Journal of the Korea Convergence Society
Vol. 10. No. 12, pp. 17-22, 2019

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2019.10.12.017

시계열 방사축과 원통좌표계를 이용한 네트워크 트래픽 공격 시각화

장범환, 최윤성*
호원대학교 컴퓨터학부 교수

Visualization of network traffic attack using time series radial axis and cylindrical coordinate system

Beom-Hwan Chang, Younsung Choi*
Professor, Division of Computer, Howon University

요 약 네트워크 트래픽 세션 데이터를 이용한 공격 분석 및 시각화 방법들은 세션 데이터 내의 송신지 및 수신지 IP주소 및 연결관계를 시각화하여 네트워크 이상 현상들을 감시한다. 트래픽의 송수신 방향은 이상 현상을 탐지하는데 있어서 매우 중요한 특징이지만, 단순히 송신지와 수신지 IP주소를 좌 · 우 또는 상 · 하 대칭적으로 시각화하는 것은 분석을 난해하게 만드는 요소가 된다. 또한, 시계열적인 트래픽 세션들의 시간 특성을 고려하지 않고 시각화 인터페이스를 설계할 경우에는 시간별 보안 상황 정보가 손실되는 위험을 감수해야 한다. 본 논문에서는 방사축을 이용하여 시계열 트래픽 데이터를 시각화하고 IP주소를 네트워크 부분과 호스트 부분으로 분할 및 원통좌표계에 표출시켜 효과적으로 네트워크 공격을 감시할 수 있는 시각화 인터페이스와 분석 방법을 제안하고자 한다. 제안하는 방법은 네트워크 공격을 직관적으로 인지하고 공격 활동을 시간흐름에 따라 파악할 수 있는 장점을 가진다.

주제어 : 네트워크 보안, 네트워크 트래픽 시각화, 네트워크 공격 감시, 보안관제

Abstract Network attack analysis and visualization methods using network traffic session data detect network anomalies by visualizing the sender's and receiver's IP addresses and the relationship between them. The traffic flow is a critical feature in detecting anomalies, but simply visualizing the source and destination IP addresses symmetrically from up-down or left-right would become a problematic factor for the analysis. Also, there is a risk of losing timely security situation when designing a visualization interface without considering the temporal characteristics of time-series traffic sessions. In this paper, we propose a visualization interface and analysis method that visualizes time-series traffic data by using the radial axis, divide IP addresses into network and host portions which then projects on the cylindrical coordinate system that could effectively monitor network attacks. The proposed method has the advantage of intuitively recognizing network attacks and identifying attack activity over time.

Key Words : Network Security, Network Traffic Visualization, Network Attack Monitoring, Managed Security

*This paper was supported by research fund (2019), Howon University.
*Corresponding Author : Younsung Choi(yschoi@howon.ac.kr)
Received November 14, 2019 Revised December 4, 2019
Accepted December 20, 2019 Published December 28, 2019

1. 서론

네트워크 트래픽 세션 데이터를 이용한 공격 분석 및 시각화 방법들은 세션 데이터 내의 송신지 및 수신지 IP 주소 및 연결관계를 시각화하여 네트워크 이상 현상들을 감시한다[1-4]. 이는 공격을 포함한 네트워크 활동들이 송신지와 수신지간의 연결설정과 데이터를 송수신하는 행위이기 때문에 그 과정들을 시각적으로 표시함으로써 비정상적인 현상들을 효과적으로 감시할 수 있기 때문이다[5]. 하지만, 단순히 트래픽 세션의 송수신 방향을 이용하여 송신지와 수신지 IP주소를 좌·우 또는 상·하 대칭적으로 시각화할 경우에는 단일 방향에 따른 반사(reflection) 문제[6]가 생기고, 시계열적인 트래픽 세션들의 시간 요소는 고려하지 않고 시각화할 경우에는 시간(상황) 정보 손실 문제가 발생한다.

시각적 표현에서 시계열 이벤트를 발생 순서대로 표시하는 것은 매우 중요하다. 시계열 이벤트는 일정 시간 간격 또는 시간 순서에 따라 정렬 배치되는 이벤트 데이터들의 수열을 말한다. 시계열 데이터는 시간에 따라 변경 내용이 측정되므로 미래 변경 내용을 예측할 수도 있고 과거 변화량을 추적·조회할 수도 있다[7,8]. 시계열 데이터의 시간요소를 고려하지 않고 시각화 인터페이스를 설계한다면 시간과 관련된 정보 손실이 발생한다.

