상대 복잡도를 이용한 네트워크 연결기반의 탐지척도 선정

문 길 종[†] · 김 용 민[††] · 김 동 국[†††] · 노 봉 남[††††]

요 약

최근 네트워크가 발전함에 따라 네트워크의 취약점을 이용한 침입과 공격이 많이 발생하고 있다. 네트워크에서 공격과 침입을 탐지하기 위해 규칙을 만들거나 패턴을 생성하는 것은 매우 어렵다. 대부분 전문가의 경험에 의해서 만들어지고, 많은 인력, 비용, 시간을 소비하고 있다. 본 논문에서는 전문가의 경험 없이 네트워크의 공격 행위를 효과적으로 탐지하기 위해서 네트워크 연결기반의 정보를 이용한 척도선정 기법과 탐지기법을 제안한다. 정상과 각 공격의 네트워크 연결 데이터를 추출하고, 상대 복잡도를 이용하여 복잡도의 임계값 설정함으로써 공격 탐지에 유용한 척도를 선정한다. 그리고 선정된 척도를 바탕으로 확률패턴을 생성하고 우도비 검증을 이용해 공격을 탐지한다. 이 탐지방법으로 임계값 조절에 따라 탐지율과 오탐율을 조절할 수 있었다. KDD CUP 99 데이터를 이용하여 공격행위를 분석, 분류하고, 결정트리 알고리즘의 규칙기반 탐지 결과와 비교함으로써 본 논문에서 제시한 기법이 유용함을 확인하였다.

키워드 : 침입 탐지, 상대 복잡도, 우도비, 네트워크 척도

Selection of Detection Measures using Relative Entropy based on Network Connections

Gil-Jong Mun[†] · Yong-Min Kim[††] · DongKook Kim[†††] · Bong-Nam Noh[††††]

ABSTRACT

A generation of rules or patterns for detecting attacks from network is very difficult. Detection rules and patterns are usually generated by Expert's experiences that consume many man-power, management expense, time and so on. This paper proposes statistical methods that effectively detect intrusion and attacks without expert's experiences. The methods are to select useful measures in measures of network connection(session) and to detect attacks. We extracted the network session data of normal and each attack, and selected useful measures for detecting attacks using relative entropy. And we made probability patterns, and detected attacks using likelihood ratio testing. The detecting method controled detection rate and false positive rate using threshold. We evaluated the performance of the proposed method using KDD CUP 99 Data set. This paper shows the results that are to compare the proposed method and detection rules of decision tree algorithm. So we can know that the proposed methods are useful for detecting intrusion and attacks.

Key Words : Intrusion Detection, Relative Entropy, Likelihood Ratio, Network Measures

1. 서 론

현대사회는 정보화 기술이 발달함에 따라 인터넷, 통신, 채팅 등의 네트워크 사용이 증가되고 있으며 많은 사람들이 손쉽게 인터넷에 접근할 수 있는 정보화 사회이다. 네트워크가 일상생활에서 일반화됨으로써 시간단축, 정보획득, 거리단축 등의 많은 혜택을 얻고 있다. 그러나 네트워크 기술이 발달함에 따라 이를 악용하려는 사례도 늘어나고 있다. 그 중 가장 큰 문제점으로 대두되고 있는 것이 네트워크와 시스템의 취약점을 악용하는 공격들이다. 이 공격들은 시스템을 정지시키고, 정보를 훔쳐가는 등의 악의적인 행위를 하고 있으며, 인터넷을 통해 급속도로 전파되고 있다. 또한 네트워크 공격과 침입은 누구나 사용법만 익히면 쉽게 사용할 수 있어서, 그 문제가 더욱 심각하다. 현대사회는 이러한 네트워크 공격과 침입으로 인하여 시스템자원의 파괴와 불법적인 데이터 유출 등의 피해를 방지하기 위해 침입을 탐지하는 기술이 필수적으로 요구되고 있다.

침입탐지 시스템(IDS : Intrusion Detection System)은 악의적인 사용자로부터 컴퓨터 시스템으로의 불법적인 접근 및 오용행위를 감지하여 관리자에게 통보하거나 각종 침입행위를 기록하기 위한 시스템이다. 즉 컴퓨터 시스템에 대하여 인

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성지원 사업의 결과로 수행되었음.
† 준 회 원 : 전남대학교 정보보호협동과정 석사과정
†† 정 회 원 : 여수대학교 정보기술학부 전임강사
††† 정 회 원 : 전남대학교 전자컴퓨터정보통신공학부 전임강사
†††† 종신회원 : 전남대학교 전자컴퓨터정보통신공학부 교수
논문접수 : 2005년 9월 1일, 심사완료 : 2005년 10월 20일

가 유무에 의해 사용자의 오용, 남용, 비정상적인 사용 등을 알려주는 시스템으로 정의할 수 있다[1].

네트워크상의 패킷들은 *protocol, sequence number, flag, window size, packet size* 등의 많은 척도들을 가지고 있지만, 패킷에서 추출한 척도는 네트워크 세션(session)의 척도보다 단편적인 정보를 가지고 있어 정상과 공격을 분류 및 분석하기 힘들다. 본 논문에서는 정상과 각 공격을 네트워크 세션 별로 분류하고, 이를 통계기법을 사용하여 유용한 척도를 선정하고 공격을 탐지하는 기법을 제안한다. 신뢰성 있는 실험을 위해 네트워크 데이터가 세션 별로 추출되어 있는 KDD(Knowledge Discovery in Database) CUP 99 데이터[2]를 학습 및 테스트 데이터로 사용했다. 그리고 다른 알고리즘의 결과와 비교를 위해 C4.5를 통한 규칙 생성과 탐지 결과를 비교 제시한다.

