http://dx.doi.org/10.7840/kics.2016.41.12.1

네트워크 트래픽 분석을 이용한 연쇄적 사이버공격 트래픽의 발생원 추적 방법

구 영 훈◆, 최 선 오*, 이 수 강*, 김 성 민**, 김 명 섭°

A Method for Tracking the Source of Cascading Cyber Attack Traffic Using Network Traffic Analysis

Young-Hoon Goo◆, Sun-Oh Choi*, Su-Kang Lee*, Sung-Min Kim**, Myung-Sup Kim°

요 약

오늘날 인터넷으로 연결된 세상은 그물망처럼 정교해지고 있으며 이러한 환경은 사이버 테러범으로 불리는 사이버 공격자들에게 더없이 좋은 공격 환경을 제공해 주고 있다. 이에 따라 사이버 공격 횟수는 매년 크게 증가하고 있으며 네트워크 모니터링 분야에서는 악성행위 및 사이버 공격트래픽을 찾아내려는 많은 연구들이 이루어지고 있다. 하지만 사이버 공격트래픽은 매 공격마다 알려지지 않는 새로운 형태의 트래픽이 발생하며 이는 사이버 공격트래픽 탐지를 어렵게 한다. 본 논문에서는 트래픽 데이터를 구성하는 플로우 정보 사이의 연관 관계를 정의하고, 연관성이 높은 플로우를 연쇄적으로 그룹화 하여 사이버 공격트래픽의 발생원을 추적하는 방법을 제안한다. 본 논문에서 제안한 사이버 공격트래픽 발생원 추적방법을 실제로 발생했던 사이버 공격 트래픽에 적용한 결과 신뢰할 만한 수준의 결과를 얻을 수 있었다.

Key Words : Traffic Analysis, APT Traffic Analysis, APT Atack Tracking, Cascade Grouping, Network Management

ABSTRACT

In these days, the world is getting connected to the internet like a sophisticated net, such an environment gives a suitable environment for cyber attackers, so-called cyber-terrorists. As a result, a number of cyber attacks has significantly increased and researches to find cyber attack traffics in the field of network monitoring has also been proceeding. But cyber attack traffics have been appearing in new forms in every attack making it harder to monitor. This paper suggests a method of tracking down cyber attack traffic sources by defining relational information flow of traffic data from highest cascaded and grouped relational flow. The result of applying this cyber attack source tracking method to real cyber attack traffic, was found to be reliable with quality results.

※ 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원(No.B0101-16-0300) 및 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원(No.2015R1D1A3A01018057)을 받아 수행된 기초연구사업임.
◆ First Author : Korea University Department of Computer and Information Science, gyh0808@korea.ac.kr, 학생회원
° Corresponding Author : Korea University Department of Computer and Information Science, tmskim@korea.ac.kr, 종신회원
* Network Security Research Section, Cyber Security Research Laboratory, ETRI. suno@etri.re.kr
** Korea University Department of Computer and Information Science, {sukanglee, gogumiking}@korea.ac.kr, 학생회원
논문번호 : KICS2016-03-043, Received December 22, 2016; Revised December 22, 2016; Accepted December 22, 2016

Ⅰ. 서 론

오늘날 인터넷으로 연결된 세상은 그물망처럼 정교해지고 있으며 이러한 환경은 사이버 테러범으로 불리는 사이버 공격자들에게 더없이 좋은 공격 환경을 제공해주고 있다. 이러한 환경적 요인은 사이버 공격이 급격히 증가하게 된 원인중 하나이며 사이버 악성행위 및 공격트래픽 탐지는 업계와 학계에서 많은 요구사항을 받고 있다. 2016년 보안 동향 보고서[1]에서는 전 세계적으로 보안 사고는 2014년 245건으로 2010년 대비 600% 증가, 보안취약점은 2010년 18건에서 2014년 159건으로 800% 증가한 것으로 나타났다. 국내에서는 대표적인 사례로 2015년 한국수력원자력 해킹 공격으로 원전 관련 설계 도면이 유출되었으며, 한국 철도공사 네트워크 망 구성도등 주요 정보통신 기반시설 공문서가 유출된 사례가 있다. 이와 같이 현실 세계에 직접 영향을 끼칠 수 있는 보안 사고들을 사전에 방지하고, 보안사고 발생 시 신속한 사고 처리, 복구를 위한 많은 연구들이 이루어지고 있다.

네트워크 보안 분야에서는 악성행위 탐지를 위해 IDS/IPS 기반의 실시간 탐지 방법과 네트워크에서 발생한 패킷을 일정 기간 동안 저장하고, 보안 사고가 발생했을 때 과거에 저장해둔 패킷을 재검사(Retroactive)하는 방법이 연구되고 있다. 첫 번째 방법인 IDS/IPS 기반 실시간 악성행위 탐지 방법은 악성행위 검출 규칙을 적용하는 시점부터 보안위협에 대응할 수 있으며, 악성행위 검출 규칙을 적용하기 전 발생할 수 있는 보안 위협에 대해서는 대처가 불가능하므로 IDS/IPS 기반의 실시간 악성행위 탐지 방법은 보안 공백 기간이 발생할 수 있으며, 이에 따른 보안 사고가 일어날 수 있다. 따라서 이러한 보안 공백 기간을 최소화시키기 위한 방법으로 보안 사고가 발생했을 때 과거에 저장해둔 패킷을 재검사하여 보안 사고를 검출하고 대응하는 방법이 있다. 이 방법은 보안 사고가 발생 했을 때 최단 시간 내에 공격자의 트래픽을 분류하고, 공격자의 공격 형태와 위치 등을 분석하여 사이버 공격트래픽의 검출 규칙을 생성하기 위한 방법이다. 검출 규칙을 생성하기 위해서는 먼저 트래픽을 여러 속성정보를 이용하여 분석해야 한다.

