나이브 베이지안과 데이터 마이닝을 이용한 FHIDS(Fuzzy Logic based Hybrid Intrusion Detection System) 설계

이 병 관*, 정 은 희**

A Design of FHIDS(Fuzzy logic based Hybrid Intrusion Detection System) using Naive Bayesian and Data Mining

Byung-Kwan Lee*, Eun-Hee Jeong**

요 약

본 논문에서 나이브 베이지안 알고리즘, 데이터 마이닝, Fuzzy logic을 이용하여 이상 공격과 오용 공격을 탐지하는 하이브리드 침입탐지시스템인 FHIDS(Fuzzy logic based Hybrid Intrusion Detection System)을 설계하였다. 본 논문에서 설계한 FHIDS의 NB-AAD(Naive Bayesian based Anomaly Attack Detection) 기법은 나이브 베이지안 알고리즘을 이용해 이상 공격을 탐지하고, DM-MAD(Data Mining based Misuse Attack Detection)기법은 데이터 마이닝 알고리즘을 이용하여 패킷들의 연관 규칙을 분석하여 새로운 규칙기반 패턴을 생성하거나 변형된 규칙 기반 패턴을 추출함으로써, 새로운 공격이나 변형된 공격을 탐지한다. 그리고 FLD(Fuzzy Logic based Decision)은 NB-AAD과 DM-MAD의 결과를 이용하여 정상인지 공격인지를 판별한다. 즉, FHIDS는 이상과 오용공격을 탐지 가능하며 False Positive 비율을 감소시키고, 변형 공격 탐지율을 개선한 하이브리드 공격탐지시스템이다.

Abstract

This paper proposes an FHIDS(Fuzzy logic based Hybrid Intrusion Detection System) design that detects anomaly and misuse attacks by using a Naive Bayesian algorithm, Data Mining, and Fuzzy Logic. The NB-AAD(Naive Bayesian based Anomaly Attack Detection) technique using a Naive Bayesian algorithm within the FHIDS detects anomaly attacks. The DM-MAD(Data Mining based Misuse Attack Detection) technique using Data Mining within it analyzes the correlation rules among packets and detects new attacks or transformed attacks by generating the new rule-based patterns or by extracting the transformed rule-based patterns. The FLD(Fuzzy Logic based Decision) technique within it judges the attacks by using the result of the NB-AAD and DM-MAD. Therefore, the FHIDS is the hybrid attack detection system that improves a transformed attack detection ratio, and reduces False Positive ratio by making it possible to detect anomaly and misuse attacks.

Keywords : FHIDS, Anomaly attack, Misuse attack, Fuzzy logic, Navie Bayesian, Data Mining

* 관동대학교 컴퓨터학과 (bklee@kwandong.ac.kr),
** 교신저자 강원대학교 지역경제학과 (jeongeh@kangwon.ac.kr)
접수일자 : 2012년 8월 2일, 수정일자 : 2012년 8월 20일, 심사완료일자 : 2012년 9월 10일

Ⅰ. 서 론

침입탐지기법은 오용탐지(misuse detection)와 이상 탐지(anomaly detection)의 두 가지 유형으로 나누어진다[1]. 대부분의 상용제품들은 오용탐지시스템으로 탐지속도와 탐지율이 빠르고 효율적이라는 장점을 가지지만, 시스템이 공격에 대한 정보가 없으면 공격을 탐지할 수 없고, 동일한 형태의 공격이라고 하더라도 공격 형태를 우회할 수 있는 방법이 있다면 탐지할 수 없다는 단점을 가진다. 이상탐지기법은 오랜 기간 축적된 정상적인 데이터나 공격 데이터를 수집하여 학습시킴으로써 모델링된 데이터와 다른 형태의 패턴을 가진 데이터를 탐지하는 기법으로 가장 큰 특징은 새로운 형태의 공격을 탐지할 수 있다. 하지만, False positive가 높으며, 네트워크 기반 침입탐지에는 적용이 어렵고, 장기간 학습기간이 필요하다는 단점이 있다.