2. 관련 연구

침입탐지 시스템은 일반적으로 호스트기반 탐지(host-based detection)와 네트워크기반 탐지(network-based detection)로 구분할 수 있고, 침입을 탐지하는 방법으로는 비정상행위 탐지(anomaly detection) 기법과 오용행위 탐지(misuse detection) 기법으로 구분할 수 있다. 현재 침입탐지 시스템은 대부분 다량의 네트워크 패킷을 실시간으로 탐지할 수 있도록 하기 위해 비정상행위 탐지와 오용행위 탐지 기법을 병행하고 있다. 본 논문에서는 오용행위 탐지기법을 기본으로 하고 있다. 오용행위 탐지 기법은 패킷으로부터 얻어지는 척도(feature)를 분석 및 분류하고 이를 규칙(rule) 또는 패턴(pattern)으로 생성하여 탐지하는 방법이다. 데이터 마이닝(data mining)이나 기계 학습(machine learning)을 이용하여 시간과 비용이 많이 드는 전문가 기반 시스템의 단점을 보완 하고 있다. 하지만 규칙 기반(rule-based) 침입탐지 시스템은 학습하지 않은 공격에 대해서는 탐지 할 수 없는 단점이 있기 때문에, 이것을 해결하기 위해 통계기반 침입탐지 기법이 제안되었다.

통계기반 침입탐지(SBID : A Statistical-Based Intrusion Detection)는 베이지 이론(Baye's theorem)과 같은 통계 모델을 바탕으로 하고 있다. 그리고 비정상행위를 탐지하는데 주로 사용하는 방법이다. 시스템, 사용자의 행동을 시간 변화에 따라 여러 가지 척도를 기준으로 데이터를 수집한다. 각 세션의 연결시간, 프로세스 사용량, 메모리 할당량 등이 그 예이다. 정보를 수집하고 이를 통계적으로 분석한 후, 입력된 정보와 비교하여 침입을 탐지하는 것이다. 통계기반 침입탐지 모델은 1988년 이후로 개발된 규칙기반 탐지 모델과 통계 기반 탐지 모델을 결합한 IDES(Intrusion Detection Expert System)[3]와 네트워크에 있는 메인프레임의 정보보호를 위해 배치된 실시간 MIDAS(Monitoring, Intrusion Detection, Administration System)[4]가 있다. 그리고 스노트(snort)에서 플러그인으로 작동하는 SPADE(Statistical Packet Anomaly Detection Engine)[5]와 그 외에 Haystack[6]등이 제안되었다.

3. 통계적 침입탐지시스템

이 장에서는 통계적 기법을 이용하여 척도를 선정하고 공격을 탐지하는 알고리즘을 제안한다. 먼저 실험 데이터로 사용된 KDD CUP 99 데이터와 통계적 침입탐지 시스템의 구성에 대해 살펴보고, 제안된 통계적 기법에 근거한 척도 선정과 침입탐지 기법을 제시한다.

3.1 KDD CUP 99 데이터

KDD CUP 99 데이터는 1998년 DARPA[7] 덤프(dump)를 침입 탐지에 관련된 척도를 추출하여 제공한 것이다. KDD CUP 99 데이터는 크게 <표 1>과 같은 DoS(Denial of Service), R2L(Remote to Local), U2R(User to Root), Probes의 4가지 공격 유형과 정상으로 분류한다.

〈표 1〉 KDD CUP 99의 훈련 데이터의 공격 유형과 이름

공격 유형	공격 이름
DoS	back, land, neptune, pod, smurf, teardrop
R2L	buffer_overflow, load_module, multihop, phf, spy, warezclient, warezmaster
U2R	ftp_write, guess_passwd, imap, load_module, perl, rootkit,
Probes	ipsweep, nmap, portsweep, satan

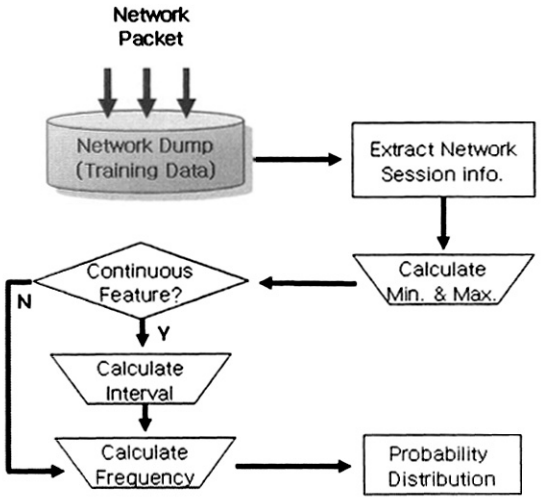
KDD CUP 99 데이터는 네트워크 세션정보로 구성되어 있고, 크게 3가지 유형으로 구분할 수 있다. *duration, protocol type, flag* 등과 같은 각 TCP 세션의 기본적인(Basic) 척도들과 *logged in, su attempted, hot* 등과 같은 세션 안에서의 콘텐츠(Contents) 척도들, 그리고 *packet count, syn error rate* 등과 같은 트래픽(Traffic) 척도들로 나눌 수 있다. 이 척도들은 다시 이산적인(discrete) 척도와 연속적인(continuous) 척도라는 두 가지 속성으로 나뉜다. 세션 상의 *duration, ugent* 등의 정보는 연속적인 속성을 가지고 있으며, *protocol_type, service* 등의 척도는 이산적인 속성을 갖는다. <표 2>는 KDD CUP 99 데이터를 구분한 것이다.

〈표 2〉 KDD CUP 99의 척도유형에 따른 3가지 분류와 값에 따른 2가지 속성

척도유형	척도속성	척도 이름	개수
basic feature	이산형	protocol_type, service, flag, land	4
	연속형	duration, src_byte, dst_byte, wrong_fragment, urgent	5
contents feature	이산형	logged_in, root_shell, su_attempted, is_hot_login, is_guest_login	5
	연속형	hot, num_failed_logins, num_file_creations, num_shells, num_access_files ,num_outbound_cmds, num_compromised, num_root	8
traffic feature	이산형	-	0
	연속형	count, serror_rate, rerror_rate, srv_rerror_rate, same_srv_rate, diff_srv_rate, srv_diff_host_rate, st_host_count, dst_host_srv_count, dst_host_same_srv_rate, dst_host_diff_srv_rate, dst_host_same_src_port_rate, dst_host_srv_diff_host_rate, st_host_serror_rate, dst_host_srv_serror_rate. dst_host_rerror_rate, dst_host_srv_rerror_rate	19

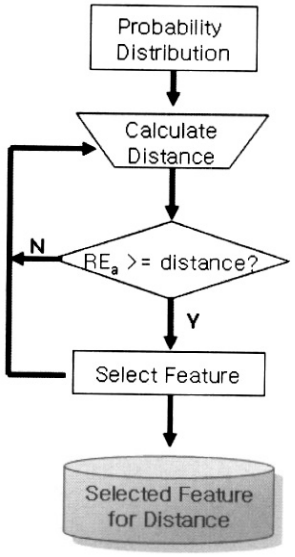
3.2 시스템 구성도

본 논문에서 제시한 침입탐지 구성도는 (그림 1, 2, 3)과 같은 3단계로 구성되어 있다.