송신지와 수신지 IP주소를 양쪽(좌·우, 상·하) 대칭 평면으로 설계하고 단방향으로 표현 및 중첩하는 것은 구조적인 문제를 갖는다. 통신하는 각각의 종단 호스트(IP주소)들은 때로는 송신지 역할이었다가 때로는 수신지 역할을 수행하는 구조여서 고정적인 통신 진행 방향은 존재하지 않는다. 대표적인 트래픽 세션 정보인 시스코 넷플로우(Netflow)는 단일 방향으로 전송되는 패킷 집합을 하나의 독립된 트래픽 플로우로 정의한다. 종단간에 왕래하는 패킷 데이터들은 방향이 각각 다른 2개의 단방향 트래픽 플로우로 제공한다[6,9]. 다수의 호스트와 세션 정보들을 연결선으로 중첩 표시한다면 송수신 방향을 구분하는 것이 불가능하고 의미가 없다.

본 논문에서는 트래픽의 시간요소 표현과 대칭평면 시각화 구조 문제를 해결하기 위해서 IP주소를 네트워크 부분과 호스트 부분으로 분할하고 방사축을 이용하여 시계열 트래픽 데이터를 원통좌표계에 표출시키는 네트워크 공격 감시를 위한 효과적인 시각화 인터페이스를 제안한다.

2. 관련 연구

네트워크 트래픽 플로우 기반 시각화 기술에는 FlowScan[10], NVisionIP[11], VisFlowConnect-IP[12], FloVis[13] 등이 있다. FlowScan은 라우터들에서 보고하는 넷플로우 데이터를 실시간으로 시각화하여 네트워크 트래픽을 감시하는 도구이다[10]. 선형 시간축과 선-영역 그래프를 사용하여 프로토콜별 트래픽 추이를 감시하고 정확한 정보 전달을 위해 텍스트를 결합한 후 웹 인터페이스를 통해 결과를 제공한다[8]. 시간 정보를 활용하여 데이터를 시간 순서데로 표현하고 있지만 호스트들간의 자세한 연결 정보 및 보안 정보는 표시가 안된다.

NVisionIP는 비정상적인 트래픽의 패턴을 탐지하기 위해 트래픽을 하나의 화면에 시각화하는 도구이다. 2D 매트릭스 속에 전체 네트워크의 서브넷들과 호스트 IP 주소를 4-픽셀 사각형으로 표시한다[11]. 각 사각형의 색상은 트래픽 내의 포트번호에 따라 매핑하고 있다. 하지만, 시각화는 한 번에 한 가지 상태만을 보여주며, 시간이 지남에 따라 변칙적인 행동은 한 눈에 감시할 수 없다. Small Multiple View는 전체 네트워크의 상황 정보 제공보다는 두 개의 막 대형 차트를 사용하여 호스트에 대한 추가 정보를 제공한다. 제한된 양의 호스트만 화면에 표시 될 수 있으므로 전체 상황 정보가 유실되며 자세한 정보를 얻기 위해 분석가는 Machine View에서 원시 트래픽 데이터를 조사해야 한다[14].

VisFlowConnect-IP[12]는 트래픽 세션의 연결 정보에 초점을 맞추고 외부 도메인 시스템들과 내부 시스템들 간의 트래픽 흐름을 3개의 '평행 수직축(parallel axes)'을 사용하여 상황을 표현하는 시각화 도구이다[6]. 내부 도메인의 호스트를 표시하는 축을 중심으로 좌측에는 외부 도메인에서 데이터를 송신하는 송신지 호스트를 표현하는 축, 우측에는 데이터를 수신하는 외부 수신지 호스트를 표시하는 축으로 구성되며 연결선을 이용하여 내·외부 호스트간의 연결 관계를 표현한다[6].

FloVis[10]은 네트워크 트래픽 흐름을 FlowBundle, NetBytes Viewer, Activity Plot 화면으로 시각화하는 도구이다. 특히, NetBytes Viewer는 3D 임펄스 그래프를 사용하여 네트워크 내의 서브넷과 개별 호스트들의 트래픽 데이터를 시각화한다. 하지만, 네트워크 활동 자체가 아닌 활동 수만을 표시하므로 네트워크 공격이 잘못 해석 될 수도 있다[15].

3. 시각화 인터페이스 설계

수집·정제된 1개의 트래픽 플로우 이벤트를 송신지 노드(〈발생시간정보, 송신지IP주소, 프로토콜번호, 송신지 포트번호〉)와 수신지 노드(〈발생시간정보, 수신지IP주소, 프로토콜번호, 수신지포트번호〉)로 분리한 후, 송신지IP 주소와 수신지IP주소는 Eq. (1)에 따라 Fig. 1와 같이 호스트 평면의 점좌표 N_1과 N_2로 표시하고, 송신지포트번호와 수신지포트번호는 Eq. (2)에 따라 Fig. 2와 같이 포트 평면의 점좌표 P_1과 P_2로 표시한다.