본 논문에서는 네트워크 트래픽의 플로우 헤더정보(IP, Port, Protocol)와 통계정보(패킷의 크기, 전송 방향, 발생 시간, 지속 시간 등)를 이용한 발생원 추적방법을 제안하는데, 그 방법은 사이버 공격트래픽이라 의심되는 플로우와 관련 있는 플로우를 연속적으로 그룹화 하여 사이버 공격트래픽들을 추적하는 것이다.

본 논문은 다음과 같이 구성된다. 2장에서는 최근 발생한 사이버공격의 유형과 사이버공격을 탐지하기 위한 트래픽 분류방법에 대하여 살펴본다. 3장에서는 두 플로우 간 연결성(Connectivity)과 유사성(Similarity)을 수치화하기 위해 정의한 FCI(Flow Correlation Index)와 FCI를 이용하여 사이버공격이라 판단되는 플로우를 그룹화, 추적하기 위한 방법론을 설명한다. 4장에서는 본 논문에서 제안하는 방법론의 성능을 입증하기 위해 실제 사이버 공격이 포함된 트래픽 데이터에 사이버공격 추적 방법을 적용한 실험 결과를 기술한다. 마지막으로 5장에서는 결론과 향후 연구 과제를 기술한다.

Ⅱ. 관련 연구

최근 발생한 사이버공격들은 유형별로 크게 2가지로 나눌 수 있다. 하나는 목표로 정한 특정 서버를 대상으로 불법 접속을 시도하는 것이며, 주로 공격 목표가 된 기업이나 정부의 기밀 자료를 탈취하기 위해 공격하는 경우가 많다. 다른 하나는 불특정 다수 서버 또는 개인 PC의 보안 취약점을 악용하는 데이터를 무차별적으로 보내고 보낸 데이터에 반응하는 호스트에 대해 다음 공격을 진행한다. 주로 개인 정보를 빼내어 금전적인 이득을 취하거나 DDoS와 같은 공격을 진행할 목적으로 실행한다. 2008년부터는 웜 바이러스나 멀웨어와 같은 악성코드의 위협은 감소추세에 있으나 DDoS, APT와 같은 공격은 급격히 증가하고 있는 추세이다.

DDoS[2]는 분산 서비스 거부 공격(Distributed Denial of Service)의 약자이며 분산된(Distributed) 다수의 컴퓨터로 특정 서버에 엄청난 트래픽을 유발하고, 네트워크 가용성을 떨어트려 해당 서버의 서비스를 방해하는 공격이다.

그림 1처럼 DDoS Attacker(공격자)는 실제 공격에 사용될 다수의 Agent(좀비 PC)를 확보하기 위해 소스코드 형태의 공격 코드를 유포하여 감염시킨다. 초창

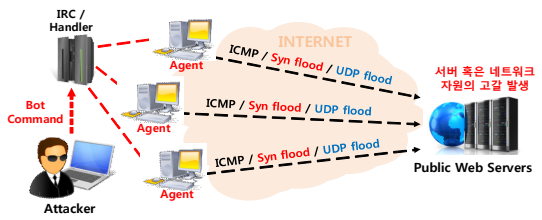


그림 1. 분산 서비스 거부(DDoS) 공격 시나리오
Fig. 1. The scenario of DDoS Attack

기의 DDoS 공격은 Attacker가 IRC 프로토콜을 이용하거나 HTTP나 P2P 프로토콜을 이용하여 공격 명령을 전송하였으나 최근에는 유포한 소스코드 내부에 공격 시간, 공격 대상 등의 정보가 포함되어 있는 경우도 있다. 감염된 Agent들은 타겟 서버에 엄청난 트래픽을 지속적으로 발생시켜 타겟 서버의 네트워크 기능을 마비시킴으로써, 장시간동안 서버의 정상 작동을 방해한다.

APT(Advanced Persistent Threat)[3,4]는 특정 대상을 목표로 다양한 해킹 기술을 이용해 은밀하고 지속적으로 공격하는 행위를 뜻한다. 공격기간은 특정할 수 없지만 길게는 5년까지도 이루어질 수 있으며 공격 목적을 달성하기까지 표적이 알아차릴 수 없도록 각종 방어기술을 우회하는 방법을 사용한다.

APT 공격은 크게 4단계로 진행된다. 첫 번째 조사 단계에서는 타겟에 대한 심층적 스캔을 진행한다. 두 번째 침투 단계에서는 조사 단계에서 획득한 취약점을 악용하여 타겟의 네트워크, 시스템에 침투한다. 세 번째 제어권 획득 단계에서는 타겟의 주요 시스템에 대한 제어권을 획득하게 된다. 마지막 유출단계에서는 기밀자료를 유출하거나 해당 시스템을 파괴하여 최종 공격 목표를 달성한다. APT 공격은 잠복 기간이 길고 매 공격마다 새롭고 다양한 해킹 기술을 사용하기 때문에 공격 패턴을 초기단계에서 공격을 탐지하기 어렵다. 이러한 이유로 공격을 미리 탐지하는 것 보다는 빠른 사고처리 및 대응이 최선이며 이를 위해서는 네트워크의 트래픽 데이터 분석이 필수적이다.