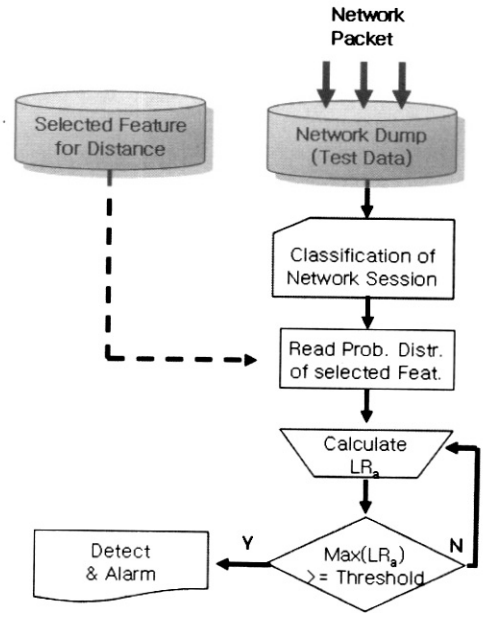
(그림 1) 데이터 수집, 가공 및 처리(1단계)

1단계는 데이터 수집, 가공 및 처리 과정으로써, 네트워크 데이터를 덤프 데이터로 저장하고, 저장된 패킷 데이터를 실험에 필요한 세션 기반 정보로 변환한다. 그리고 각 공격에 해당하는 각 척도의 확률분포(probability distribution)를 구하고 저장한다.



(그림 2) 척도 선정(2단계)

2단계는 척도를 선정하는 과정이다. 1단계에서 구한 정상 데이터와 각 공격 데이터의 확률분포를 바탕으로 공격 판단에 유용한 척도를 각 공격 척도의 상대 복잡도를 사용하여 선정하는 과정이다. (그림 2)에서 RE_a는 각 공격 척도의 상대 복잡도이고 distance는 임계값이다($a \in \{a_1, a_2, ..., a_n\}$, n은 공격개수).



(그림 3) 공격 탐지 테스트 (3단계)

3단계는 우도비를 이용한 테스트 과정이다. 학습단계에서 선정한 척도에 대해서 확률 분포 패턴과 테스트 정보를 비교한 후, 임계값(threshold)을 이용하여 탐지율과 오탐율을 조절한다. LR_a는 각 공격의 우도비 값이다.($a \in \{a_1, a_2, ..., a_n\}$, n은 공격개수) 실험의 신뢰성을 위해 네트워크 데이터가 세션별로 추출되어 있는 KDD CUP 99 데이터를 사용하였다. 그러므로 1단계에서 데이터 수집, 가공 및 처리 단계를 생략하였다.

3.3 척도의 특징과 분류

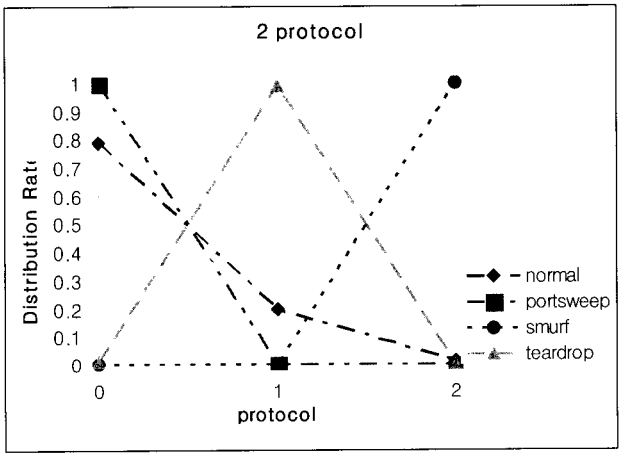
통계적 기법에 근거하여 유용한 척도를 선정하기 위해 먼저 각 공격과 정상에 대한 각 척도의 확률 분포가 필요하다. 이산적인 유형의 값을 가지는 척도는 각 값에 해당하는 빈도를 이용하여 확률 분포를 쉽게 구할 수 있다. 그러나 연속적인 유형의 값을 갖는 척도는 각 값이 일정하지 않아서, 그에 해당하는 확률 분포를 구하는 것이 어렵다. 그래서 그 척도의 최소, 최대값을 구한 후, 연속적인 유형의 데이터를 일정한 구간(interval)으로 나누어 이산화 시킨다. 연속적인 유형의 값을 이산적인 유형의 값으로 변화시킴으로써, 그에 해당하는 구간의 빈도를 계산하여 확률 분포를 구할 수 있다. 그리고 <표 2>에서 제시한 연속적인 유형의 척도라 할지라도 일정한 값을 갖는 척도가 존재한다. 그 척도에 대해서는 간격을 나누지 않고 이산적인 유형의 척도처럼 각 값에 대한 통계값을 구한다.

<표 3>은 KDD CUP 99에서 제시한 분류를 다시 구성한 것이다. 굵은 글씨는 연속형 척도가 이산형 척도로 재분류된 것이다. 기본 척도와 컨텐츠 척도는 연속형 척도를 이산형 척도로 변환할 수 있는 척도가 각 2, 6개 존재함을 알 수 있었다. 트래픽 척도는 네트워크 패킷의 통계량을 사용하므로 이산형 척도로 변환할 수 있는 척도가 존재 하지 않았다.

