논문 16-41-02-18 The Journal of Korean Institute of Communications and Information Sciences '16-02 Vol.41 No.02
http://dx.doi.org/10.7840/kics.2016.41.2.277

K-평균 클러스터링을 이용한 네트워크 유해트래픽 탐지

신 동 혁•, 안 광 규*, 최 성 춘**, 최 형 기°

Malicious Traffic Detection Using K-means

Dong Hyuk Shin•, Kwang Kue An*, Sung Chune Choi**, Hyoung-Kee Choi°

요 약

인터넷 서비스의 질을 떨어뜨리고 온라인 범죄를 유발시키는 네트워크 공격들은 오늘날 현대 사회에서 해결해야 될 문제 중 하나이다. 이러한 문제 해결을 위해 시그니처 IDS(Intrusion Detection System)라는 침입 탐지 시스템이 개발되었지만 이들은 기존에 알려진 유형의 공격만 탐지해 낸다. 결과적으로 알려지지 않은 공격들에 대해서는 탐지하지 못하기 때문에 네트워크 공격 탐지를 위한 근본적인 해결책이라 할 수 없다. 본 논문에서는 시그니처 IDS의 단점을 보완하고자 K-평균 알고리즘 기반의 네트워크 유해트래픽 탐지 방법을 제안한다.

Key Words : IDS, K-means, DDoS, Witty Worm, Slammer Worm

ABSTRACT

Various network attacks such as DDoS(Distributed Denial of service) and orm are one of the biggest problems in the modern society. These attacks reduce the quality of internet service and caused the cyber crime. To solve the above problem, signature based IDS(Intrusion Detection System) has been developed by network vendors. It has a high detection rate by using database of previous attack signatures or known malicious traffic pattern. However, signature based IDS have the fatal weakness that the new types of attacks can not be detected. The reason is signature depend on previous attack signatures. In this paper, we propose a k-means clustering based malicious traffic detection method to complement the problem of signature IDS. In order to demonstrate efficiency of the proposed method, we apply the bayesian theorem.

Ⅰ. 서 론

최근 네트워크 공격 패턴의 변화로 인해 Snort, Bro, Suricata와 같은 시그니처 기반 IDS(Intrusion Detection System)로도 탐지 할 수 없는 유해 트래픽들이 생겨나고있다[1-5]. 시그니처 기반 유해 트래픽 탐지 방법 같은 경우에는 과거 발생하였던 공격에 대한 트래픽 분석을 통해 패턴을 찾아내고 이를 시그니처로 저장하여 유해트래픽을 탐지하는 방법이기에 새로운 유형의 공격에는 탐지 불가능하다는 치명적인 문제가 존재한다. 따라서 위와 같은 시그니처 기반 유해트래픽 탐지 방법의 문제점을 해결하기 위한 새로운 탐지법이 필요하다. 이러한 이유로 최근에는 주성분 분석(Principal Components Analysis) 시계열 예측 기법(Time Series Prediction), 서포트 벡터 머신(Support Vector Machine), 클러스터링(Clustering) 등 마이닝 알고리즘을 활용한 유해트래픽 탐지 방법이 제안 되고 있다[6-9]. 각각의 알고리즘들은 네트워크 환경에서

※ 본 연구는 중소 기업청 기술혁신개발사업의 연구 결과로 수행되었음(2014-0841-000)
• First Author : College of Information and Communication Engineering, Sungkyunkwan Univ, dhshin@hit.skku.edu, 학생회원
° Corresponding Author : College of Information and Communication Engineering, Sungkyunkwan Univ, hkchoi@hit.skku.edu, 정회원
* Business Development Engineer at ELUON, Korea, loriket@eluon.com
** Business Development Engineer at ELUON, Korea, choisc@eluon.com
논문번호 : KICS2015-10-350, Received October 31, 2015; Revised January 13, 2016; Accepted January 13, 2016

이상 현상을 탐지할 수 있는 데이터들의 통계치 분석을 통해 공격을 탐지한다. 제한된 알고리즘 모두 시그니처에 의지하지 않고 유해트래픽을 탐지 할 수 있기에 IDS보다 DDoS(Distributed Denial of service)나 웜(Worm) 유형의 공격에 대해 높은 탐지율을 가진다. 하지만 위와 같은 탐지 방법에도 문제점이 존재한다. 단일 유형의 공격에 대해서만 높은 탐지율을 가짐으로 다양한 공격이 발생하는 네트워크 환경에서 적합한 방법이라 할 수 없다. 따라서 본 논문에서는 DDoS와 웜 두 가지 유형의 공격 모두 높은 확률로 탐지 해낼 수 있는 K-평균 알고리즘 기반의 유해트래픽 탐지 기술을 제안한다.

