Journal of The Korea Society of Computer and Information
Vol. 17, No. 12, December 2012
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2012.17.12.179

Rough Set Theory와 Support Vector Machine 알고리즘을 이용한 RSIDS 설계

이 병 관*, 정 은 희**

A Design of RSIDS using Rough Set Theory and Support Vector Machine Algorithm

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

요 약

본 논문에서는 RST(Rough Set Theory)과 SVM(Support Vector Machine) 알고리즘을 이용한 RSIDS (RST and SVM based Intrusion Detection System)를 설계하였다. RSIDS는 PrePro(Preprocessing) 모듈, RRG(RST based Rule Generation) 모듈, 그리고 SAD(SVM based Attack Detection) 모듈로 구성된다. PrePro 모듈은 수집한 정보를 RSIDS의 데이터 형식에 맞게 변경한다. RRG 모듈은 공격 자료를 분석하여 공격 규칙을 생성하고, 그 규칙을 이용하여 대량화된 데이터에서 공격정보를 추출하고, 그리고 추출한 공격정보를 SAD 모듈에 전달한다. SAD 모듈은 추출된 공격 정보를 이용하여 공격을 탐지하여 관리자에게 통보한다. 그 결과, 기존의 SVM과 비교해볼 때, RSIDS는 평균 공격 탐지율 77.71%에서 85.28%로 향상되었으며, 평균 FPR은 13.25%에서 9.87%로 감소하였다. 따라서 RSIDS는 기존의 SVM을 이용한 공격 탐지 기법보다 향상되었다고 할 수 있다.

▸ Keywords : 러프셋 이론, 지지벡터머신, 침입탐지시스템, 공격규칙

Abstract

This paper proposes a design of RSIDS(RST and SVM based Intrusion Detection System) using RST(Rough Set Theory) and SVM(Support Vector Machine) algorithm. The RSIDS consists of PrePro(PreProcessing) module, RRG(RST based Rule Generation) module, and SAD(SVM based Attack Detection) module. The PrePro module changes the collected information to the data format of RSIDS. The RRG module analyzes attack data, generates the rules of attacks, extracts attack

• 제1저자 : 이병관 • 교신저자 : 정은희
• 투고일 : 2012. 12. 05, 심사일 : 2012. 12. 16, 게재확정일 : 2012. 12. 20.
* 관동대학교 컴퓨터학과(Dept. of Computer, Kwandong University)
** 강원대학교 지역경제학과(Dept. of Regional Economics, Kangwon National University)

information from the massive data by using these rules, and transfers the extracted attack information to the SAD module. The SAD module detects the attacks by using it, which the SAD module notifies to a manager. Therefore, compared to the existing SVM, the RSIDS improved average ADR(Attack Detection Ratio) from 77.71% to 85.28%, and reduced average FPR(False Positive ratio) from 13.25% to 9.87%. Thus, the RSIDS is estimated to have been improved, compared to the existing SVM.

▸ Keywords : RST, SVM, RSIDS, RRG, SAD, ADR, FPR

I. 서 론

컴퓨터의 급속한 발전과 초고속 통신의 보급으로 수많은 사람들이 네트워크를 이용하여 정보를 접하는 일이 많아졌다. 그로 인해 정보의 가치가 증대되었으나 개인 정보의 노출, 바이러스, 인터넷 웜, 해킹 등의 위험에 노출되고, 기업이나 조직들의 정보시스템에 서비스 장애나 마비를 불러일으키고자 하는 악의적인 공격시도가 급증하고 있다[1]. 따라서 보안성을 강화하는 것이 인터넷 사회에서의 핵심적인 문제가 되었으며, 그 해결 방안 중의 일부가 침입탐지시스템이라 볼 수 있다.

침입 공격의 유형이 계속 진화해 나가고 있으며, 점차 지능화, 분산화, 자동화, 대규모화 되어가고 있지만, 현재 광범위하게 사용되고 있는 침입탐지시스템들은 대량화된 탐지 정보를 적절하게 가공하거나 분석하지 못하고, 침입정보들 간의 연관성 분석의 부족으로 대형화된 공격을 탐지 못하거나, 침입탐지시스템에 내장된 정보부족으로 False Positive를 생성해내는 경향이 있다.