본 논문에서 나이브 베이지안 알고리즘, 데이터 마이닝, Fuzzy logic을 이용하여 오용공격과 이상공격을 탐지하는 하이브리드 침입탐지시스템인 FHIDS(Fuzzy logic based Hybrid Intrusion Detection System)를 설계한다. FHIDS는 전 처리된 감사 자료를 나이브 베이지안 알고리즘으로 분석하여 이상 공격을 탐지하고, 전 처리된 트래픽 자료는 데이터 마이닝, Fuzzy logic 기법을 이용해 규칙기반 패턴을 생성하여 오용 공격을 탐지한다. 따라서 새로운 공격 탐지율 향상, 변형 공격 탐지율을 향상, False positive 비율을 감소시킴으로써 공격 탐지율이 향상된 침입탐지시스템을 제공하고자 한다.

Ⅱ. 관련연구

1. 나이브 베이지안(Naive Bayesian)

나이브 베이지안 알고리즘은 통계적인 분류(Classification)에 활용될 수 있는 매우 단순하면서도 강력한 알고리즘으로, Bayes 이론으로 주어진 데이터가 특정 클래스에 속할 확률을 예측할 수 있다.

$\{x_1,x_2,...,x_n\}$라는 n 차원의 특징 벡터인 X 가 존재하며, $\{C_1,C_2,...,C_m\}$라는 m 개의 클래스가 존재한다고 가정한다. 임의의 데이터 X가 가장 높은 사후확률을 가지는 클래스에 속할 것이라는 예측은 Bayes 이론을 사용하여 다음과 같이 계산할 수 있다[2].

$$P(C_i|X) = \frac{P(X|C_i)P(C_i)}{P(X)},\ 1 \le i \le m$$

P(X)는 모든 클래스에 대해 일정한 값을 가지므로, 오직 $P(X|C_i)P(C_i)$만을 최대화 하도록 고려한다. 만약 클래스의 사전확률을 알 수 없다면 $P(X|C_i)$만을 고려할 수 있다. $P(X|C_i)$는 나이브 베이지안 알고리즘의 독립가정에 의해 아래 식과 같이 계산하며, 그 결과 X는 가장 큰 사후 확률을 가지는 클래스로 분류할 수 있다[2,3].

$$\begin{aligned} P(X|C_i)P(C_i) &= P(x_1,...,x_n|C_i)P(C_i) \\ &= P(x_1|C_i)P(x_2|C_i)...P(x_n|C_i) \\ &= P(C_i)\prod_{k=1}^{n}P(x_k|C_i) \end{aligned}$$

2. Fuzzy Logic

퍼지 논리는 불분명한 상태, 모호한 상태를 참 혹은 거짓의 이진 논리에서 벗어난 다치성으로 표현하는 논리개념으로 근사치나 주관적 값을 사용하는 규칙들을 생성함으로써 부정확함을 표현할 수 있는 규칙기반 기술을 말한다.

크리스프 집합과 같이 원소가 집합에 속하거나 속하지 않는 두 가지 중의 하나로 결정되지 않고 단위구간 [0,1] 사이의 모든 실수값을 소속도로 취하는 원소들로 구성되는 집합을 퍼지집합이라 한다. 크리스프 집합에서는 전체집합 X의 원소x가 집합A에 속하면 1, 속하지 않으면 0의 두 가지 값에만 대응시키기 때문에 $\mu_A(x):x\rightarrow\{0,1\}$로 표시되는 반면, 퍼지 집합에서는 전체집합 X의 원소 x가 퍼지집합 A에 소속될 가능성을 소속도 $\mu_A(x)$로 표현하기 때문에 $\mu_A(x):x\rightarrow[0,1]$로 표시된다[4,5,6].

퍼지제어는 인간 행동의 노하우를 "만약 상태가 A로 되면 조작량을 B로 한다"라고 하는 "If-then" 형식의 언어적 제어 규칙으로 표현 된

다. 또한 복수개의 규칙들이 모여 제어규칙집합을 만들고 이를 기초로 추론을 행하여 조작량을 출력한다[6,7].