본 논문의 Ⅱ장에서는 기존에 존재하는 유해트래픽 탐지 기법과 관련연구에 대해 소개하고 Ⅲ장에서는 제안하는 유해트래픽 탐지 방법에 대해 설명한다. Ⅳ장에서는 실험에 사용된 데이터들에 대한 간략한 설명과 트래픽 분석에 대해 설명하고 Ⅴ장에서는 실험 결과에 대해 소개한다. 마지막으로 Ⅵ장에서는 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

알고리즘 기반의 유해트래픽 탐지 방법에는 주성분 분석, 서포트 벡터 머신, 시계열 예측 기법, 클러스터링 등이 대표적으로 사용되고 있다[6-9].

주성분 분석은 고차원의 데이터를 저차원의 데이터로 낮추는 차원 축소 방법이다. 네트워크 플로우 내에서 유해 트래픽 특성을 나타낼 만한 파라미터(Parameter)를 주성분으로 선정하여 이를 기준으로 차원을 축소해 나가면서 유해 트래픽을 탐지한다. 주성분 분석을 이용한 네트워크 유해트래픽 탐지 방법은 A. Lakhina에 의해 처음으로 제안 되었다[10]. A. Lakhina는 수 많은 링크로부터 수집된 OD(Origin-Destination) 플로우의 바이트 양을 주성분으로 설정하여 유해트래픽 탐지를 수행 하였다. 위와 같은 탐지 방법은 주성분에 따라 탐지율 변화가 크기 때문에 파라미터 선정이 중요시 여겨진다. 이와 관련하여 주성분 파라미터가 주성분 분석 기법의 탐지율 변화에 얼마만큼 영향을 미치는지 비교 분석한 연구[11]가 있다.

한편, 서포트 벡터 머신은 주어진 데이터를 두 개의 그룹으로 분류하는 이진 분류법으로 경계선을 기준으로 정상 트래픽과 유해 트래픽을 탐지하는 방법이다. 경계선은 서포트 벡터라 불리는 데이터에 의해 결정된다. 이 기법은 경계선에 따라 탐지율 변화가 크기 때문에 경계선 선택 문제가 존재한다. 경계선 문제를 해결하기 위해 계층적 클러스터링(Hierarchical Clustering)이라는 서포트 벡터 그룹화 방식을 사용한 연구[12]와 서포트 벡터 머신 훈련 과정에서 발생하는 시간 복잡도 문제를 해결하기 위해 유전 알고리즘(Generic Algorithm) 사용을 제안한 연구[13] 등이 있다.

시계열 예측기법은 과거시점에서 관찰된 값들을 기반으로 미래시점에 값을 예측하는 방법이다. 과거에 유입된 트래픽의 양 또는 패킷수의 변화 추세를 분석하여 예측값을 설정한 뒤 실제 측정값과 비교하여 편차를 계산한다. 만일 편차가 일정 범위 내에서 지속적으로 유지될 경우 유해 트래픽으로 분류할 수 있다. 시계열 예측 기법 중 하나인 홀트 윈터(Holt-Winter)를 사용하여 유해트래픽을 탐지한 연구[14]가 있다.

클러스터링 알고리즘은 데이터들의 유사성을 비교하여 비슷한 속성을 가지는 데이터들을 하나의 그룹으로 묶는 기법이다. 클러스터링 방법은 비 계층적 클러스터링(Non hierarchical)과 계층적 클러스터링(Hierarchical)으로 나뉜다. 비 계층적 클러스터링은 분할 영역 K개를 지정하여 데이터를 분할하는 방법이다. K개의 그룹에는 K개만큼의 중심점이 존재하며 이 중심점들과 데이터들 사이의 거리를 계산해 데이터들을 분류한다. 한편 계층적 클러스터링은 각 데이터를 하나의 클러스터로 설정한 다음 데이터들 간에 거리를 계산하여 인접한 위치에 존재하는 데이터들끼리 그룹을 형성하는 방법이다. 비 계층적 알고리즘 유해트래픽 탐지방법을 제안한 연구[15]와 계층적 클러스터링를 이용하여 유해트래픽 탐지한 연구[16] 등이 존재한다. 하지만, 기존 연구들에서는 특정한 단일 유형의 공격을 탐지하는 연구들이 대부분이며, 둘 이상의 공격 유형을 동시에 탐지하며 높은 탐지율을 보이는 연구는 부족한 실정이다.