〈표 3〉 확률 분포를 통해 재분류한 KDD CUP 99의 3가지 타입과 2가지 유형

척도타입	척도유형	척도 이름	개수
basic feature	이산형	protocol_type, service, flag, land, wrong_fragment, urgent	6
	연속형	duration, src_byte, dst_byte	3
contents feature	이산형	logged_in, root_shell, su_attempted, is_hot_login, is_guest_login, hot, num_failed_logins, num_file_creations, num_shells, num_access_files,num_outbound_cmds	11
	연속형	num_compromised, num_root	2
traffic feature	이산형	-	0
	연속형	count, serror_rate, rerror_rate, srv_rerror_rate, same_srv_rate,diff_srv_rate, srv_diff_host_rate, dst_host_count,dst_host_srv_count, dst_host_same_srv_rate, dst_host_diff_srv_rate, dst_host_same_src_port_rate, dst_host_srv_diff_host_rate, st_host_serror_rate, dst_host_srv_serror_rate. dst_host_rerror_rate, dst_host_srv_rerror_rate	19

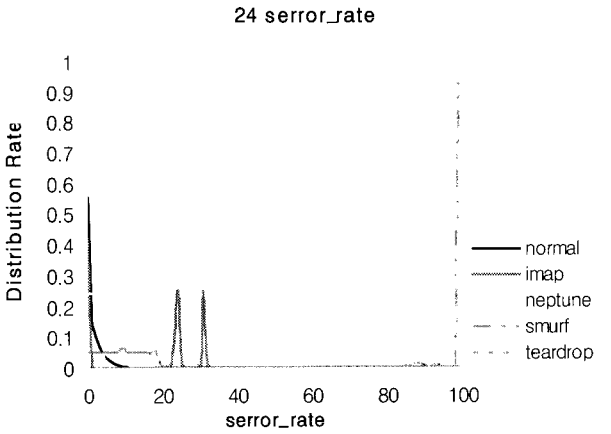
이산형 척도와 연속형 척도를 이산형 척도로 변환하는 과정을 통해 KDD CUP 99 데이터로부터 각 공격과 정상에 대한 각 척도의 확률분포를 구했다. 구해진 확률 분포를 분석한 결과 공격과 정상을 구분할 수 있는 특징을 가지는 척도가 존재함을 알 수 있었다.



(그림 4) 이산형 척도인 protocol에 대한 확률 분포로써, 0은 TCP를 나타내고, 1은 UDP, 2는 ICMP를 나타냄

공격과 정상을 구분할 수 있는 특징을 가지는 척도 중 (그림 4)는 이산적인 유형의 *protocol* 척도의 확률 분포를 나타낸 것이다. KDD CUP 99에서 제시한 41개의 척도 중 2번째 척도인 *protocol*은 이산적인 유형의 특징을 가지고 있으며, 네트워크 연결이 TCP 프로토콜을 이용하면 0의 값을 가지고 UDP를 이용하면 1의 값, ICMP는 2의 값을 가진다[2]. (그림 4)에서 portsweep 공격의 분포를 살펴보면 100% TCP를 이용하는 특징을 살펴볼 수 있었고, smurf 공격은 100% ICMP 프로토콜을 이용하고, teardrop 공격은 UDP를 이용함을 알 수 있다. 이 외에도 그림에서는 생략됐지만 land, warezmaster, loadmodule 등의 공격들이 TCP 프로토콜을 이용함을 알 수 있었고, 그와 비교하여 phf, nmap 공격은 고른 프로토콜 분포를 보였으며, ipsweep, pod 공격은 ICMP 프로토콜을 이용하는 것을 알 수 있었다.

(그림 5)는 연속적인 유형의 척도 중 *serror_rate*의 확률 분포를 나타낸 그래프이다. 연속적인 유형의 척도 *serror_rate*는 한 개의 연결 중에 "SYN" 에러비율에 대한 확률 분포 그래프이다. smurf 공격은 100% 에러를 발생함을 알 수 있고, normal을 포함한 imap, neptune, teardrop 공격은 비교적 낮은 "SYN" 에러비율을 가지고 있음을 알 수 있다. (그림 5)에서는 표현하지 않았지만 spy, rootkit 등의 공격들은 100% 에러가 없음을 알 수 있었다.



(그림 5) 연속형 척도인 24번째 serror_rate의 확률 분포

(그림 4, 5)에서 제시한 두 가지 척도 외에도 정상과 비교해 공격을 구분할 수 있는 척도들이 존재하는 것을 실험을 통해 알 수 있었다.

3.4 통계적 기법에 근거한 척도 선정 및 탐지 알고리즘

본 논문에서는 KDD CUP 99 데이터 중에서 kddcup.data_10percent.data를 훈련 데이터로 사용한다. 이 데이터는 kddcup.data의 10%인 75MB를 사용하고 있으며, 이는 정상과 22가지의 공격이 포함된 데이터이다. kddcup.data_10percent.data는 kddcup.data에 포함된 데이터 중 몇 개의 공격들이 다른 공격들에 비해서 너무 많은 데이터를 가지고 있는 것을 조절하기 위한 데이터이다. 테스트 데이터는 corrected.data로써 KDD CUP 99에서 테스트 데이터로 제공한 것다. 이것은 학습에 포함되어 있던 22가지 공격 외에 snmpgetattack, named, xsnoop 등의 17가지 새로운 공격을 포함하고 있다. <표 4>는 KDD CUP 99 데이터의 훈련 데이터와 테스트 데이터의 각 공격에 대한 개수이다.

