개선과 후처리 분석을 이용한 자동문서분류의 성능향상 방법" , 한국 정보처리학회 논문지, VOL. 12-B NO. 07, pp. 0811 ~ 0822 2005 . 12

[2] 김병구, 정채명, " 침입탐지 기술의 현황과 전망" , 정보과학회지, VOL. 18, NO. 1, pp.29~39, 2000.

[3] 유신근, 이남훈, 심영철, " 침입탐지 시스템의 평가 방법론" , 한국정보처리학회 논문지, VOL. 7, NO. 11, pp.3445-3460, 2000.11.

[4] Axelsson S., " The Base-rate Fallacy and the Difficulty of Intrusion Detection" , ACM Transactions on Information and System Security, VOL.3, NO 3, pp.186-205,2000.

[5] Wenke Lee, et al ., " Data Mining Approaches for Intrusion Detection" , In proceedings of the 7th USENIX Security Symposium, San Antonio, TX, 1, 1998.

[6]Wenke Lee, et al ., " Mining Audit Data to Build Intrusion Detection Models" , In proceedings of the 4th International Conference on Knowledge Discovery and Data Mining, New York, 8, 1998.

[7] 박명언, 김동국, 노봉남, " 가우시안 혼합모델을 이용한 네트워크 침입탐지시스템" , 한국정보과학회, 제32회 추계학술발표회 논문집, VOL.32, NO.2