Ⅲ. K-평균 알고리즘 기반 유해트래픽 탐지

K-평균 알고리즘은 비 계층적 클러스터링 방법에서 자주 사용되는 알고리즘으로 데이터의 유사도를 이용하여 그룹을 분류한다. 데이터의 유사도는 N차원 공간에서 데이터들 간의 거리 값으로 표현될 수 있다. 예를 들어 N차원 공간에서 주어진 데이터가 m개라고 한다면 데이터들은 사전에 정해진 K값만큼의 그룹을 형성한다. K개의 그룹은 각각의 중심점을 가지며 이들은 m개의 데이터들과 자신과의 거리 값을 계산해 데이터들을 자신의 그룹에 포함 시킨다. 데이터가 그룹에 포함되는 원리는 각 중심점과 데이터간의 거리 차가 가장 최소인 중심점의 그룹에 데이터가 할당되

는 방식을 사용한다. 이런 K-평균 알고리즘을 사용하여 유해트래픽을 탐지하는 방법에 있어서 가장 중요한 점은 바로 축 설정이다. 축 설정에 따라 탐지율 변화가 크고 네트워크 공격 유형마다 탐지 가능한 축이 서로 다르기 때문에 다양한 공격을 탐지할 수 있는 공통된 축을 찾는 것은 쉽지 않다. 본 연구에서는 기존 연구에서 유해트래픽 탐지를 위해 사용되었던 파라미터 표 1을 토대로 K-평균 알고리즘에 적용 가능한 새로운 파라미터 표 2를 도출하였다. 표 2에 분류된 파라미터들 중 유해트래픽 탐지에 최적화 된 축을 선별해 내기 위해 임의의 조합으로 실험을 수행하였다. 그 결과, 1초간에 유입된 전체 패킷의 수, 바이트 양, 서로 다른 소스 IP 주소 & 동일한 목적지 IP 주소 쌍을 축으로 사용할 경우 가장 높은 탐지율을 가진다는 사실을 확인했다. 축 설정에 따른 탐지율 차이에 대해서는 V장에서 설명하도록 한다. 유해트래픽 탐지 실험을 위한 K-평균 알고리즘의 수행 절차는 아래와 같이 5단계에 걸쳐 진행된다.

1) 주어진 m개의 데이터들을 그룹으로 분할하기 위해 K값을 설정한다.
2) 생성된 K개 그룹의 초기 중심점을 설정한다.
3) 그룹의 중심점과 데이터 사이에 거리를 계산하여 최소 거리를 가지는 그룹에 데이터를 할당한다.
4) 각 클러스터에 할당된 데이터들의 평균 거리를 계산하여 새로운 중심점을 할당한다.
5) 과정 3,4)를 반복 수행한다. 만약 이전 단계에서 생성된 그룹과 차이가 없을 경우에는 알고리즘을 종료한다.

표 1. 유해트래픽 탐지를 위해 사용된 파라미터 분류
Table 1. Classification for Malicious Traffic Detection

Classification	DoS	DDoS	Worm	Ref
Average of Packet Per Flow	O	O		[17]
Average of Bytes Per Flow	O	O		[17]
Percentage of Pair-flows	O	O		[17]
Given Port Total Number of Packet	O			[15]
Given Port total Number of Byte	O			[15]
Given Port Number of Different Src-Dst Pairs	O			[15]
Src Port	O	O		[18] [19]
Dst Port	O	O		[18] [19]
Protocol Type	O			[18]