본 논문에서는 RST(Rough Set Theory)와 SVM (Support Vector Machine) 알고리즘을 이용한 RSIDS (RST and SVM based Intrusion Detection System)를 설계하여 이러한 문제점을 해결하고자 한다. RSIDS는 RRG(RST based Rule Generation) 모듈로 자료를 분류하여 규칙을 생성하고, 그 규칙을 이용하여 대량화된 데이터에서 공격정보를 추출하고, SAD(SVM based Attack Detection) 모듈을 이용하여 추출된 공격 정보에서 공격을 탐지함으로써 False Positive를 감소시키고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구인 RST와 SVM을 살펴보고, 3장에서는 본 논문에서 제안한 RSIDS를 기술한다. 4장에서 RSIDS에 대한 실험결과를 설명하고, 이를 통해 RSIDS의 우수성을 입증하고, 5장에서 결론을 맺는다.

II. 관련 연구

1. RST

RST(Rough Set Theory)는 1980년대 초에 Pawlak에 의해 소개 되었으며, 어떤 집합에서 확실하게 분류되는 하한 근사 공간(Lower Approximation)과 불확실하게 분류되는 상한 근사 공간(Upper Approximation)을 집합이론을 통해 나타낸다. 하한 근사와 상한 근사에 따라 경계영역을 계산 할 수 있으며 수식으로 나타내면 다음과 같다[2][3][4].

$$\underline{R}X = \cup\{Y \in U|R : Y \subseteq X\} \quad \text{식(1)}$$

$$\overline{R}X = \cup\{Y \in U|R : Y \cap X \neq \varnothing\} \quad \text{식(2)}$$

$$BN(X) = \overline{R}X - \underline{R}X \quad \text{식(3)}$$

러프 집합에서는 경계영역이 적고 하한근사에 해당되는 범위가 큰 집합일수록 그 집합의 정확도가 높다고 하며 정확성 척도를 이용하여 계산한다.

$$\alpha_R(X) = \frac{card\,\underline{R}}{card\,\overline{R}} \quad (\text{단, } X \neq \varnothing) \quad \text{식(4)}$$

러프 집합에 근거한 데이터의 분석과 가공은 행과 열로 구성된 데이터 집합에서부터 출발하며 분류(Classification) 대상이 되는 데이터 집합을 정보 시스템이라 부른다. 일반적으로 수식으로 표현하는 정보시스템 S는 유한한 전체집합 U에 대해 조건 속성(Condition Attribute) C와 결정 속성(Decision Attribute) D로 아래의 식(5)과 같이 표현한다.

$$S = (U, C, D) \quad \text{식(5)}$$

러프 소속 함수[5]는 확률적인 이론을 포함하고 있으며 개체가 결정 속성의 동치류에 대해 속하는 정도를 확률로 나타낸다. 그리고 A라는 정보 시스템이 있을 때 집합 X에 대해 러프 A-소속 함수는 식(6)과 같이 표현 한다.

(U,A)이며 $\varnothing \neq X \subseteq U$ 이고 $x \in U$, $\mu \equiv 0$ 일 때,

$$^{A}x) = \frac{[x]_A \cap}{[x]_A} \quad \text{식(6)}$$

러프 소속 함수 값은 확률에 근거한 값이기 때문에 그 결과는 0~1 사이의 값을 가진다.

2.2 SVM

SVM(Support Vector Machine)은 러시아의 통계학자인 Vapnik(1998)에 의해 처음 소개된 기계학습알고리즘 기법으로 입력공간과 관련된 비선형 문제를 고차원의 특징 공간의 선형 문제로 사상(mapping)시켜 나타내기 때문에 수학적으로 분석하는 것이 수월하다는 장점이 있다[6]. 또한 SVM은 조정해야 할 파라미터의 수가 그리 많지 않아서 비교적 간단하게 학습에 영향을 미치는 요소를 규명할 수 있고, 구조적 위험을 최소화함으로써 과적합화 문제에서 벗어날 수 있다. 그리고 블록함수를 최소화하는 학습을 진행하기 때문에 지역적인 해가 아닌 전체적인 전역 최적해를 구할 수 있다는 점에서 성능이 좋은 기계학습기법으로 주목 받고 있다[7][8].