KDD CUP 99 데이터는 모두 41개의 세션 척도를 제공한다. 하지만 이 모든 척도들이 정상과 각 공격들을 구분할 수 있는 특징을 가지고 있는 것은 아니다. 본 논문에서는 각 공격별로 정상과의 특징을 구별하기 위해 확률 분포 사이의 거리를 구하는데, 사용되는 상대 복잡도[8, 9]를 탐지에 유용한 척도 선정의 방법으로 사용하였다. 상대 복잡도는 비정상행위 탐지 시 훈련 데이터와 테스트 데이터의 유사함을 판단

〈표 4〉 훈련과 테스트 데이터에 포함된 공격 개수

	data file(.data)	kddcup 10%	kddcup	correct
no	공격 이름	개수		
1	Normal	97277	972780	60593
2	buffer_overflow	30	30	22
3	loadmodule	9	9	2
4	perl	3	3	2
5	neptune	107201	1072017	58001
6	smurf	280790	2807886	164091
7	guess_passwd	53	53	4367
8	pod	264	264	87
9	teardrop	979	979	12
10	portsweep	1040	10413	354
11	ipsweep	1247	12481	306
12	land	21	21	9
13	ftp_write	8	8	3
14	back	2203	2203	1098
15	imap	12	12	1
16	satan	1589	15892	1633
17	phf	4	4	2
18	nmap	231	2316	84
19	multihop	7	7	18
20	warezmaster	20	20	1602
21	warezclient	1020	1020	0
22	spy	2	2	0
23	rootkit	10	10	13
24	etc	0	0	18729

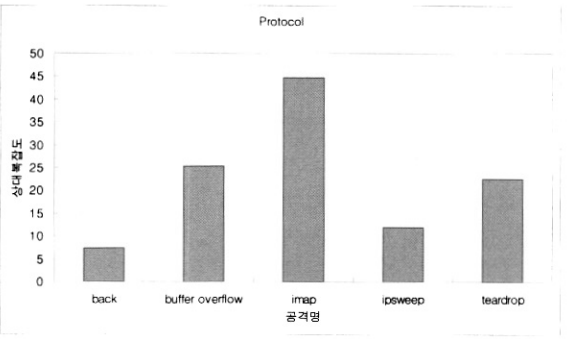
하기 위해 사용되기도 한다. 상대 복잡도가 작으면 두 데이터는 비슷한 데이터로 판단을 할 수 있고, 높으면 높을수록 전혀 다른 데이터로 판단할 수 있다.

$$D_{KL}(p(X)\,|\,q_j(X)) = \sum_X q_j(X)\ln\left(\frac{q_j(X)}{p(X)}\right) \qquad (1)$$
$$D_j = D_{KL}(p(X)\,|\,q_j(X)) + D_{KL}(q_j(X)\,|\,p(X))\ (j = 1, 2, \ldots, n)$$

식 (1)에서 X는 척도의 벡터(vector) 집합 $X \in \{ x_1, x_2, \ldots, x_N\}$을 나타내는 랜덤변수(random variable)이며, $_N$은 척도의 전체 개수이다. 그리고 각 척도는 서로 독립적이라 가정한다. p(X)는 정상에 대한 X의 확률 분포이고, $q_j(X)$는 j번째 공격에 대한 확률 분포이다($j \in \{ 1, 2, \ldots, n\}$, n은 공격개수). D_{KL}은 정상과 j번째 공격에 대한 상대 복잡도이다. p(X)와 $q_j(X)$의 위치가 바뀌었을 때, D_{KL}값은 달라지므로 거리를 구할 수 없다. D_j는 $D_{KL}(p(X)|q_j(X))$의 상대복잡도와 위치가 바뀐 $D_{KL}(q_j(X)|p(X))$의 합을 구함으로써, 두 랜덤변수의 위치에 따른 값의 변화를 막을 수 있다.

(그림 6)은 식 (1)을 사용해서 각 공격의 척도 중 *protocol*의 상대 복잡도를 구한 결과이다. 공격 imap은 정상 데이터와 많은 차이점을 보이는 것을 알 수 있었다. 이같이 정상 데이터와 많은 차이를 보이는 것일수록 해당 공격을 판단하는데 유용한 척도임을 알 수 있다.

침입 탐지를 위해서는 각 공격에서 선정된 척도에 해당하는 확률의 차이를 구하는 기법이 필요하다. 본 논문에서는 베이즈 정리(Baye's theorem)에 근거한 우도비 검증(Likelihood 특정 벡터 X가 주어졌을 경우, 그 특정 벡터가 속한 클래스를 결정하는 문제에 우도비 검증이 주로 사용된다.



(그림 6) 각 공격의 프로토콜 척도에 따른 상대복잡도의 차이

공격 a의 가설 H_{1a}과 공격 a일 때의 정상 가설 H_{0a}가 있다. 그리고 공격 a에 대해 선정된 척도의 집합은 $X_a = \{ x_{a1}, x_{a2}, \ldots, x_{aM}\}$, ($a_M$은 공격 a에 대해 선정된 척도 개수)이다. 각 테스트 데이터가 공격인 것을 판단하는 것은 식 (2, 3, 4)를 통해서 알 수 있다. 식 (2, 3)은 각 척도 $x_{a1}, x_{a2}, \ldots, x_{aM}$는 서로 독립적이라는 가정 하에 성립한다. $a \in \{ 1, 2, \ldots, m\}$는 공격 번호이며, X는 선정된 척도의 벡터집합이다.

식 (2)는 공격 a에 대한 정상일 가설 H_{0a}에서 선정된 척도에 대한 확률의 합을 나타낸다.

$$p(X|H_{0a}) = p(x_{a1}|H_{0a})p(x_{a2}|H_{0a})\ldots p(x_{an}|H_{0a}) = \sum_{i=1}^{n} p(x_{ai}|H_{0a}) \qquad (2)$$

식 (3)는 공격 a에 대한 공격일 가설 H_{1a}에서 선정된 척도에 대한 확률의 합을 나타낸다.

$$p(X|H_{1a}) = p(x_{a1}|H_{1a})p(x_{a2}|H_{1a2})\ldots p(x_{an}|H_{1a}) = \sum_{i=1}^{n} p(x_{ai}|H_{1a}) \qquad (3)$$

식 (4)는 구해진 $p(X|H_{1a})$와 $p(X|H_{0a})$를 이용해 모든 공격에 대한 우도비를 구한 후, 임계값을 적용한다.

$$\max\left\{L_a = \frac{p(X|H_{1a})}{p(X|H_{0a})}\right\} \geq threshold \qquad (4)$$

모든 공격에 대한 최대 L_a가 임계값 이하일 경우, 공격이 아닌 정상으로 판단하게 된다. 그리고 임계값 이상일 때, 최대값을 가지는 공격 a를 최종 공격으로 판단하게 된다. 식 (4)의 임계값을 사용하여 탐지율과 오탐율을 조절할 수 있음을 실험을 통해 알 수 있었다.