그림 1은 K-평균 알고리즘이 수행되는 예를 보이고 있다. 2차원 좌표 공간 위에 6개의 입력 데이터들이 존재하고 초록색과 파란색 중심점이 랜덤하게 선택된다. 중심점들을 제외한 나머지 4개의 데이터들은 2개의 중심점과의 거리를 계산하여 자신과의 거리차가 더 작은 중심점과 그룹을 형성하게 된다. 형성된 그룹은 그룹 내 데이터들 간 평균거리를 계산하여 새로운 중심점을 선정한다. 새롭게 선정된 중심점은 다시 나머지 데이터들과의 거리 값을 계산하여 그룹을

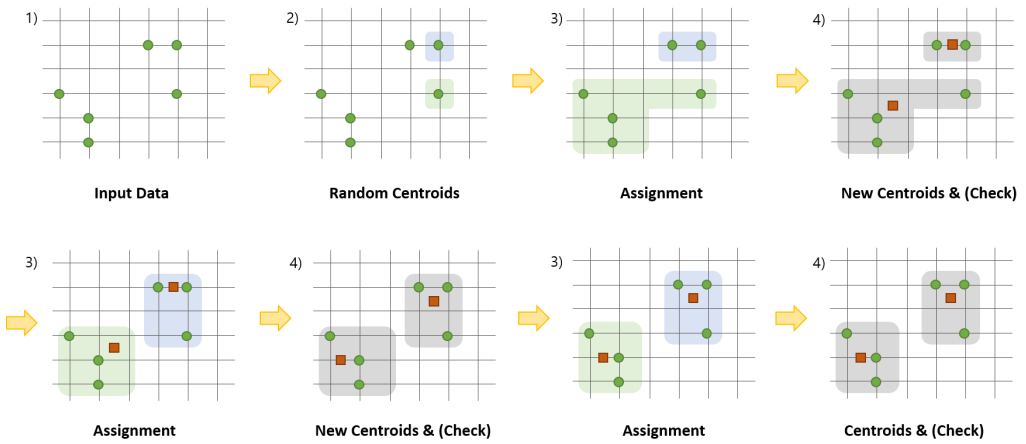

그림 1. K-평균 알고리즘 수행 과정
Fig. 1. K-means Algorithm Procedure

표 2. K-평균 알고리즘에 적용 가능한 파라미터 분류
Table 2. Selected Parameters in the K-means

	Classification	DoS	DDoS	Worm
1	Different Src IP & Same Dst IP Pair Number	O	O	O
2	Same Src, Dst IP Pair Number	O		
3	Same Src IP & Difference Dst IP Pair Number	O		
4	Different Src Port & Same Dst Port Pair Number		O	O
5	Same Src, Dst Port Pair Number	O		O
6	Total Packet Byte	O	O	O
7	Total Packet Number	O	O	O
8	IP Scan Speed			O
9	SYN Number	O	O	

재형성하는 과정을 반복 수행한다.

Ⅳ. 네트워크 트래픽 데이터 셋 분석

제안하는 기법의 효율성을 입증하기 위해 Caida[20]에서 제공한 DDoS 데이터 셋과 MAWI Working Group[21]에서 제공한 위티 웜(Witty Worm) 데이터 셋을 이용하여 테스트를 수행하였다. Caida DDoS 데이터 셋은 ICMP Ping Flooding 공격으로 특정 시간 이후로 최소 200Kbits/s에서 최대 80Mbits/s로 ICMP 에코 리퀘스트 패킷을 전송한다. 그림 2와 그림 3을 보면 ICMP 패킷수와 바이트 양이 급격하게 변하는 구간을 확인할 수 있다. 한편 MAWI Working Group에서 제공한 위티 웜 데이터 셋은 UDP Port 4000번을 이용하여 709~1,321 바이트 크기의 UDP 패킷을

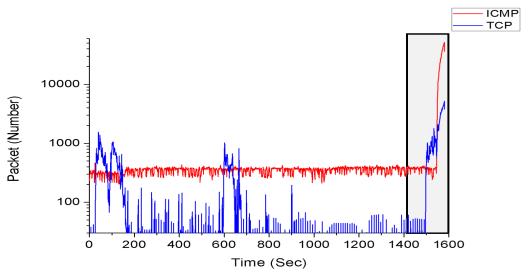

그림 2. 초 당 전송된 DDoS 데이터 패킷 수
Fig. 2. Total Number of DDoS Packet (Per Second)