네트워크 트래픽은 패킷 또는 플로우 단위로 구분할 수 있으며, 패킷은 실제 네트워크에서 전송되는 단위로 실제 전송되는 데이터와 데이터의 출발지, 목적지, 프로토콜 정보 등을 포함하고 있는 헤더로 이루어져 있다. 플로우[5]는 다양한 방법으로 정의될 수 있는데 본 연구에서는 패킷의 출발지와 목적지, 포트 번호, 프로토콜이 동일한 정방향, 역방향의 세션 정보를 하나의 양방향 플로우로 정의되며 플로우에는 패킷과 마찬가지로 출발지와 목적지, 프로토콜 정보가 포함되어 있으며, 주고받은 패킷의 수, 크기, 패킷 간 inter-arrival time 등의 정보와 필요에 따라서는 패킷의 데이터(payload)도 포함될 수 있다.

그림 2. APT 공격 단계
Fig. 2. The steps of APT Attack

플로우와 패킷의 정보를 이용하여 다양한 방법으로 트래픽을 분류할 수 있는데 그 방법은 크게 헤더정보 기반 트래픽 분류방법, 통계정보 기반 트래픽 분류 방법, 페이로드 기반 트래픽 분류방법이 있다. 헤더정보 기반 트래픽 분류 방법[5,6]는 특정 응용을 서비스 하는 서버 또는 공격자의 헤더 정보의 5-Tuple(출발지·목적지 IP, 출발지·목적지 Port, 프로토콜)를 시그니쳐로 추출하여 트래픽을 분석한다. 통계정보 기반 트래픽 분류 방법[7,8,9]은 플로우의 통계정보인 패킷 수, 패킷의 크기, 패킷의inter-arrival time 등의 통계적 특징을 시그니쳐로 사용하여 트래픽을 분류한다. 통계정보 기반 트래픽 분류 방법은 응용 및 세부 서비스별 분류와 암호화 트래픽 분석이 가능하다는 장점이 있다. 페이로드 기반 트래픽 분류 방법[10,11]은 플로우에 포함된 패킷의 데이터(payload)에 나타나는 특정 문자열 패턴을 시그니쳐로 사용하여 트래픽을 분류한다. 페이로드 기반 트래픽 분류 방법은 타 분류 방법과 비교하여 분석 정확도가 높고 응용 및 세부 서비스별 분류가 가능한 반면 암호화된 트래픽 분석이 불가능하다.

본 논문에서는 여러 플로우들 간의 연관성을 찾고 이를 그룹화 하여 사이버공격 트래픽의 발생원을 추적하는 방법을 제안한다. 이를 위해 플로우의 헤더정보와 통계정보를 이용하여 플로우들 간의 연관성을 찾는 방법을 제시한다.

Ⅲ. 사이버공격 발생원 추적 방법

본 장에서는 트래픽 분류 방법 중 헤더정보와 통계정보를 이용한 트래픽 분류 방법을 이용하여 트래픽 데이터에 포함된 사이버공격의 발생원을 추적하는 방법을 제안한다.

APT 공격은 시스템에 침투하고 바로 공격을 진행하는 것이 아니라 침투 후 전체 시스템에 대한 전반적인 구조를 파악한 다음 유용한 데이터를 수집하고, 수집한 정보를 유출함과 동시에 해당 시스템의 운영을 방해하거나 장비를 파괴한다. 이처럼 APT 공격은 여러 단계를 거쳐 공격을 실행하게 되며 각 단계별로 발생한 악성 행위는 네트워크 트래픽에 그대로 반영되어 나타나게 된다.

3.1 Seed정보를 이용한 트래픽 그룹화 개요

그림 3에서 표현된 Seed Info는 악성행위에 사용된 트래픽을 추적하기 위한 첫 단서 정보이다. Seed Info에는 시간, 헤더정보(5-Tuple), 문자열 정보가 포함될 수 있다. 전체 트래픽에서 Seed Info와 일치하는 트래

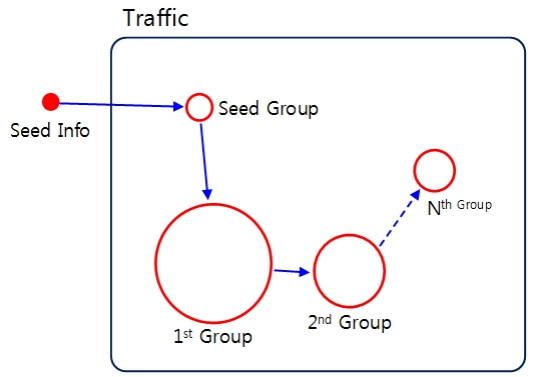


그림 3. Seed 정보를 이용한 트래픽 그룹화 개요
Fig. 3. Overview of traffic grouping method using seed information

픽 집합을 Seed Group으로 그룹화 한다. 즉, Seed Group은 Seed Info와 매칭 되는 플로우의 집합이며 간단한 예를 들면 SeedGroup(SIP=192.168.12.120, "abc")인 경우 출발지 IP 주소가 192.168.12.120이고 페이로드에 "abc" 문자열을 포함하는 플로우의 집합인 것이다.