SVM은 입력 벡터를 고차원의 특징 공간으로 사상시킨 후 두 분류집합 사이의 여백을 최대화시키는 분리 경계면을 찾는 것을 목적으로 한다. 학습 집합 $(x_1,y_1),...,(x_l,y_l)\}$이 주어졌을 때, 분리 경계면은 $wx+b=0$ 이다. 여기서 $x \in$ ^{n} 는 입력 벡터이고, w는 가중치 벡터, $y \in \{-1,+1\}$ 는 타겟 값, b는 바이어스를 나타낸다. 이때, 입력 벡터 x에서 분리경계면까지의 마진은 $2/\|w\|$ 이며, 이를 최대화하기 위해 식(7)과 같이 비용함수를 정의한다.

$$\Phi(w) = \frac{1}{2}\|w\|^2 \quad \text{식(7)}$$

타겟값과 분리경계면식의 곱은 항상 양수라는 제약조건을 적용하면, 식(7)을 라그랑지안 최적화 기법을 이용해 식(8)의 최적의 w 와 b_0을 구할 수 있다.

$$w_0 = \sum_{i=1}^{l} \alpha_{oi} y_i x_i \ , b_o = -\frac{1}{2} w_o \cdot [x_r + x_s] \quad \text{식(8)}$$

여기서 α는 라그랑쥐 계수이다. 이때, SV(Support Vector)인 x에 대해서만 라그랑쥐 계수가 0이 아닌 값을 가짐으로써 SV만이 w를 계산하는데 의미를 가지게 된다. 학습 데이터 중 마진에 직접 관여하는 벡터만을 골라내는 이러한 능력이 SVM의 큰 특징 중의 하나이다[9].

III. RSIDS 설계

본 논문에서 설계한 RSIDS는 자료를 전 처리하는 PrePro(Preprocessing) 모듈, 규칙을 생성하고, 그 규칙에 따라 공격형 자료를 추출하는 RRG(RST based Rule Generation) 모듈, 그리고 공격을 판단하고 매니저에게 통보하는 SAD(SVM based Attack Detection) 모듈로 구성된다.

그림 1은 RSIDS의 구조를 설명한 것이다.

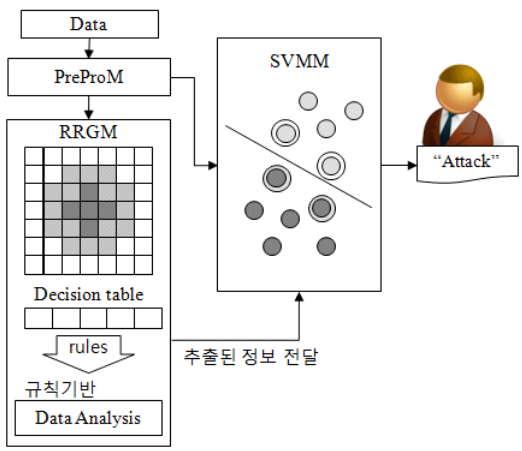

그림 1. RSIDS 구조
Fig. 1. RSIDS Architecture

3.1 PrePro 모듈 설계

PrePro(Preprocessing) 모듈은 수집한 모든 패킷들을 RSIDS의 RRG 모듈과 SAD 모듈이 필요한 데이터 구조로 변경하여 RRG 모듈과 SAD 모듈에 전달한다.

RRG 모듈은 수집한 패킷에서 프로토콜 유형, 서비스 유형, 근원지 IP, 근원지 Port, 목적지 IP, 목적지 Port 정보만을 정리하고, 프로토콜 유형에 따라 코드를 변경한다.

그림 2는 KDD Cup 1999 데이터를 PrePro 모듈이

RRG 모듈에 적합한 데이터 형태로 변환시키는 것을 설명한 것이다. 텍스트 문자는 숫자로 변화시키는데 표1을 참조하여, TCP→1, http→1, uucp→2, SF→10, S0→6, normal→0, neptune→2(DOS공격)으로 변환시킨다.