Ⅲ. FHIDS 설계

본 논문에서 제안하는 FHIDS는 이상행동을 탐지하는 NB-AAD(Naive Bayesian based Anomaly Attack Detection)기법과 오용행동을 탐지하는 DM-MAD(Data Mining based Misuse Attack Detection) 기법, 그리고 두 모듈의 결과를 이용하여 공격인지를 결정하는 FLD(Fuzzy Logic based Decision) 기법으로 구성되며, 전체적인 구조는 그림 1과 같다.

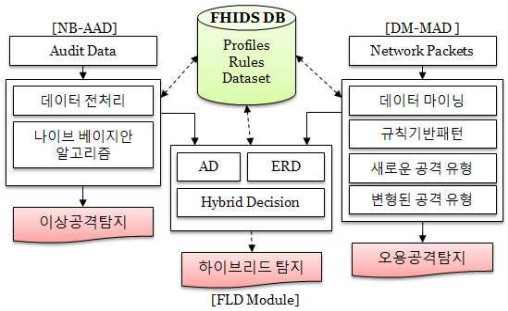


그림 1. FHIDS 구조
Fig. 1 The Structure of FHIDS

3.1 이상탐지 기법 설계

본 논문에서는 나이브 베이지안 알고리즘을 이용하여 분석할 자료를 분류하고, 분류된 데이터에 대한 확률과 조건부 확률을 계산한다. 그리고 이 확률을 이용해 이상 행동을 탐지함으로써 False positive를 감소시키고자 NB-AAD(Naive Bayesian based Anomaly Attack Detection)을 설계한다. NB-AAD기법의 처리 절차는 다음과 같다[7].

[1 단계] NB-AAD은 감사(Audit) 데이터를 NB-AAD 모듈에서 처리할 데이터 형태로 먼저 변환시킨다. 이때, 전 처리된 데이터 집합(Dataset)을 $D=\{D_1,D_2,...,D_n\}$집합에 대한 속성 집합 $A=\{A_1,A_2,...A_n\}$데이터에 대한 클래스 집합 $C=\{C_1,C_2,...,C_m\}$으로 분류한다.

[2 단계] NB-AAD은 클래스 집합에 대한 확률 $P(C_i)$를 구하고, 클래스 집합과 속성에 대한 조건부 확률 $P(D|C_i)$를 구한다.

$$P(D|C_i)=\prod_{k=1}^{n}P(D_k|C_i)$$
$$=P(D_1|C_i)\times P(D_2|C_i)\times ...\times P(D_n|C_i)$$

[3 단계] NB-AAD은 2단계에서 계산한 조건부 확률 $P(D|C_i)$에 클래스 C에 대한 확률을 곱하여 집합 D에 대한 확률의 최대값을 찾는다.

$$P(D)=P(D|C_i)\times P(C_i)$$

[4 단계] NB-AAD은 클래스 C에 대한 $P(D)$에 대한 확률이 최대값을 선정하여 이상행동인지를 예측한다. 그리고 그 결과를 데이터베이스에 저장하고, 임계치 이상인 경우에는 “공격탐지”메시지를 공지한다.

3.2 오용탐지기법 설계

본 논문에서 설계한 오용탐지기법인 DM-MAD (Data Mining based Misuse Attack Detection)은 Data Mining 알고리즘[8,9,10]으로 패킷들의 연관 규칙을 분석하여 새로운 규칙기반 패턴을 생성하거나 변형된 규칙 기반 패턴을 추출함으로써, 새로운 공격이나 변형된 공격을 탐지하고자 한다.