그림 3은 Seed 정보를 이용한 트래픽 그룹화 과정을 간단하게 도식화한 그림이다. 트래픽 그룹화 과정은 그림 3과 같이 Seed Group으로부터 1st Group, 2nd Group, 더 이상 그룹화 되는 그룹이 없을 Nth Group까지 찾게 되며 이 때 사용되는 값을 FCI(Flow Correlation Index)라고 한다.

FCI는 기준 플로우와 비교 대상 플로우 간 관련성을 계산하기 위한 값으로 세부적으로는 연결성(Connectivity)과 유사성(Similarity)으로 나누어지며, 이를 수치화 한 값이 FCI로 정의된다.

3.2 연결성(Connectivity) 계산 방법

플로우간 연결성(Connectivity)은 해당 플로우의 발생시간(StartTime;st)과 출발지 IP 주소(Source IP Address;sip), 출발지 포트(Source Port;sport), L4 프로토콜(prot), 도착지 IP 주소(Destination IP Address;dip), 도착지 포트(Destination Port;dport) 총 6개의 속성 값을 이용하여 계산된다.

$$Conn(f_x,f_y)=\sum_{i=1}^{6}(w_i\times a_i(f_x,f_y)) \quad (1)$$

식(1)은 플로우 f_x와 플로우 f_y사이의 연결성을 계산하는 수식이다. w는 가중치(weight value)를 나타내며 각 가중치의 합(w_1+w_2+ ... + w_6)은 1을 넘을 수 없다. 사용자는 사이버공격의 종류에 따라 w_i의 값을 변경할 수 있다. a_1, a_2, ..., a_6은 연결성 계산 시 사용하는 6가지 속성 값을 가리킨다.

그림 4는 Seed flow로부터 플로우의 시작시간(a_{st})을 이용하여 그룹화 하는 과정을 표현한 그림이다. 비교 대상 플로우와 기준 플로우의 시작 시간을 계산하여 점선 원으로 표현한 범위(임계값)안에 포함되면 비교 대상 플로우를 그룹화 하는 것이다.

$$a_{st}(f_x,f_y)=1-\sqrt{\frac{dist(f_x,f_y)}{maxdist(F)}} \quad (2)$$

식(2)는 플로우 f_x와 플로우 f_y사이의 시간적 연결성을 계산하는 수식이며 min-max 정규화를 통해 식(2)의 결과 값은 0과 1 사이의 값이 나오게 된다. 식(2)의 $dist(f_x,f_y)$는 두 플로우의 시작시간 차이를 의미한다. $maxdist(F)$는 수집한 트래픽의 전체 플로우들의 시작시간 차이 중 최대값을 의미하며 F는 트래픽의 전체 플로우 집합을 의미한다. 플로우 f_x와 플로우 f_y간의 시작시간 차이가 적을수록 식(2)의 값은 1에 가까운 결과 값이 나오게 된다.

그림 5는 Seed flow로부터 플로우의 IP 주소 쌍(SIP:DIP)을 이용하여 그룹화 하는 과정을 표현한 그림이다. 비교 대상 플로우와 기준 플로우의 IP 주소 쌍을 비교하여 점선 원으로 표현한 범위(임계값) 안에 포함되면 비교 대상 플로우를 그룹화 하는 것이다.

$$a_{ip}(f_x,f_y)=\left(\frac{prefixlen_{src}(f_x,f_y)}{32}\right)^2+\left(\frac{prefixlen_{dst}(f_x,f_y)}{32}\right)^2 \quad (3)$$

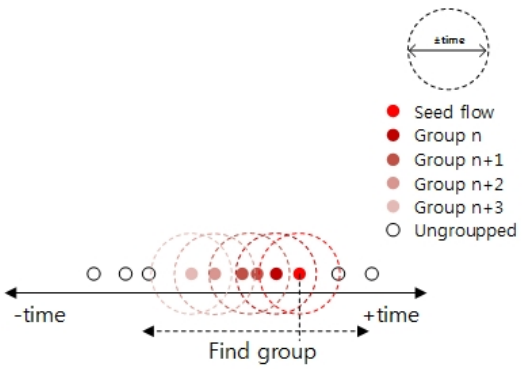


그림 4. 시작시간을 이용한 그룹화 과정
Fig. 4. Grouping process that uses starting time

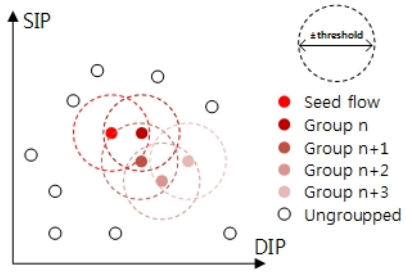


그림 5. IP 주소 쌍을 이용한 그룹화 과정
Fig. 5. Grouping process that uses with IP address pair