4. 실험 및 결과

이 장에서는 3장에서 제시한 기법을 바탕으로 KDD CUP 99 데이터로 실험하여 얻은 유용한 척도와 탐지결과를 제시한다. 척도 선정을 위해 KDD CUP 99 데이터의 kddcup.

data_10_percent.data를 사용하고, 침입 탐지를 위한 테스트 데이터로 kddcup.data와 corrected.data를 사용한다. kddcup data는 학습에서 사용된 데이터의 100% 데이터이고, corrected. data는 학습에서 존재했던 공격과 존재 하지 않았던 새로운 17개의 공격을 포함하고 있는 테스트 데이터이다.

4.1 척도 선정

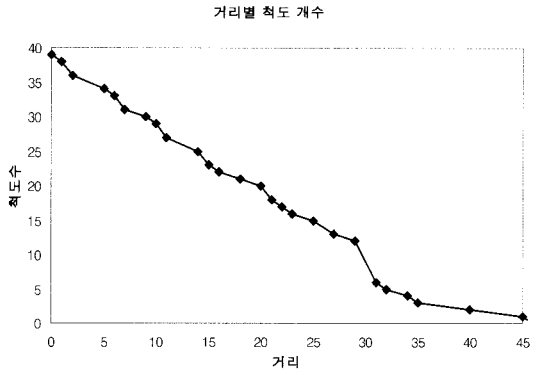
침입을 탐지하기 위해 3장에서 제시한 척도 선정 기법을 적용하여 유용한 척도를 선정한다. 실험을 통해 얻은 결과인 <표 5>는 실험을 통해 $D_j \geq distance(distance = \{ 0.0, 1.0, ..., 14.0\})$를 만족하는 공통 척도를 보여준다. 전체 거리에서 선정된 척도와 선정되지 않은 척도는 제외됐다. <표 5>에서 제시한 척도는 결정트리 알고리즘으로 탐지 패턴을 생성하기 위해서 사용된다. (그림 7)은 거리의 변화에 따른 척도 개수를 표현한 것으로써, 거리가 늘어남에 따라 2~4개의 척도들이 선정되지 않았음을 알 수 있다. 공통적으로 선택된 척도들은 결정 트리를 이용한 규칙 탐지와 본 논문에서 제시한 통계적 기법의 결과를 비교하기 위해 사용된다. 실험 결과로 $D_j \geq 14.0$일 때, 각 공격에서 선정되는 척도가 존재하지 않아서, $D_j \geq 14.0$ 이상의 조건에 만족하는 거리에 대한 실험은 실행하지 않았다.

4.2 침입탐지 실험결과

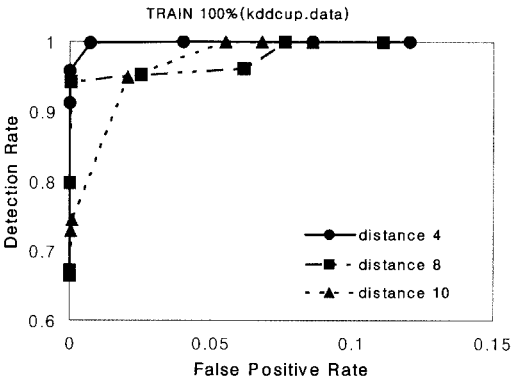
선정된 척도를 사용하여 탐지실험을 하였다. 우선 kddcup.data_10_percent.data를 사용하여 학습 후, 학습 데이터의 100%인 kddcup.data로 선정된 척도에 의한 탐지를 수행함으로써 성능이 좋은 탐지를 위한 거리와 임계값을 얻을 수 있음을 증명할 수 있다. 거리의 변화에 따라서 선정된 척도를 이용해 테스트해 본 결과, (그림 8, 9)와 같은 결과가 나타났다. 거리는 0.0~14.0까지 실험하였고, 그 중 중복되거나 비슷한 결과를 제외하고 3개의 결과만 제시한다.

(그림 8)은 kddcup.data에 대한 테스트로써 탐지율(detection rate)과 오탐율(false positive rate)을 Receiver Operating Characteristic(ROC) 커브로 표현한 것이다. 학습시키지 않은 90% 데이터를 합한 데이터에서 99%가 넘는 높은 탐지율과 0.02%의 낮은 오탐율이 나타남을 볼 수 있다. (그림 9)는 corrected.data를 테스트한 탐지율과 오탐율을 보여준다. 97%이상의 높은 탐지율과 0.5%의 낮은 오탐율이 나타남을 볼 수 있다.

(그림 8)과 (그림 9)를 비교했을 때, 학습에 사용한 100% 데이터의 테스트와 새로운 테스트 데이터의 ROC가 비슷한 탐지율과 오탐율을 나타내는 것을 볼 수 있다. 이로써 학습시