그림 2는 본 논문에서 설계한 DM-MAD의 처

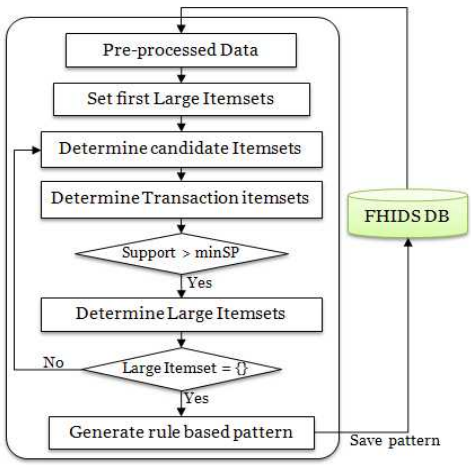


그림 2. DM-MAD 처리 과정
Fig. 2 The procedure of DM-MAD

리과정을 설명한 것으로 AprioriTid 알고리즘[11]에 의해 추출된 빈발 리스트로 규칙 기반 패턴을 생성한다. 이때, 규칙기반 패턴은 support 제약 조건을 만족하는 규칙들의 집합이며, 규칙 생성에 사용된 support 제약조건들은 연관규칙의 관계를 평가하는데 사용하는 양적인 표준이 된다.

DM-MAD의 단계별 처리 과정은 다음과 같다[7].

[1 단계] DM-MAD은 raw packet을 DM-MAD에서 사용할 수 있는 데이터 형태로 변환시킨다.

[2 단계] DM-MAD은 전 처리된 1단계의 데이터를 AprioriTid 알고리즘을 사용해 첫 번째 빈발 리스트(Large itemsets)를 작성한다.

[3 단계] 2단계의 빈발리스트로 candidate itemsets을 생성한다.

[4 단계] candidate itemsets의 각 items을 조합하여 itemsets의 부분집합인 transaction itemsets를 생성한다.

[5 단계] transaction itemsets의 support를 계산하여 minSF보다 큰 item으로 Large itemsets을 생성한다.

[6 단계] Large itemsets가 공집합이 이면 마지막 Large itemsets를 규칙기반 패턴으로 생성하고, Large itemsets가 공집합이 아니면 새로운 candidate itemsets을 생성한다. 그리고 4단계로 이동하여 Large itemsets가 공집합이 될 때까지 반복한다.

이렇게 분석된 연관규칙 결과를 규칙패턴으로 생성하여 DB에 저장하고, 이 규칙을 이용하여 공격을 탐지한다.

3.3 FLD(Fuzzy Logic based Decision) 기법 설계

본 논문에서는 나이브 베이지안 알고리즘으로 이상 공격 탐지 기법은 NB-AAD을 설계하였고, 데이터 마이닝 기법을 이용한 오용탐지기법인 DM-MAD를 설계하였다. 각 모듈의 결과들은 데이터베이스에 저장되어 있다.

Fuzzy Logic을 이용한 의사결정 모듈인 FLD 기법은 두 탐지 기법의 결과를 이용하여 정상인지 공격인지를 판별하는 AD(Attack Decision) 서브 모듈과 공격으로 판별된 데이터의 연관 규칙을 분석하여 새로운 공격 유형 또는 변형된 공격 유형의 규칙들을 생성하고, 생성된 규칙으로 두 모듈의 결과를 한번 더 분석하여 정상인지 공격인지를 판별하는 ERP(Expanded Rule base Pattern) 서브 모듈로 구성된다. FLD 기법은 이 두 모듈을 실행함으로써 침입 탐지율을 향상시키고, False positive를 감소시키고자 한다.

그림 3은 FLD 기법의 전반적인 흐름을 설명한 것이다.

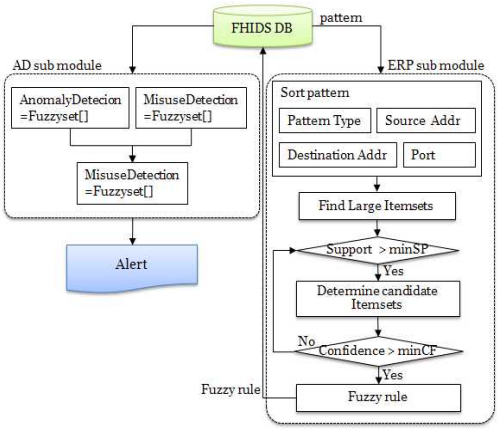


그림 3. FLD의 흐름도
Fig. 3 The flowchart of FLD

FLD 기법의 AD 서브 모듈의 처리 절차는 다음과 같으며, 공격 탐지에 따라 완벽한 공격은 CA(Completely Attack), 약한 공격은 SA(Slightly Attack), 공격이 아닌 것은 CN(Completely Normal)이라 설정한다.