식(3)은 플로우 f_x와 플로우 f_y사이의 IP 주소 간 연결성을 계산하는 수식이며 두 플로우의 출발지 주소와 도착지 주소를 비트별로 비교하여 계산한다. 식(3)의 $prefixlen_{src}(f_x,f_y)$는 f_x의 출발지 주소와 f_y의 출발지 주소의 32비트 중 앞부분이 같은 비트의 개수와 f_x의 출발지 주소와 f_y의 도착지 주소의 32비트 중 앞부분의 같은 비트의 개수 중 큰 값을 의미한다. $prefixlen_{dst}(f_x,f_y)$는 반대로 f_x의 도착지 주소와 f_y의 도착지 주소의 32비트 중 앞부분이 같은 비트의 개수와 f_x의 도착지 주소와 f_y의 출발지 주소의 32비트 중 앞부분의 같은 비트의 개수 중 큰 값을 의미한다. 식(3)의 결과 값은 0과 1사이의 값이 나오게 되며 플로우 f_x와 플로우 f_y사이의 IP 주소가 유사할수록 1에 가까운 결과 값이 나오게 된다.

그림 6은 그림 4와 그림 5에서 표현한 내용을 합친 것으로 Seed flow로부터 플로우의 시작시간과 IP 주소 쌍을 이용하여 그룹화 하는 과정을 표현한 그림이다. 즉, 두 플로우의 시작시간 차이와 IP 주소의 유사도의 임계값이 점선 원으로 표현되는 것이며 이를 만족하면 그룹화 되는 것이다.

$$a_{port}(f_x,f_y)=\begin{cases}0: f_x.PT \neq f_y.PT\\ 1: f_x.PT = f_y.PT\end{cases} \quad (4)$$

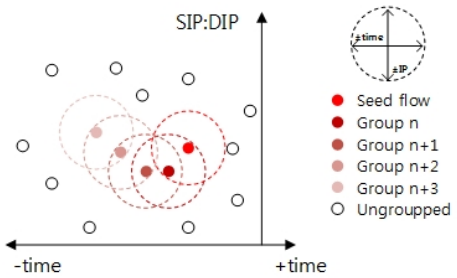


그림 6. 시작시간, IP 주소 쌍을 이용한 그룹화 과정
Fig. 6. Grouping process that uses starting time, IP address pair

$$a_{prot}(f_x,f_y)=\begin{cases}0: f_x.PROT \neq f_y.PROT\\ 1: f_x.PROT = f_y.PROT\end{cases} \quad (5)$$

식(4)와 식(5)는 플로우 f_x와 플로우 f_y사이의 포트번호, 프로토콜의 연결성을 계산하는 수식이며 두 수식의 결과 값은 0 또는 1이 나오게 된다. 즉, 두 플로우의 포트번호 또는 프로토콜이 같으면 1, 다르면 0이 나오는 것이다.

3.3 유사성(Similarity) 계산 방법

플로우간 유사성(Similarity)은 플로우의 통계정보인 플로우의 지속시간, 플로우에 포함된 패킷 수, 플로우를 구성하는 최대 5개까지의 패킷 크기, 패킷의 inter-arrival time 총 4개의 속성 값들 중 하나를 이용하여 두 플로우 사이의 코사인 유사도(Cosine Similarity) 값을 계산하게 된다.

코사인 유사도는 내적공간의 두 벡터 간 각도의 코사인 각도가 0도일 때의 코사인 값은 1이며, 다른 모든 각도의 코사인 값은 1보다 작다. 따라서 벡터의 크기가 아닌 방향의 유사도를 판단하는 목적으로 사용되며, 두 벡터의 방향이 완전히 같을 경우 1, 두 벡터의 각도가 90도의 각을 이룰 경우 0 값을 갖는다.

$$\cos(\theta)=\frac{A\cdot B}{\|A\|\|B\|}=\frac{\sum_{i=1}^{n}A_i\times B_i}{\sqrt{\sum_{i=1}^{n}(A_i)^2}\times\sqrt{\sum_{i=1}^{n}(B_i)^2}} \quad (6)$$

식(6)은 코사인 유사도를 계산하는 수식이며, 플로우 f_x와 플로우 f_y사이의 유사성(Similarity)을 계산하는 수식은 식(7)이 된다.

$$Sim(f_x,f_y)=\frac{f_x\cdot f_y}{\|\overrightarrow{f_x}\|\cdot\|\overrightarrow{f_y}\|} \quad (7)$$

$Sim(f_x,f_y)$의 결과값은 0과 1사이의 값이 나오게 되며 두 플로우의 유사도가 높은 경우 1에 가까운 결과 값이 나오게 된다.

$$f_a=\{+120,-150,+20,+20,-1600\}$$
$$f_b=\{+100,-120,+30,-10,-1000\}$$
$$f_c=\{+20,+20,-140,+10,-500\}$$

위와 같이 3개의 플로우가 있다고 가정한다. 괄호 안에 표현된 값들은 플로우의 패킷 크기를 의미하며

부호 값은 패킷의 방향을 의미한다. 즉, f_a의 출발지 IP주소가 α, 도착지 IP주소가 β일 경우 α에서 β로 전송된 패킷의 방향은 +, β에서 α로 전송된 패킷의 방향은 -로 표현되며 부호 뒤의 값은 전송된 패킷의 크기를 나타내는 것이다. 기준 플로우 f_a와 비교 대상 플로우 f_b, f_c를 식(7)에 적용한 값은 $Sim(f_a,f_b)$ =0.998971, $Sim(f_a,f_c)$=0.950542가 된다. 만약 유사성 그룹화 임계값이 0.97인 경우에는 플로우 f_a를 기준으로 플로우 f_b만 그룹화 되며, 플로우 f_c는 그룹화에서 제외된다. 결국 우리는 코사인 유사도 값을 이용하여 플로우 f_a는 플로우 f_c보다 f_b와 유사도가 높다고 판단하는 것이다.