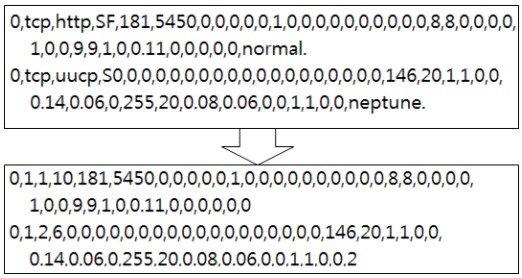

그림 2. PrePro 모듈 결과
Fig. 2. The result of ProPro Module

표 1은 PrePro 모듈에서 데이터의 텍스트를 숫자로 변환할 때 사용하는 변환테이블이다.

표 1. 변환 테이블
Table 1. The transformation table

유형	종류	값
프로토콜	TCP	1
	UDP	2
	ICMP	3
서비스	HTTP	1
	UUCP	2
플래그	OTH	1
	REJ	2
	RST0	3
	RSTOS0	4
	RSTR	5
	S0	6
	S1	7
	S2	8
	S3	9
	SF	10
	SH	11
공격	Normal	0
	Probe	1
	DoS	2
	U2R	3
	R2L	4

3.2 RRG 모듈 설계

RRG(RST based Rule Generation) 모듈은 DT(Decision Table)를 이용하여 공격 정보를 분석하여 공격 유형에 대한 규칙을 생성하고, 그 규칙에 따라 수집한 정보들 중에서 공격으로 의심되는 정보를 추출하도록 설계한다. 그리고 추출된 정보를 SAD 모듈에 전달함으로써 SAD 모듈의 처리시간을 줄이고, 침입탐지시스템의 False Positive를 줄이고자 한다.

RRG 모듈은 DT의 속성 값을 이용하여 decision을 결정하거나, 새로운 규칙을 생성할 때, 모든 속성 값을 사용하는 것은 비효율적이다. 본 논문에서는 공격정보라는 판단에 영향을 미치지 않는 속성은 제외시킨 후, 나머지 속성들로 규칙을 생성하도록 설계한다. RRG 모듈의 공격 규칙 생성과정은 다음과 같다.

〔1 단계〕 RRG 모듈은 정보 시스템(Information System)을 다음과 같이 정의한다.

$$S \quad (U, A, D) \qquad \text{식(9)}$$

여기서, U는 수집된 정보 전체를 말하고, A는 RRG 모듈에서 정의한 프로토콜, 근원지 IP, 근원지 Port, 목적지 IP, 목적지 Port 등의 속성집합을 의미하고, 그리고 D는 공격 형태에 대한 결정 속성을 말한다.

정보함수는 다음과 같이 정의하며, 수집된 정보들과 속성집합에 따라 공격인지를 결정하게 된다.

$$f : U \times A \rightarrow D \qquad \text{식(10)}$$

〔2 단계〕 RRG 모듈은 PrePro 모듈로부터 전달 받은 정보로 DT(Decision Table)을 생성한다. 예를 들어, U={1,2,3,4,5,6}, A={a,b,c,e}이라면, DT는 표 2와 같이 작성한다.

표 2. RRG 모듈의 DT(Decision Table)
Table 2. DT of RRG Module

U \ A	a	b	c	e	d (decision)
1	1	1	0	1	1
2	1	1	1	0	1
3	1	0	0	0	0
4	1	1	1	1	1
5	0	1	0	0	0
6	0	0	1	1	0

〔3 단계〕 RRG 모듈은 공격 규칙 생성에 불필요한 속성들을 제거한다. 먼저, 속성값 중에서 맨 첫 번째 속성값을 제거한 후, $a, a_3, \ldots, a_n\}^* = A^*$ 인지를 비교한다. 비교 결과가 참이면, 두 번째 속성값을 제거한 후, $\{a_3, \ldots, a_n\}^* = A^*$ 인지를 비교한다. 만약 비교 결과 거짓이면, 속성 제거 작업

을 종료한다.

그림 3은 표 2의 DT에서 첫 번째 속성을 제거하는 과정을 설명한 것이다.

〔4 단계〕 RRG 모듈은 공격 정보를 이용하여 공격 정보에 대한 규칙을 생성한다. 이때, 3단계에서 속성 a를 규칙생성에서 제외시켰으므로 표 1의 속성 b, c, e를 이용한다. RRG 모듈의 규칙 생성 과정은 3단계와 마찬가지로 규칙 1에서 속성을 하나씩 차례대로 제외시킨 후 $b,c,e\}^* \leq \{d\}^*$, $\{c,e\}^* \leq \{d\}^*$, $\{e\}^* \leq d^*$, $\{c\}^* \leq d^*$ 를 확인한다. 확인한 결과가 참인 것만 비교하여 규칙을 생성한다.