(그림 7) 거리의 변화에 따라 선정된 전체 척도의 개수

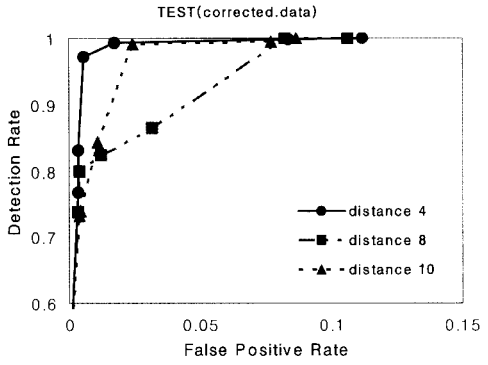


(그림 8) 학습 데이터인 kddcup.data의 테스트 결과

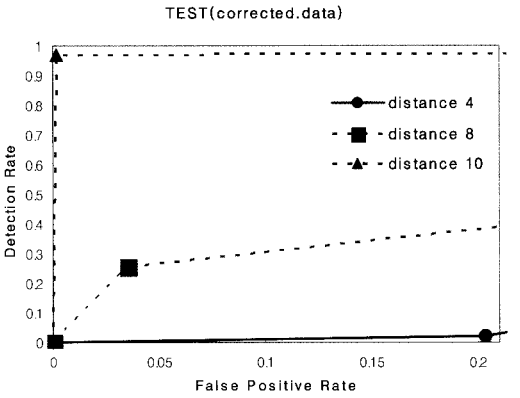
〈표 5〉 거리의 변화에 따라 선정된 공통된 척도

척도 / 거리	1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	22	23	24	28	29	30	40	41
0	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
1	o	o		o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
2		o		o	o	o	o	o	o	o	o	o	o	o	o		o	o	o	o	o	o	o
3		o		o	o	o	o	o	o	o	o	o	o	o	o		o	o	o	o	o	o	o
4		o		o	o	o	o	o	o	o	o	o	o	o	o		o	o	o	o	o	o	o
5		o		o	o	o	o	o	o	o		o		o	o		o	o	o	o	o	o	o
6		o		o	o	o		o	o	o		o		o	o		o	o	o	o	o	o	o
7		o		o	o	o		o	o	o		o			o		o	o		o	o	o	o
8		o		o	o	o		o	o	o		o			o		o	o		o	o	o	o
9		o		o	o	o		o	o	o		o			o		o	o		o	o	o	
10		o		o	o	o		o	o	o		o			o		o	o		o	o	o	
11		o			o	o		o	o	o		o			o		o	o		o	o		
12		o			o	o		o	o	o		o			o		o	o		o	o		
13		o			o	o		o	o	o		o			o		o	o		o	o		
14		o			o	o		o		o		o			o		o	o			o		

삭제된 척도 중 전체 거리에서 선정된 것 : 3, 4, 18, 19, 25~27, 31~39
삭제된 척도 중 전체 거리에서 선정되지 않은 것 : 20, 21



(그림 9) 테스트 데이터인 corrected.data의 테스트 결과



(그림 10) C4.5를 이용한 corrected.data의 테스트 결과

킨 데이터에 포함된 공격과 테스트에 포함된 공격이 비슷한 통계적 특징을 가지고 있다는 것을 알 수 있고, 본 논문에서 제시한 기법을 통해서 공격을 탐지했을 때, 좋은 결과를 얻을 수 있음을 알 수 있었다. (그림 10)은 결정 트리 알고리즘 중 C4.5[11]를 사용하여 거리 변화에 다른 규칙을 생성 후, corrected.data의 테스트 결과이다. (그림 9)와 (그림 10)을 비교해봄으로써, 통계적 기법을 이용한 탐지와 C4.5의 규칙 기반 탐지의 결과를 비교할 수 있다. 탐지율과 오탐율은 비교적 비슷한 결과를 나타내는 것을 볼 수 있다. 하지만 본 논문에서 제시한 통계기반의 탐지와 C4.5의 규칙기반 탐지를 실험을 비교했을 때, 통계기반의 탐지기법은 탐지에 영향을 미치는 유용한 척도를 각 공격 별로 찾을 수 있었고, 임계값을 조정함으로써 탐지율과 오탐율을 조정할 수 있었다. 그에 비해 결정 트리 기반의 규칙기반 탐지는 각 공격의 유용한 척도를 따로 선정할 수 없어서, 공통된 척도를 선택해야만 했다. 그리고 생성된 규칙에 의해서만 탐지가 되므로 탐지율을 극대화시키거나, 오탐율을 극소화 시키는 임계값을 적용할 수 없다.

<표 6>은 (그림 9)의 테스트 결과 중 $D_j \geq 4.0$에 만족하는 임계값에 따른 탐지율과 오탐율을 나타낸 것이다. 그 중 임계값이 0.3일 때 97%의 탐지율과 0.01%의 오탐율이 나타나는 것을 볼 수 있고, 임계값에 따라 탐지율과 오탐율을 조절할 수 있는 것을 볼 수 있다.

(그림 8, 9)의 실험 결과를 살펴봄으로써 최적의 척도를 선정할 수 있었다. <표 7>은 통계적인 기법을 이용하여 침입탐지를 실행했을 때 가장 탐지율이 높고, 오탐율이 낮은 $D_j \geq 4.0$에서 선정된 각 공격의 척도들이다. 각 공격에 따라 다른 척도들이 선택되었음을 알 수 있다. 본 실험을 통해 최적의 척도를 선정함으로써, 각 공격의 선정된 척도만으로 공격을 판단할 수 있는 것을 알 수 있다.

〈표 6〉 $D_j \geq 4.0$을 만족하는 각 공격의 척도

$D_j \geq 4.0$	2	3	4	6	7	8	9	10	11	12	13	14	15	16	17	18	19	23	24	25	26	27	28	29	30	31	32	33	34	35	36	38	39	40	41
back	o	o						o		o																			o	o				o	o
land	o	o	o		o					o								o	o	o	o				o	o	o	o	o	o	o	o		
neptune	o	o	o							o								o		o	o			o	o		o	o	o	o	o	o	o		
pod	o	o				o				o																o	o	o	o	o	o				
smurf	o	o								o								o	o							o	o	o			o				
teardrop	o	o				o				o								o								o	o	o	o	o	o				
buffer overflow	o	o						o		o		o						o	o							o	o	o	o	o	o				
loadmodule	o	o													o	o		o	o							o	o	o	o	o	o				
perl	o	o								o		o			o	o		o	o							o	o	o	o	o	o			o	
rootkit		o																o	o							o	o	o	o	o	o				
ftp_write	o	o					o											o	o							o	o	o	o	o	o				
guess password	o	o	o					o	o									o	o			o	o			o	o	o	o	o	o	o	o	o	o
imap	o	o	o															o	o	o	o		o			o	o	o	o	o	o	o	o		
phf	o	o						o		o		o					o	o	o							o	o	o	o	o	o				
multihop	o	o						o			o			o	o			o	o							o	o	o	o	o	o				
spy	o	o											o					o	o							o	o	o	o	o	o	o	o		
warezclient	o	o						o		o								o	o							o	o	o		o	o				
warezmaster	o	o		o														o	o							o	o	o	o	o	o				
ipsweep		o								o								o								o	o		o	o	o				
nmap		o	o							o								o								o	o	o	o	o	o	o	o		
portsweep		o	o							o									o			o	o			o	o	o	o	o	o			o	o
satan		o	o							o								o		o		o		o	o	o	o	o	o	o		o		o	o