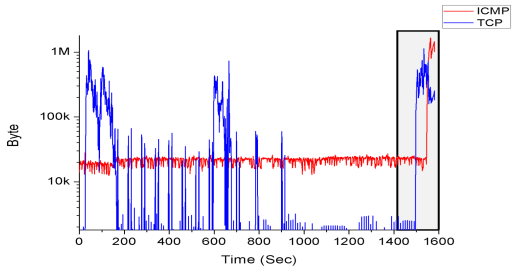

그림 3. 초 당 전송된 DDoS 데이터 바이트 양
Fig. 3. Total Number of DDoS Packet Bytes (Per Second)

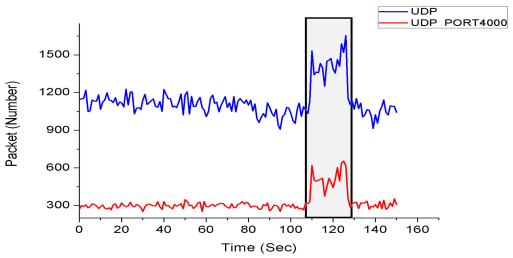

그림 4. 초 당 전송된 위티 웜 데이터 패킷 수
Fig. 4. The Number of Witty Worm Packet (Per Second)

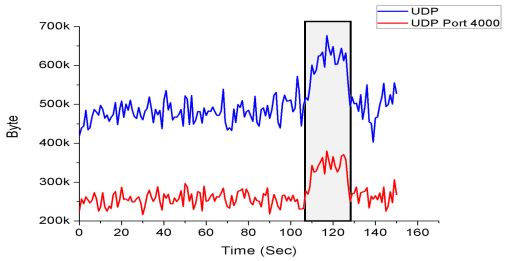

그림 5. 초 당 전송된 위티 웜 데이터 바이트 양
Fig. 5. Total Number of Witty Worm Bytes (Per Second)

전송하는 공격으로 그림 4와 그림 5를 통해 패킷수와 바이트 양의 변화를 확인 할 수 있다.

Ⅴ. 성능 분석 및 평가

각각의 데이터 셋은 Ⅲ절에서 언급한 시간 간격과 축 기준에 따라 3차원 공간에서 한 개의 점으로 표현되었다. 실험결과 내에서 빨간색 점과 파란색 점이 정상트래픽과 유해트래픽을 나타낸다. DDoS 데이터 셋은 3차원 공간에서 총 1,581개의 점으로 표현 되었으며 이 중 정상 1,547개, 공격 34개를 포함한다. 반면 위티 웜 데이터 셋은 총 151개의 점 중 정상 133개, 공격 18개를 포함한다. 데이터 셋에 대한 테스트 결과

는 그림 6부터 그림 9과 같다. 그림 6과 그림 7에서는 1초간에 유입된 전체 패킷의 수, 바이트 양, 서로 다른 소스 IP 주소 & 동일한 목적지 IP 주소 쌍을 축으로 사용한 결과를 나타낸다. 그림 6에서 원으로 표시된 영역을 보면 정상인 트래픽과 유해트래픽이 인접하여 몰려 있는 것을 확인할 수 있다. 이런 현상이 발생하는 이유는 DDoS 공격의 패킷수가 급격히 증가하기 전 정상 패킷의 수가 갑작스럽게 증가했기 때문이다. 실제로 영역 내에 찍힌 점들의 출력 결과를 확인해 본 결과 정상트래픽을 유해트래픽으로 판단한 갯수가 34개 존재한다는 사실을 알 수 있었다. 한편 그림 7에서는 정상트래픽과 유해트래픽이 뚜렷이 식별되는 것을 확인 할 수 있다. 그림 6의 결과와 차이가 나는 이유는 웜 공격 같은 경우 공격이 시작되는 순간 정상트래픽에 비해 바이트 양이 급격하게 증가 하는 것이 확연히 드러나기 때문이다. 앞서 분석한 그림 5를 통해 UDP Port 4000번으로 전송되는 패킷 바이트 양이 증가할 때 UDP 프로토콜을 사용하는 패킷의 바이트 수가 급격하게 증가되는 것을 확인 할 수 있다. 그림 7에서는 정상 트래픽을 유해트래픽으로 식별한 경우가 1개 밖에 존재하지 않았다는 것을 출력결과를 통해 확인하였다.