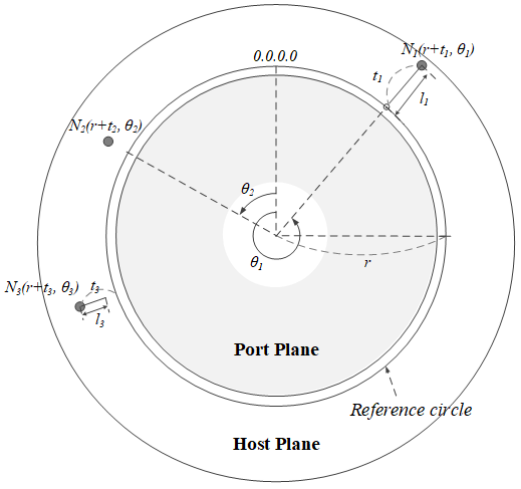

Fig. 1. Host plane viaualization using 2D cylindrical coordinate system

$$N_1(r+t_1, \theta_1),$$
$$where \quad \theta_1 = \frac{[Host\ Idenifier\ of\ IPAddr_1]}{2^{16}} \times 2\pi \quad \cdots \text{Eq. (1)}$$

Fig. 1.에서 점좌표 N_1의 각도(θ_1)는 IP주소의 B-클래스를 기준으로 호스트ID 부분을 2^{16}으로 나누고 2π를 곱한 값이고, 반지름($r+t_1$)은 포트 평면과 호스트 평면을 구분짓는 기준 참조원의 반지름(r)과 이벤트가 마지막으로 발생된 시간(t_1)의 합이다. 따라서 점좌표 N_1의 꼬리선(l_1)은 이벤트가 최초 발생한 시간부터 마지막으로 발생한 시간까지의 시간 간격을 의미하는 방사축 구조를 갖는다. 즉, Fig. 1에 표시된 N_1은 감시 시작 시점부터 감시 종료 시점까지 발생한 호스트 노드이고, N_2는 전체 감시 시간 동안 1회 발생한 호스트 노드, 그리고 N_3는 일정 시간 동안 발생한 호스트 노드이다.

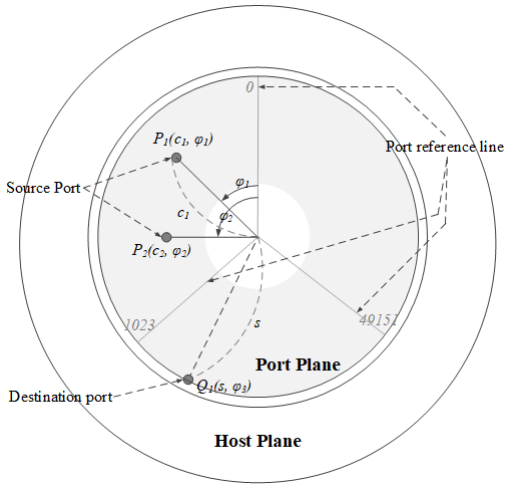

Fig. 2. Port plane viaualization using 2D cylindrical coordinate system

$$P_1(c_1, \varphi_1),$$
$$where \quad \varphi_1 = \frac{[Port\ Nmber]}{2^{16}} \times 2\pi \quad \cdots\cdots \text{Eq. (2)}$$

Fig. 2에서 송신지포트번호를 표시하는 점좌표 P_1의 각도(φ_1)는 포트번호를 2^{16}으로 나누고 2π를 곱한 값이고, 반지름(c_1)은 발생빈도를 누적한 값으로써 반지름을 통해 해당 포트의 이용빈도를 감시할 수 있도록 한다. 수신지포트번호를 표시하는 점좌표 Q_1의 반지름(s)은 고정된 길이를 가짐으로써 송신지포트와 구분하여 표시한다. 추가적으로, 대표 프로토콜(ICMP, TCP, UDP, 기타 프로토콜)에 따라 포트평면의 점좌표들(P_1, P_2, Q_1)에게는 프로토콜에 따라 특정 색상을 부여함으로써, 사용자가 특정 프로토콜을 선택할 경우 해당 프로토콜을 이용한 호스트 노드와 포트 노드를 표시하여 프로토콜별 보안상황을 효율적으로 감시하도록 한다.