선택되지 않아 생략된 척도 : 1, 5, 20~22
전부 선택되어 생략된 척도 : 37

〈표 7〉 (그림 9)에서 거리가 4일 때, 임계값 변화에 따른 탐지율과 오탐율의 변화

임계값	탐지율(Detection Rate)	오탐율(False Positive Rate)
0.0	1.000	0.1118
0.1	0.9990	0.0833
0.2	0.9922	0.0172
0.3	0.9712	0.0056
0.4	0.8302	0.0034
0.5	0.7678	0.0033
0.6	0.5652	0.0008
0.7	0.5646	0.0
0.8	0.0	0.0

5. 결론 및 향후 연구

본 논문에서는 침입탐지를 위한 척도선정 기법과 공격탐지 기법을 제시한다. 테스트 데이터로 DARPA 1998 덤프 데이터를 가공한 네트워크 세션 기반인 KDD CUP 99 데이터를 사용하였다. KDD CUP 99 데이터의 정상과 22가지 각 공격의 41가지 척도에 대한 확률 분포를 구하고, 상대 복잡도를 통해 정상과 각 공격의 특징을 알 수 있는 유용한 척도를 선정한 후, 우도비 검증을 이용해 임계값에 의한 탐지 실험을 실행하였고, 실험 대조군으로 결정트리 알고리즘 중 C4.5를 이용한 척도 선정과 탐지 실험도 병행되었다. 통계적인 기법과 C4.5에 의한 탐지 결과, 두 기법 모두 높은 탐지율과 낮은 오탐율이 나타남을 알 수 있었다. 하지만 두 결과를 비교했을 때, 통계적인 기법은 거리에 따라 각 공격별로 중요한 척도를 다르게 선정할 수 있었지만, C4.5는 각 공격에 대해 척도를 선정할 수 없어 공통된 척도를 선택하였다. 그리고 통계적인 기법의 탐지는 임계값을 조정함으로써 탐지율과 오탐율을 조절할 수 있었지만, C4.5는 생성된 규칙에 의한 탐지만을 할 수 있었다. 본 논문에서 제시한 결과로써 제시한 기법이 유용함을 알 수 있다.

향후에는 오프라인이 아닌 실세계의 네트워크에 이 기법들을 적용해서 탐지 실험을 실행해야겠고, 많은 종류의 공격 패턴을 생성하기 위해, 폭넓은 공격 데이터 확보가 우선 필요하다. 또한 비정상행위 탐지와 UDP, ICMP 프로토콜에 대한 통계적 기법의 실험이 필요하다.

참 고 문 헌

[1] D. E. Denning, "An Intrusion-Detection Model," IEEE Trans. on Software Engineering, No.2, Feb., 1987.

[2] The third international Knowledge discovery and data mining tools competition dataset KDD99 CUP, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 1998.

[3] Smaha, Stephen E., "Haystack: An Intrusion Detection System," Proceedings of the Fourth Aerospace Computer Security Applications Conference, 1988.

[4] S. Mukkamala and A. Sung, "Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques," Intl. of Digital Evidence. Vol. 1., 2003.

[5] E. Eskin, A. Arnold, M, Prerau and L. Portnoy, "A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data," Application of Data Mining in Computer Security, Kluwer., 2002.

[6] Y. Liao and R. Vemuri, "Using Text Categorization Techiques for Intrusion Detection," the 11th USENIX Security Symposium, 2002.

[7] Richard P.Lippmann and David J. Freid etc., "Evaluating Intrusion Detection System:The 1998 DARPA off-line Intrusion Detection Evalution,"

[8] W. Lee and D. Xiang, "Information-Theoretic Measures for Anomaly Detection," IEEE Symposium on Security and Privacy, 2001.

[9] R. O. Duda, P. E. Hart and D. G. Stork, Pattern Classification 2nd edition, Wiley-INTERSCIENCE., 2001.

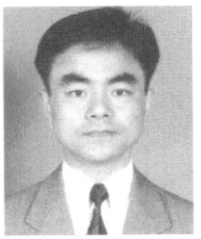
[10] 진성해, "네트워크 침입 탐지를 위한 변형된 통계적 학습 모형," 정보처리학회논문지C, 2003.

[11] J.Ross Quinlan, C4.5 : Programs for Machine Learing, Morgan Kaufmann Publishers.

문 길 종

e-mail : alcor@lsrc.chonnam.ac.kr
2004년 전남대학교 컴퓨터정보학부(이학사)
2004년~현재 전남대학교 정보보호협동과정 석사과정
관심분야 : 네트워크 보안, 침입탐지, 데이터 마이닝 등

김 용 민



e-mail : bluearain@yosu.ac.kr
1989년 전남대학교 전산통계학과(이학사)
1991년 전남대학교 전산통계학과(이학석사)
2002년 전남대학교 전산통계학과(이학박사)
2003년~2004년 전남대학교 리눅스시스템 보안연구센터 Post-doc.
2004년~현재 여수대학교 정보기술학부 전임강사
관심분야 : 시스템 및 네트워크 보안, 전자상거래보안 등

김 동 국

e-mail : dkim@chonnam.ac.kr
1989년 전남대학교 전자공학과(학사)
1991년 포항공과대학 전자전기공학과(석사)
2003년 서울대학교 전기컴퓨터공학부(박사)
1991년~1993년 삼성전자 정보통신연구원
1993년~1999년 삼성종합기술원 전문연구원
2003년~2004년 한국전자통신연구원 선임연구원
2004년~현재 전남대학교 전자컴퓨터정보통신공학부 전임강사
관심분야 : 음성인식, 패턴인식, 침입탐지, 기계학습, 통계적신호처리

노 봉 남

e-mail : bongnam@chonnam.ac.kr
1978년 전남대학교 수학교육과(학사)
1982년 KAIST 전산과(석사)
1994년 전북대학교 전산과(박사)
1983년~현재 전남대학교 전자컴퓨터정보통신공학부 교수
2000년~2003년 리눅스시0스템보안연구센터 소장
2004년~현재 시스템보안연구센터 소장
관심분야 : 컴퓨터와 네트워크 보안, 정보보호시스템, 전자상거래 보안, 사이버사회와 윤리