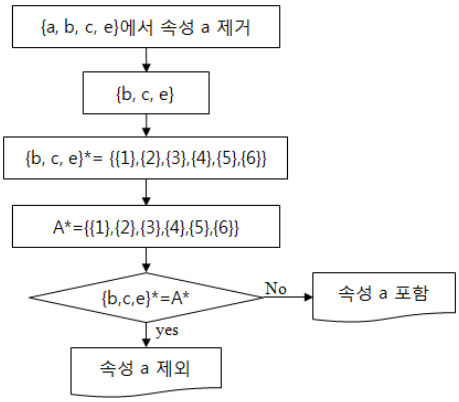

그림 3. 속성 제거 과정
Fig. 3. The process of attribute elimination

그림 4는 표 2의 규칙 생성 과정을 설명한 것이다.

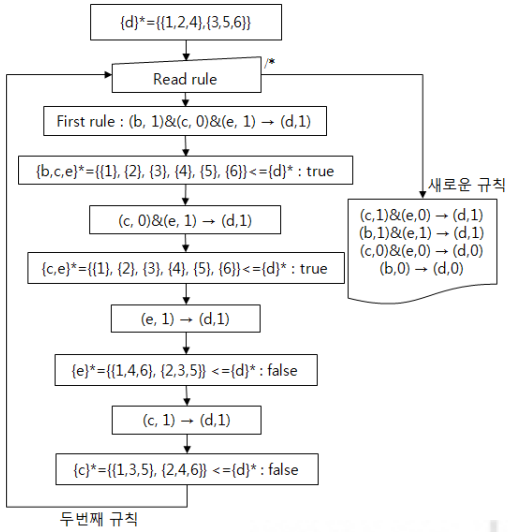

그림 4. 규칙 생성 과정
Fig. 4. The process of rule generation

이렇게 생성된 규칙을 이용하여 RSIDS는 수집된 정보를 평가하여 공격 유형으로 의심되는 정보를 SAD 모듈에 전달한다.

3.3 SAD 모듈 설계

SAD(SVM based Attack Detection) 모듈은 RRG 모듈에서 추출된 공격 의심 정보들을 공격인지를 판단하여 관리자에게 통보한다. RRG 모듈에서 추출된 공격 의심 정보를 이용하여 공격을 탐지함으로써 공격 탐지율을 향상시키고자 한다.

SAD 모듈의 공격 탐지 처리절차는 다음과 같다.

〔1 단계〕 SAD 모듈은 RRG 모듈에서 전달받은 데이터를 train data라고 정의하고, 이 데이터가 정상 또는 공격인지를 구분하기 위한 카테고리를 (normal : -1, attack : 1)로 설정한다.

〔2 단계〕 SAD 모듈은 데이터를 SVM의 카테고리로 분류한다. 입력 데이터와 출력 데이터를 다음과 같이 나타낸다.

$$(x\ , y_1), ..., (x_n, y_n), x \in \quad ^m, y \in +1, -1 \text{ 식(11)}$$

여기서, $(x_1,y_1), ..., (x_n,y_n)$는 train data이고, n은 표본의 수, m은 입력 벡터를 의미한다. 즉, x는 입력 데이터, 그리고 y는 정상 또는 공격 데이터를 의미한다.

〔3 단계〕 SAD 모듈의 분류 경계면은 그림 5와 같이 두 영역으로 나누어지며, 분류 경계면의 공식은 $(w.x) + b = 0$이다. 여기서 w는 가중치를 의미하고, b는 편이(bias)를 의미한다.

2단계의 카테고리에 따라 분류 경계면의 카테고리를 정리해보면 다음과 같다.

$$(w.x) + b \geq \text{if } y_i = +1,$$
$$(w.x) + b \leq \text{if } y_i = -1$$

이때, 마진이 최대가 되는 분류 경계면인 $(w.x) + b$을 찾는 것인 매우 어려운데, 본 논문에서는 polynomial 커널 함수를 사용하여 분류 경계면을 찾도록 설계한다.