[1 단계] 이상공격탐지에 대한 fuzzy set을 설정한다.

AnomalyDetection
= FuzzySet[{CA, x}, {SA, y}, {CN, z}]

[2 단계] 오용공격탐지에 대한 fuzzy set을 설정한다.

MisuseDetection
= FuzzySet[{CA, a}, {SA, b}, {CN, c}]

[3 단계] 두 개의 FuzzySet의 교집합을 구한 후, FuzzySet 항목 중에서 가장 큰 값으로 의사결정을 한다. 예를 들어, 1단계와 2단계의 FuzzySet의 교집합의 결과가 FuzzySet[{CA, 0.3}, {SA, 0.5}, {CN, 0.7}]이라면 {CN, 0.7}이 가장 큰 값이므로 완벽하게 정상인 것으로 판단한다.

FLD의 ERP 서브 모듈의 처리 절차는 다음과 같다.

[1 단계] FHIDS DB에 저장되어 있는 규칙 기반 패턴을 Pattern Type, Destination Addr, Soruce Addr, Service Port에 따라 분류한다.

[2 단계] AprioriTid 알고리즘을 이용해 large itemsets를 생성한다.

[3 단계] support가 minSP보다 큰 것만 candidate itemsets를 생성한다.

[4 단계] Confidence > minCF 조건을 만족하지 않으면, 3단계로 이동하고, Confidence > minCF 조건을 만족하면 Fuzzy rules을 생성한다. 그리고 그 결과를 FHIDS DB에 저장한다.

Ⅳ. 시뮬레이션

본 논문에서 설계한 FHIDS의 실험환경은 운영체제 Windows 7, Intel Core i3 CPU 3.07 GHz, RAM 2.0GB이고, 실험 데이터는 Lincoln Laboratory에 의해 제공되는 DARPA Intrusion Detection[12] 오프라인 평가 데이터를 사용하였다. 이 데이터에는 Normal, Probe, R2L, U2R, DoS으로 구분할 수 있는 공격에 대한 자료를 포함하고 있다.

본 논문에서는 이 실험 데이터 중에서 Testing Data을 이용하여 공격탐지율(Attack Detection Ratio), False Positive Ratio(FPR)을 실험하였으며, 실험결과는 표 1과 같다.

ADR =(검출된 공격 수/ 공격 수)×100%

FPR =(공격으로 분류되지 않은 데이터/데이터) ×100%

표 1. FHIDS 평가
Table 1.The evaluation of FHIDS

rate / 데이터	ADR	FPR
Normal	99.3	1.3
DoS	97.4	2.4
R2L	90.3	5.4
U2R	81.3	4.2
Probe	96.1	2.2

Ⅴ. 결론

본 논문에서 나이브 베이지안 알고리즘, 데이터 마이닝, Fuzzy logic을 이용하여 이상공격, 오용공격을 탐지하는 FHIDS(Fuzzy logic based Hybrid Intrusion Detection System)을 설계하였다. FHIDS은 NB-AAD 기법, DM-MAD 기법, FLD 기법로 구성되며, 그 특징은 다음과 같다.

첫째, NB-AAD 기법은 나이브 베이지안 알고리즘을 이용해 이상 행동을 탐지함으로써 False positive를 감소시켰다.

둘째, DM-MAD 기법은 데이터 마이닝 알고리즘을 패킷들의 연관 규칙을 분석하여 새로운 규칙기반 패턴을 생성하거나 변형된 규칙 기반 패턴을 추출함으로써, 새로운 공격이나 변형된 공격을 탐지할 수 있다.

셋째, 공격 탐지 의사결정 모듈인 FLD 기법은 NB-AAD 기법과 DM-MAD 기법의 결과를 이용하여 정상인지 공격인지를 판별함으로써 침입 탐지율을 향상시키고, False positive를 감소시켰다.