3.4 FCI 사이버공격 트래픽 원천 추적 방법

FCI(Flow Correlation Index)는 기준 플로우와 비교 대상 플로우 간 관련성을 계산하기 위한 값으로 세부적으로는 연결성(Connectivity)과 유사성(Similarity)로 나누어지며, 이를 수치화 한 값이 FCI로 정의된다.

$$FCI(f_x,f_y) = w_c \times Conn(f_x,f_y) + w_s \times Sim(f_x,f_y) \quad (8)$$

식(8)은 두 플로우 f_x와 f_y의 FCI 값을 구하는 식으로 w_c는 연결성의 가중치 값이며 w_s는 유사성의 가중치 값이다. 두 가중치 값은 0 또는 1이며, 결과적으로 $FCI(f_x,f_y)$의 결과는 0에서 1사이의 값이 나오게 된다. 즉, 결과값이 1에 가까울수록 두 플로우의 발생 연관성이 높다는 것이다.

그림 7은 FCI를 사용하여 플로우의 연결성 또는 유사성을 사용자가 선택하고 계산하는 알고리즘인 HSC(Hybrid Similarity and Connectivity)를 순서도로 표현한 것이다. 사용자에게 입력받은 Seed Info를 바탕으로 Traffic Trace에서 Seed group을 찾고, Seed group을 시작으로 사용자에게 그룹화에 사용될 FCI (연결성 또는 유사성)를 선택받아 다음 플로우 그룹을 그룹화하게 되며, 그룹화 된 플로우는 종료하기 전에 바이너리 또는 텍스트 형태로 저장한다.

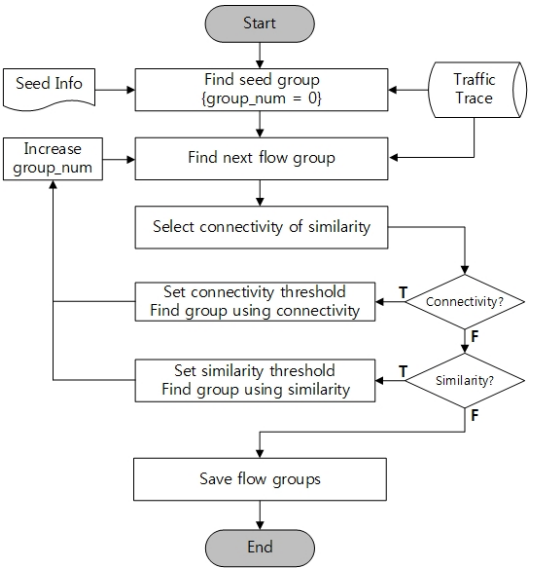


그림 7. FCI값을 이용한 그룹화 순서도
Fig. 7. Flowchart of grouping with FCI

Ⅳ. 실험 및 성능 평가

실험에 사용되는 트래픽 데이터는 2013년 국내에서 발생한 3.20대란 해킹 시나리오를 재현하고 이 때 발생한 트래픽을 수집하여 사용하였다. 그림 8은 시나리오를 표현한 것이며 수집된 트래픽 트레이스에는 APT 공격의 과정이 단계별로 존재한다.

표 1은 VMware를 사용하여 3.20 해킹 시나리오를 재현하기 위한 PC 구성 환경이며 표 2는 해킹 시나리오를 재현하여 수집한 트래픽의 정량적 정보이다.

전체 트래픽의 플로우 개수는 15,459개이며 그림 8의 ①부터 ⑦까지의 공격에 사용된 플로우의 개수는 26개였다. 공격에 사용된 플로우는 전체 플로우의 0.1%(패킷과 바이트는 전체의 0.3%)를 차지하며 전체 트래픽 중에서 매우 낮은 비율을 차지하고 있는 것을 알 수 있었다.

우리는 그림 8의 ⑦과정에서 피해를 입은 호스트의 IP주소(192.168.120.47)와 백신업데이트서버의 IP주소(192.168.120.61) 정보를 Seed Info로 사용하여 두 가지 트래픽 그룹화 실험을 진행했다. 실험 결과를 평

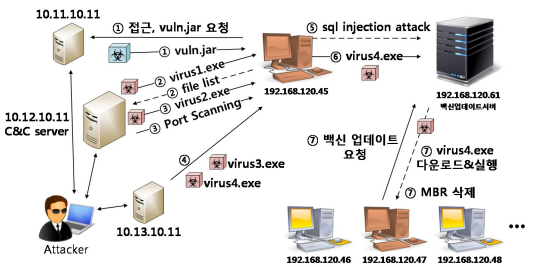


그림 8. 실험에 사용된 APT 공격 시나리오
Fig. 8. The scenario of APT attack that us used experiment