그림 8과 그림 9는 Y축을 서로 다른 소스 Port & 동일한 목적지 Port 쌍의 수로 변환한 출력결과를 나타낸다. Y축을 변환한 이유는 DDoS나 웜 같은 공격이 일반적으로 타겟 PC의 특정 Port에서 발생하는 과거 사례를 확인하였기 때문이다. 그림 8의 결과를 보면 그림 6과는 다르게 정상트래픽과 유해트래픽 구간이 확실하게 나눠진 것을 확인 할 수 있다. 그러나 출력 결과를 확인해 본 결과 탐지율이 더 떨어지는 것을 확인했다. 그 이유는 유해트래픽을 정상 트래픽으로

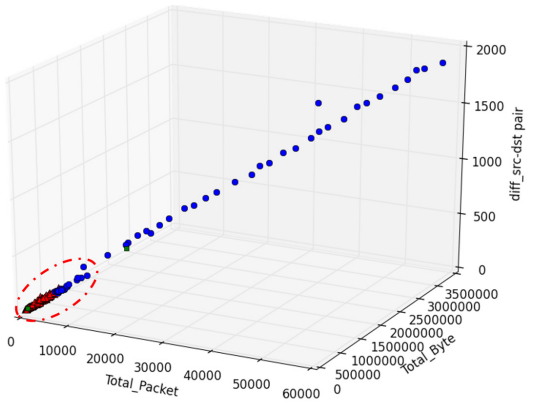

그림 6. 표 2의 파라미터 1,6,7을 이용한 DDoS 공격 탐지
Fig. 6. DDoS Detection Using Parameter 1,6,7 in Table 2

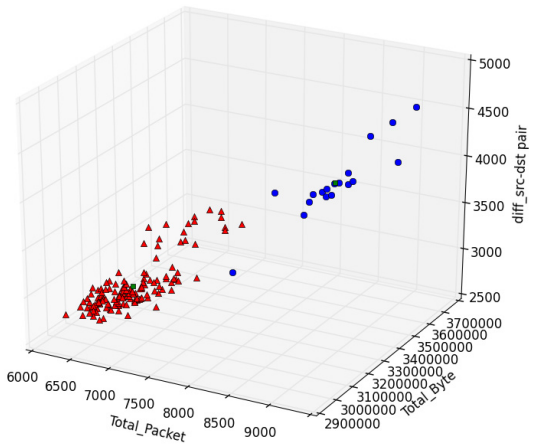

그림 7. 표 2의 파라미터 1,6,7을 이용한 위티 웜 공격 탐지
Fig. 7. Witty Worm Detection Using Parameter 1,6,7 in Table 2

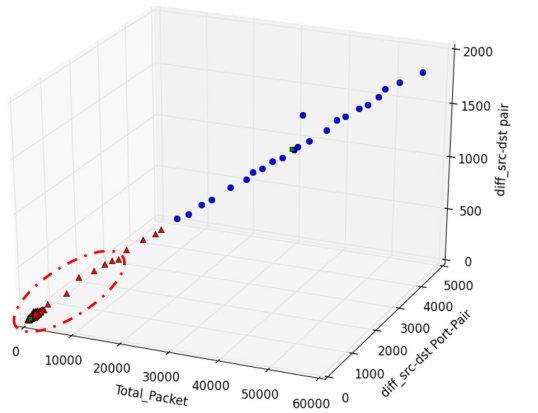

그림 8. 표 2의 파라미터 1,4,6을 이용한 DDoS 공격 탐지
Fig. 8. DDoS Detection Using Parameter 1,4,6 in Table 2

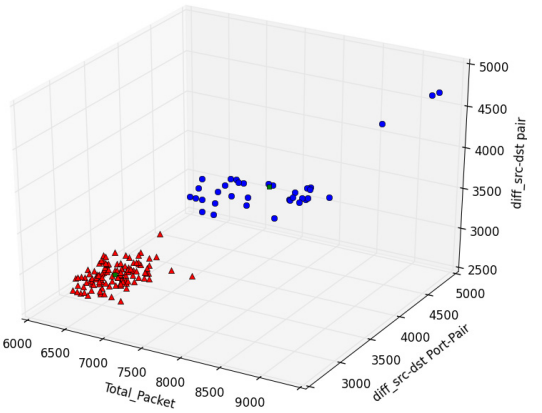

그림 9. 표 2의 파리미터 1,4,6을 이용한 위티 웜 공격 탐지
Fig. 9. Witty Worm Detection Using Parameter 1,4,6 in Table 2