따라서 본 논문에서 설계한 FHIDS는 이상공격 탐지와 오용공격탐지가 가능할 뿐만 아니라, 새로운 공격 탐지율 향상, 변형 공격 탐지율을 향상, False positive 비율을 감소시킴으로써 공격 탐지율이 향상된 하이브리드 침입탐지시스템이라 할 수 있겠다.

참 고 문 헌

[1] T. F. Lunt, “A survey of intrusion detection techniques,” Computer & Security, vol. 12, no.4, pp.405-418, June 1993

[2] D. Heckerman, “A Tutorial on Learning with Bayesian Networks,” Technical Report MSR-TR-95-06, Microsoft Research, PP.339-337, March, 1995

[3] 김용집 , "분류속성가중치와 Naive Bayesian 알고리즘을 이용한 2-Way 기반 협력적 필터링", 인하대학교, 전자계산공학과 석사학위논문, 2004

[4] Hosmer, H. A. “Security is fuzzy! applying the fuzzy logic paradigm to the multipolicy paradigm.”Proceedings of the 1992-93 workshop on New Security Paradigms, Little Compton, RI, USA, August, 1993, pp. 175-184.

[5] Ovchinnikov, S. “Fuzzy Sets and Secure Computer Systems,” Proceedings of the workshop on New security paradigms, pp. 54-62, 1994, Little Compton, Rhode Island, United States

[6] Aly El-emary, Janica Edmonds, Jes´us Gonzalez and Mauricio Papa, “A Framework for Hybrid Fuzzy Logic Intrusion Detection Systems,” The 2005 IEEE International Conference on Fuzzy Systems, pp.325-330, 2005.

[7] 정은희, 김학춘, 이병, “베이지안 알고리즘과 데이터 마이닝 기법을 이용한 HIDS 설계”, 한국인터넷정보학회 하계학술발표대회 논문집, 제13권 제1호, pp.241-242, 2012

[8] 김운용, “데이터마이닝 기반 승강기 안전관리 서비스 시스템 설계”, 한국정보전자통신기술학회 논문지, 제3권 제4호, pp.83-90, 2010

[9] Lee, W., S. Stolfo, and K. Mok. 1998, Mining audit data to build intrusion detection models, In Proceedings of the fourth international conference on knowledge discovery and data mining held in New York, New York, August 27-31, 1998, edited by Rakesh Agrawal, and Paul Stolorz, 66-72, New York, NY:AAAI Press

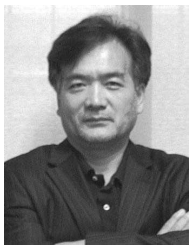
[10] Rakesh Agrawal, Ramakrishnan Srikant, “Fast algorithms for mining association rules,” Proceedings of the 20th VLDB Conference(Santiago, Chile), pp.487-499, September 1994, http://rakesh.agrawal-family.com/papers /vldb94apriori.pdf

[11] ZHI-CHAO LI, PI-LIAN HE, MING LEI , “A high efficient aprioritid algorithm for mining association rule,” Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 18-21 August 2005

[12] 이영석, “DDoS 공격 대응 프레임워크 설계 및 구현”, 한국정보전자통신기술학회 논문지, 제3권 제3호, pp.31-38, 2010

저자약력

이 병 관 (Byung-Kwan Lee) **종신회원**



1979년 2월 : 부산대학교 기계설계학과 공학사
1986년 2월 : 중앙대학교 전자계산공학과 공학석사
1990년 2월 : 중앙대학교 전자계산공학과 공학박사
1988년 3월 ~ 현재 : 관동대학교 공과대학 컴퓨터학과 교수

<관심분야> 네트워크 보안, 컴퓨터 네트워크, 네트워크 포렌직

정 은 희 (Eun-Hee Jeong) **종신회원**

1991년 2월 : 강릉대학교 통계학과 이학사
1998년 2월 : 관동대학교 전자계산공학과 공학석사
2003년 2월 : 관동대학교 전자계산공학과 공학박사
2003년 9월 ~ 현재 : 강원대학교 인문사회과학대학 지역경제학과 부교수

<관심분야> 네트워크 보안, 웹 프로그래밍, 전자상거래