표 1. 실험을 위한 3.20 해킹 시나리오의 PC 구성 환경
Table 1. Environment of 3.20 hacking scenario for the experiment

Name(IP)	Specifications
Attacker PC (10.14.10.11)	Windows XP Pro SP3
C&C1 Server (10.12.10.11)	Windows XP Pro SP3
C&C2 Server (10.13.10.11)	Windows XP Pro SP2 APM(Apache,PHP,MySQL)
Web Server (10.11.10.11)	Windows XP Pro SP3 APM(Apache,PHP,MySQL)
PMS Server (192.168.120.61)	Windows XP Pro SP3 APM(Apache,PHP,MySQL) APC(Ahnlab Policy Center)
User1 PC (192.168.120.45)	Windows 7 Ultimate x86 Java 7 Update7
User2 PC (192.168.120.47)	Windows 7 Ultimate x86 V3 Internet Security 8.0

표 2. 실험에 사용된 트래픽의 정량적 정보
Table 2. Quantitative information on the traffic used in the experiment

	Flow	Packet	Byte(KB)
Total Traffic	15,459	193,574	108,144
Attack Traffic	26	640	430

표 3. 임계값을 고정한 추적 방법 적용 실험 결과
Table 3. The experimental results using fixed threshold

Threshold		Precision	Recall
Con	Sim		
0.71	-	92.86%	100%
0.71	0.5	1.03%	100%
0.65	-	68.42%	100%
0.6	0.5	0.43%	80.77%

Precision과 Recall 모두 100%의 결과를 얻을 수 있었다. 실험을 통해 그룹화 단계별로 임계값을 변화시키는 것이 고정된 임계값을 이용한 그룹화 결과보다 더 정확한 사이버 공격 트래픽을 추적할 수 있음을 확인하였다.

V. 결 론

본 논문에서는 네트워크 트래픽을 이용하여 네트워크에서 발생한 사이버공격 트래픽을 추적하는 방법을 제안하였다. 악성행위로 의심되는 플로우의 정보를 가하는 지표로 분석률(Recall)과 정확도(Precision)를 이용하였다. Recall은 전체 악성 트래픽 중에서 본 논문에서 제안하는 방법에 의해 그룹화된 플로우의 비율을 나타낸 것으로 분석률을 의미하며 Precision은 그룹화된 플로우 중에서 실제 악성 행위에 사용된 트래픽의 비율을 나타낸 것으로 정확도를 의미한다.

첫 번째 실험은 그룹화 임계값을 고정시킨 후 사이버공격 추적 실험을 진행했다. 표 3과 같이 첫 번째 실험 결과, 임계값을 고정시켰을 때 플로우의 연결성만 이용했을 때 정확도가 높았다. 하지만 플로우의 유사성을 함께 이용하여 그룹화를 진행했을 때는 정확도가 급격히 떨어짐을 알 수 있다. 여러 번의 실험 결과 실험에 사용되는 트래픽은 포트스캐닝 과정을 제외하면 전부 다른 형태의 플로우가 발생하였고, 유사성을 사용하여 그룹화를 진행하면 정확도가 급격히 떨어지는 것이었다. 따라서 두 번째 실험을 진행할 때에는 플로우의 연결성만을 계산하여 그룹화를 진행하였고, 각 그룹화 단계별로 임계값을 선택할 수 있게 하였다.

표 4는 그룹화 단계별로 임계값을 변경하면서 플로우의 연결성만을 계산하여 그룹화를 진행한 결과이다. 첫 번째 실험에서 가장 좋은 결과인 연결성 임계값 0.71을 시작으로 6번에 걸친 실험 결과

Seed 정보로 사용하여 Seed 그룹을 생성하고, Seed 그룹과 관련성이 높은 플로우를 그룹화 하는 방법이다. 플로우 간 관련성을 계산하기 위해 FCI(Flow Correlation Index)를 정의하였고, 실제 APT 공격 발생 시 수집한 트래픽에 적용하여 악성행위에 사용된 플로우를 100% 정확하게 찾아내었다. 이 결과는 전체 15,459개의 플로우 중 악성행위에 사용된 26개의 플로우를 찾아낼 수 있다는 것이다. 본 논문에서 제안한 방법이 완전히 자동화된 알고리즘은 아니지만, 이것을 이용할 경우 네트워크 침입, 해킹과 같은 보안사고 발생 시 빠르게 대응할 수 있음을 확인하였다. 하지만, 실험에 사용할 수 있는 실제 악성트래픽이 제한적이어서 다양한 경우의 네트워크 환경에는 사용이 제한적일 수 있다.

향후 연구로는 다양한 악성트래픽에 적용하여 본 논문에서 제안하는 방법의 성능을 발전시키고 계산 결과인 FCI 값을 머신러닝 알고리즘에 적용시켜 자동화된 악성트래픽 추적 시스템을 연구할 계획이다.