측정하는 경우가 다소 발생했기 때문이다. 마찬가지로 그림 9에서도 동일한 현상이 발생하는 결과를 확인했다. 실험 결과에 대한 정확도 평가는 베이지안 분석법을 이용하여 검증하였다. 베이지안 분석법은 패턴인식 알고리즘의 성능을 평가하는데 전통적으로 사용되는 방법 중에 하나로 TP(True Positive), FP(False Positive), FN(False Negative), TN(True Negative)으로 구성되어 있으며 각각 TPR(True Positive Rate) 과 FPR(False Positive Rate)을 측정한다. TPR은 유해트래픽을 공격이라고 판단했을 확률 TP와 유해트래픽을 정상이라고 판단했을 확률 FN을 이용하여 계산되며, FPR은 정상트래픽을 정상이라고 판단했을 확률 TN과 정상트래픽을 공격이라고 판단했을 확률 FP를 이용하여 계산된다. 축 설정에 따른 DDoS 공격과 위티 웜 공격에 대한 TPR과 FPR은 표 3과 표 4를 통해 나타내었다.

표 3과 표 4에서와 같이 전체 패킷의 수, 바이트 양, 서로 다른 소스 IP 주소 & 동일한 목적지 IP 주소, 서로 다른 소스 Port & 동일한 목적지 Port 쌍을 축으로 사용할 경우 DDoS 공격과 위티 웜 공격에서 높은 탐지율을 보임을 확인할 수 있었다.

표 3. 그림 6과 그림 7에 대한 결과
Table 3. Result of Figure 6 and Figure 7

	DDoS	Witty Worm
True Positive	33	17
False Positive	34	1
True Negative	1513	132
False Negative	1	1
True Positive Rate	0.97	0.94
False Positive Rate	0.02	0.02

표 4. 그림 8과 그림 9에 대한 결과
Table 4. Result of Figure 8 and Figure 9

	DDoS	Witty Worm
True Positive	23	17
False Positive	0	18
True Negative	1547	115
False Negative	11	1
True Positive Rate	0.67	0.94
False Positive Rate	0.00	0.13

Ⅵ. 결 론

본 연구에서는 K-평균 알고리즘 기반의 네트워크 유해트래픽 탐지 방법에서 DDoS 공격과 위티 웜 공격을 동시에 탐지할 수 있는 파라미터를 도출하였고, 이를 실험을 통해 높은 탐지율을 보인다는 것을 증명하였다. 또한 관련연구에서 제안된 주성분 분석 기법과 서포트 벡터 머신 알고리즘에 비해 계산식이 단순함으로 낮은 시간 복잡도를 가진다는 이점이 존재한다. 이는 실시간 유해트래픽 탐지에 있어서 적합한 알고리즘이라 할 수 있다. 향후 연구로는 슬래머 웜 유해트래픽 탐지에 대한 연구를 진행할 것이다.

References

[1] M. Roesch, "Snort - Lightweight intrusion detection for networks," in *Proc. USENIX LISA 99*, vol. 99, no. 1, Washington, USA, Nov. 1999.

[2] V. Paxon, "Bro: A system for detecting network intruders in real-time," in *Proc. 7th USENIX Security Symp.*, San Antonio, TX, Jan. 1998.

[3] S.-H. Yoon and M.-S. Kim, "Behavior based signature extraction method for internet application traffic identification," *J. KICS*, vol. 38, no. 5, pp. 368-376, May 2013.

[4] K.-S. Shim, S.-H. Yoon, S.-K. Lee, S.-M. Kim, W.-S. Jung, and M.-S. Kim, "Automatic generation of snort content rule for network traffic analysis," *J. KICS,* vol. 40, no. 4, pp. 666-672, Apr. 2015.

[5] W.-S. Jung, J.-S. Park, and M.-S. Kim, "Performance improvement of traffic identification by categorizing signature matching type," *J. KICS*, vol. 40, no. 7, pp. 1339-1346, Jul. 2015.