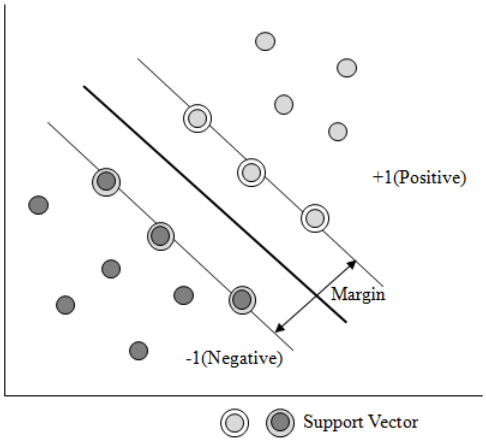

그림 5. SAD 모듈에 의한 normal, attack 분류
Fig. 5. Normal, attack classification by the SAD module

〔4 단계〕 SAD 모듈은 새로운 실험 데이터 x에 대한 분류는 다음의 식(12)에 따라 결정한다.

$$(x) = sign(\sum_{=1}^{n} \alpha_i y_i (x.x_i + b)) \qquad 식(12)$$

여기서, α_i는 라그랑지 승수로 α_i〉0이면, 그 데이터를 지지 벡터(support vector)라고 하고, $f(x)$의 계산 결과에 따라 부호가 양수이면 해당 클래스에 속한다고 판별하고, 음수이면 해당 클래스에 속하지 않는다고 판별한다.

〔5 단계〕 판별결과가 양수이면 공격으로 간주하여 관리자에게 침입탐지를 하였음을 통보한다.

IV. 시뮬레이션

본 논문의 실험환경은 운영체제 Windows XP, Intel Core Duo CPU 2.20GHz, RAM 2.0GB이고, 평가에 사용한 데이터는 1999 DARPA Intrusion Detection 오프라인 평가 데이터를 사용하였다. DARPA 1999는 DARPA에서 규정하고 있는 다양한 공격을 통하여 실험한 네트워크 패킷 데이터로, Probe, R2L, U2R, DoS로 구분할 수 있는 다양한 공격에 대한 패킷 자료를 포함하고 있다.

본 논문에서는 RRG 모듈의 DT의 decision에 5개의 클래스인 Normal, Probe, R2L, U2R, DoS로 분류하여 공격 규칙을 생성하고, 공격 정보를 탐지하도록 하였으며, SAD 모듈에서는 이 공격정보를 Normal, Probe, R2L, U2R, DoS 구분하여 공격 여부를 결정하도록 하였다.

본 논문에서는 공격 탐지율(Attack Detection Rate)은 식(13)로 계산하였고, FPR(False Positive Rate)는 식(14)로 계산하였다.

$$DR \quad \frac{\text{탐지된 공격 데이터}}{\text{공격 데이터}} \times 100 \qquad 식(13)$$

$$FPR = \frac{False\ \ Postive\text{로 판단된 데이터}}{\text{데이터}} \times 100 \qquad 식(14)$$

표 3은 RSIDS의 실험 결과를 기존의 SVM과 비교하여 설명한 것이다. RSIDS는 RRG 모듈은 공격에 대한 규칙을 생성하고, 그 규칙에 따라 공격 의심 패킷을 SAD 모듈에 전달한다. 공격 의심 패킷을 전달받은 SAD 모듈은 polynomial 커널 함수를 이용해 분류 경계면을 생성하여 공격을 판단함으로써 좀 더 정확하게 공격을 탐지하는 것을 알 수 있다.

표 3. SVM와 RSIDS의 ADR 평가
Table 3. The ADR evaluation of SVM and RSIDS

평가기법 / Attack Type	SVM	RSIDS
Normal	98.46	98.78
Probe	97.42	97.86
DoS	95.27	96.13
U2R	54.22	68.39
R2L	43.19	65.25
평균	77.71	85.28

표 4는 기존의 SVM과 본 논문에서 제안한 RSIDS의 FPR 평가를 설명한 것이다. RSIDS의 SAD 모듈은 RRG 모듈에 의해 추출된 공격 의심 정보를 공격으로 탐지하므로 기존의 SVM보다 FPR이 감소한 것을 알 수 있다.