표 4. 가변적 임계값을 사용한 추적 방법 실험 결과
Table 4. The experimental results using variable threshold

Trial	Precision	Recall		Total	SG	G1	G2	G3	G4	G5	G6
						0.69	0.7	0.71	0.69	0.7	0.71
1	74%	100%	Total Flow	35	1	1	19	5	4	3	2
			Attack Flow	26	1	1	19	5	0	0	0
						0.69	0.71	0.7	0.72	0.73	0.74
2	76%	100%	Total Flow	34	1	1	4	20	4	2	2
			Attack Flow	26	1	1	4	20	0	0	0
						0.7	0.69	0.71	0.73	0.74	0.75
3	76%	100%	Total Flow	34	1	1	21	3	4	2	2
			Attack Flow	26	1	1	21	3	0	0	0
						0.7	0.71	0.69	0.74	0.75	-
4	96%	100%	Total Flow	27	1	1	4	20	1	-	-
			Attack Flow	26	1	1	4	20	0	-	-
						0.71	0.69	0.7	-	-	-
5	100%	100%	Total Flow	26	1	1	21	3	-	-	-
			Attack Flow	26	1	1	21	3	-	-	-
						0.71	0.7	0.69	-	-	-
6	100%	100%	Total Flow	26	1	1	19	5	-	-	-
			Attack Flow	26	1	1	19	5	-	-	-

References

[1] KISA, "*2016 report of 10 issues on Internet and information security(2016),*" Retrieved Feb. 16, 2016, from http://www.kisa.or.kr/public/library/IS_View.jsp?mode=view&p_No=158&b_No=158&d_No=295

[2] J. Mirković, G. Prier, and P. L. Reiher, "Attacking DDoS at the source," in *Proc. IEEE ICNP*, pp. 312-321, Nov. 2002

[3] J.-S. Choi, W.-H. Park, and K.-H. Kook, "Analysis of the advanced persistent threat (APT) - Targeting the korean defense industry -," *Korea Ass. Defense Ind. Stud.*, vol. 19, no. 2, pp. 73-89, Dec. 2012.

[4] Y.-H. Kim and W.-H. Park, "A study on cyber threat prediction based on intrusion detection event for APT attack detection," *Multimedia Tools and Appl.*, vol. 71, no. 2, pp. 685-698, Jul. 2014.

[5] S.-H. Yoon, J.-W. Park, and M.-S. Kim, "A study on internet traffic analysis based on two-way-flow," in *Proc KICS ICC 2008*, pp. 483-486, Yonsei Univ, Korea, Nov. 2008.

[6] S.-H. Yoon and M.-S. Kim, "Research on signature maintenance method for internet application traffic identification using header signatures," *J. KSII*, vol. 12, no. 6, pp. 19-33, Dec. 2011.

[7] S.-H. Yoon and M.-S. Kim, "Research on header signature maintenance method for internet application traffic identification," in *Proc. KICS ICC 2011*, pp. 1200-1201, Jeju Island, Korea, Jun. 2011.

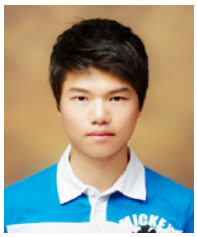
[8] H.-M. An, J.-H. Ham, and M.-S. Kim, "Performance improvement of the statistical information based traffic identification system," *KIPS Trans. Computer and Commun. Syst. (KTCCS)*, vol. 2, no. 8, pp. 335-342, Aug. 2013.

[9] H.-M. An, S,-K. Lee, J,-H. Ham, and M,-S. Kim, "Traffic identification based on applications using statistical signature free from abnormal TCP behavior," *J. Inf. Sci. and Eng.*,

vol. 31, no. 5, pp. 1669-1692, Sept. 2015.

[10] J.-S Park, J.-W. Park, S.-H. Yoon, and M.-S. Kim, “Performance improvement of application-level traffic classification algorithm based on payload signature,” in *Proc. KICS ICC 2010*, pp. 1059-1060, Jun. 2010.

구 영 훈 (Young-Hoon Goo)



2016년 : 고려대학교 컴퓨터정보학과 학사

2016년~현재 : 고려대학교 컴퓨터정보학과 석사과정

<관심분야> 네트워크 관리 및 보안, 트래픽 모니터링 및 분석

이 수 강 (Su-Kang Lee)

2014년 : 고려대학교 컴퓨터정보학과 학사

2014년~현재 : 고려대학교 컴퓨터정보학과 석사과정

<관심분야> 네트워크 관리 및 보안, 트래픽 분석, 미래인터넷

김 성 민 (Sung-Min Kim)

2014년 : 고려대학교 컴퓨터정보학과 학사

2014년~현재 : 고려대학교 컴퓨터정보학과 석사과정

<관심분야> 네트워크 관리 및 보안, 트래픽 분석, 데이터 암호화

최 선 오 (Sun-Oh Choi)

2005년 : 고려대학교 컴퓨터학과 학사

2008년 : 고려대학교 컴퓨터학과 석사

2014년 : Purdue 대학교 전자 및 컴퓨터공학과 박사

2014년~현재 : 한국전자통신연구원 선임연구원

<관심분야> 네트워크보안, 데이터 보안

김 명 섭 (Myung-Sup Kim)

1998년 : 포항공과대학교 전자계산학과 학사

2000년 : 포항공과대학교 전자계산학과 석사

2004년 : 포항공과대학교 전자계산학과 박사

2006년 : Dept. of ECS, Univ. of Toronto Canada

2006년~현재 : 고려대학교 컴퓨터정보학과 교수

<관심분야> 네트워크 관리 및 보안, 트래픽 모니터링 및 분석, 멀티미디어 네트워크