[6] L. I. Smith, *A tutorials on Principal Components Analysis*, Retrieved Oct., 14, 2015, from http://www.cs.otago.ac.nz.

[7] O. Carugo and F. Eisenhaber, *Data Mining Techniques for the Life Sciences*, Humana Press, vol. 609, 2010.

[8] E. Philippe and C. Agon, "Time series data mining," *ACM Computing Surveys (CSUR)*,

vol 45, no. 12, pp. 1-34, Nov. 2012.

[9] M. E. Celebi, H. A. Kingravi, and P. A. Vela, “A comparative study of efficient initialization methods for the k-means clustering algorithm,” *J. Elsevier*, vol. 40, no. 1, pp. 200-210, Jan. 2013.

[10] A. Lakhina, M. Crovella, and C. Diot, “Diagnosing network-wide traffic anomalies,” *SIGCOMM ’04*, pp. 219-230, Portland, USA, Aug. 2004.

[11] H. Ringberg, A. Soule, J. Rexford, and C. Diot, “Sensitivity of PCA for traffic anomaly detection,” *SIGMETRICS ’07*, pp. 109-120, San Diego, USA, Jun. 2007.

[12] L. Khan, M. Awad, and B. Thuraisingham, “A new intrusion detection system using support vector machines and hierarchical clustering,” *J. VLDB*, vol. 16, no.4, pp. 507-521, Oct. 2007.

[13] T. Shon, Y. Kim, C. Lee, and J. Moon, “A machine learning framework for network anomaly detection using SVM and Ga,” *IAW ’05*, pp. 176-183, New York, USA, Jun. 2005.

[14] J. D. Brutlag, “Aberrant behavior detection in time series for network monitoring,” in *Proc. LISA*, vol. 14, pp. 139-146, New Orleans, USA, Dec. 2000.

[15] G. Münz, S. Li, and G. Carle, “Traffic anomaly detection using k-means clustering,” GI/ITG Workshop MMBnet 2007, Hamburg, Germany, Sept. 2007.

[16] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, “DDoS attack detection method using cluster analysis,” *J. Elsevier*, vol. 34, no. 3, pp. 1659-1665, Apr. 2008.

[17] R. Braga, E. Mota, and A. Passito, “Lightweight DDoS flooding attack detection using NOX/OpenFlow,” *2010 IEEE LCN*, pp. 408-415, Denver, CO, Oct. 2015.

[18] G. R. Zargar and P. Kabiri, “Advances in data mining: Applications and theoretical aspects,” in *Proc. 10th Ind. Conf., ICDM 2010*, Berlin, Germany, Jul. 2010.

[19] F. Silveira, C. Diot, N. Taft, and R. Govindan, “ASTUTE: Detecting a different class of traffic anomalies,” in *Proc. ACM SIGCOMM ’10*, pp. 267-278, New Delhi, India, Aug. 2010.

[20] http://data.caida.org

[21] http://mawi.nezu.wide.ad.jp

신 동 혁 (Dong Hyuk Shin)

2014년 2월 : 조선대학교 컴퓨터공학과 졸업
2014년 2월~현재 : 성균관대학교 전자전기 컴퓨터공학과 석사 과정
<관심분야> 네트워크 보안, SDN, 리버싱 엔지니어링

안 광 규 (Kwang Kue An)

2014년 2월 : 아주대학교 지식정보보안학과 석사
2014년 3월~현재 : 이루온 사업개발부 대리
<관심분야> 가상화, 정보보호, 네트워크

최 성 춘 (Sung Chune Choi)

2011년 8월 : 성균관대학교 컴퓨터공학과 박사
2012년 10월~현재 : 이루온 사업개발부 차장
<관심분야> 가상화, 정보보호, 네트워크

최 형 기 (Hyoung-Kee Choi)

1992년 2월 : 성균관대학교 전자공학과 졸업
1996년 2월 : Polytechnic University in Brooklyn, NY 석사
2001년 2월 : Georgia Institute of Technology in Atlanta, GA 박사
2001년~2004년 : Lanscope 근무
2004년 3월~현재 : 성균관대학교 정보통신대학 부교수
<관심분야> 네트워크보안, 리버싱 엔지니어링