표 4. SVM와 RSIDS의 FPR 평가
Table 4. The FPR evaluation of SVM and RSIDS

	SVM	RSIDS
Normal	2.43	2.02
Probe	3.37	3.04
DoS	5.6	4.52
U2R	26.28	17.81
R2L	28.56	21.95
평균	13.25	9.87

V. 결 론

본 논문에서는 RST(Rough Set Theory)와 SVM (Suppert Vector Machine) 알고리즘을 이용한 RSIDS (Rough Set Theory and SVM based Intrusion Detection System)를 설계하였다. RSIDS는 RRG(RST based Rule Generation) 모듈의 처리에 적합한 데이터 형식으로 변환시키는 PrePro(Preprocessing) 모듈을 설계하였고, 공격 자료를 분석하여 공격 규칙을 생성하고, 그 규칙을 이용하여 대량화된 데이터에서 공격정보를 추출하는 RRG 모듈을 설계하였다. 그리고 추출된 공격 정보를 이용하여 공격을 탐지하여 관리자에게 통보하는 SAD(SVM based Attack Detection) 모듈을 설계하였다.

그 결과, 기존의 SVM과 비교해볼 때, RSIDS의 평균 공격 탐지율은 77.71%에서 85.28%로 향상되었으며, 평균 FPR은 13.25%에서 9.87%로 감소하였다.

따라서 RSIDS는 기존의 SVM을 이용한 공격 탐지 기법보다 향상되었다고 할 수 있다.

참고문헌

〔1〕 Korea Internet & Security Agency, "2010 Hacking · Virus Status and Corresponding," KISA-RP-2010- 0051, 2011.06.

〔2〕 Z. Pawlak, "Rough sets : Theoretical Aspects of Reasoning About Data," Kluwer Academic Publishers Norwell, pp.9-29, 1991

〔3〕 Wan-Seok Seo, Jae-Yearn Kim, "Discretization of Continuous Attributes based on Rough Set Theory and SOM," Journal of industrial and systems engineering, Vol.28, No.1, pp.1-7, 2005.01.

〔4〕 Jan Komorowski, Lech Polkowski, Andrzej Skowron, "Rough Sets : A Tutorial," http://secs.ceas.uc.edu/~mazlack/dbm.w2011/Komorowski.RoughSets.tutor.pdf

〔5〕 Z. Pawlak, "Rough sets and intelligent data analysis," Information Sciences, Vol.147, Issues 1-4, pp.1-12, 2002.12.

〔6〕 Hearst, M. A., S. T. Dumais, E. Osman, J. Platt, and B. Scholkopf, "Support vector machines," IEEE Intelligent System, Vol.13, No.4, pp.18-28, 1998.04.

〔7〕 Hyeon-Uk Lee, Ji-Hun Kim, Hyunchul Ahn, "An Integrated Model based on Genetic Algorithms for Implementing Cost-Effective Intelligent Intrusion Detection System," Journal of Intelligence and Information System, vol.18, No.1, pp.125-141, 2012.01.

〔8〕 Hyunchul Ahn, Kyoung-jae Kim, Ingoo Han, "Purchase Prediction Model using Support Vector Machine," Journal of Intelligence and Information System, Vol.11, No.3, pp.69-81, 2005.03.

〔9〕 Jaepil Ko, "Solving Multi-class Problem using Support Vector Machines," Journal of KISS : Software and Applications, Vol.32, No.12, pp.1260- 1270, 2005.12.

저 자 소 개

이 병 관

1979: 부산대학교 기계설계학과 공학사.

1986: 중앙대학교 전자계공학과 공학석사.

1990: 중앙대학교 전자계산공학과 공학박사

현 재: 관동대학교 컴퓨터학과 교수

관심분야: 네트워크 보안, 인터넷 보안

Email : bklee@kd.ac.kr

정 은 희

1991: 강릉대학교 통계학과 이학사.

1999: 관동대학교 전자계산공학과 공학석사.

2003: 관동대학교 전자계산공학과 공학박사

현 재: 강원대학교 지역경제학과 부교수

관심분야: 네트워크보안, 인터넷보안

Email : jeongeh@kangwon.ac.kr