Fig. 1의 호스트평면에 표시되는 점 N_1(트래픽 플로우 이벤트의 송신지IP주소 또는 수신지IP주소)은 호스트ID 부분을 이용하고 있는데, 여기서 네트워크ID 부분을 Eq. (3)을 이용하여 계산한 후, Fig. 3.과 같이 최종 3D 원통좌표계의 점으로 표시한다. 여기서, 점 N_1의 높이(h_1)는 IP주소의 네트워크주소 부분을 2^{16}로 나눈 값이다. 따라서, 동일 네트워크의 호스트들은 같은 높이의 띠 형태의 점들로 형성화된다. 점좌표 N_1을 생성하는 계산식은 Eq. (3)과 같다.

$$N_1(r+t_1, \theta_1, h_1),$$
$$where \quad \theta_1 = \frac{[Host\ Idenifier\ of\ IPAddr_1]}{2^{16}} \times 2\pi,$$
$$h_1 = \frac{[Network\ Identifier\ of\ IPAddr_1]}{2^{16}} \quad \cdots\cdots \text{Eq. (3)}$$

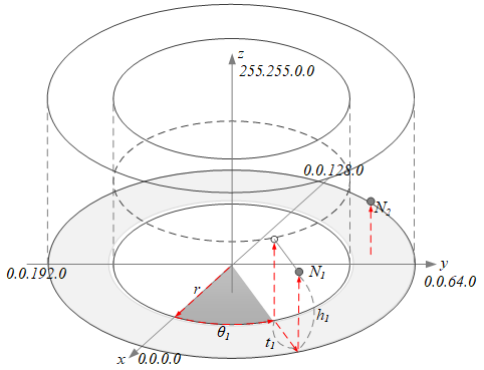

Fig. 3. Network traffic visualization using 3D cylindrical coordinate system

4. 시각화 인터페이스 구현 및 적용

2D/3D 원통좌표 트래픽 시각화 인터페이스의 구현과 적용 실험을 위해 사용한 데이터는 한국과학기술정보연구원의 라우터(KREONET과 미국의 StarTap 구간)를 통해 수집한 Netflow v5 데이터이다. 시각화 분석을 수행한 결과는 Fig. 4와 Fig. 5와 같다.

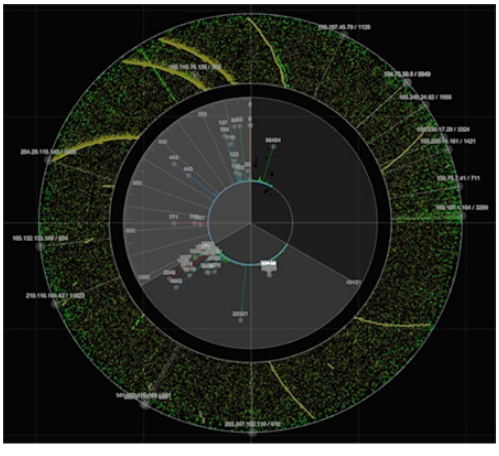

Fig. 4. Analysis network traffic using 2D cylindrical coordinate system

Fig. 4는 2D 원통좌표 시각화 분석의 결과이다. 방사형 시간축을 따라 각종 네트워크 공격들과 서버의 네트워크 활동을 패턴화하여 표출함으로써 관리자는 직관적으로 네트워크 공격들을 쉽게 관찰할 수 있다. Fig. 5는 3D 원통좌표 시각화 분석 결과로써 특정 네트워크(도메인)에서 진행되고 있는 연결(송·수신) 활동과 특정 네트워크로 집중되는 현상을 직관적으로 표출하고 있다.

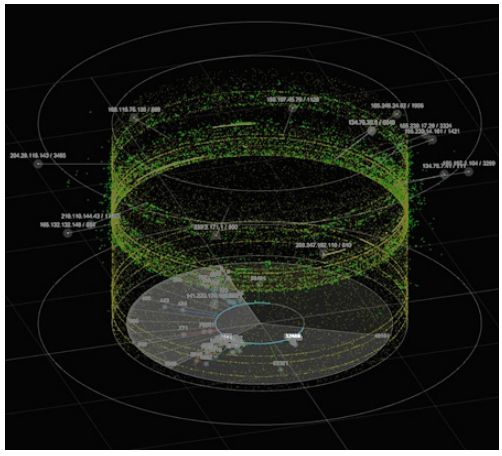

Fig. 5. Analysis network traffic using 3D cylindrical coordinate system

Fig. 4에서 개별 공격 현상과 정상 서버 등을 검출하기 위해서 특정 노드를 선택할 경우, Fig. 6-10과 같은 결과를 볼 수 있다. Fig. 6은 정상 웹 서버의 활동 모습(상대방 IP주소와 포트번호가 랜덤하게 분포됨), Fig. 7은 ICMP Echo Request를 이용한 호스트스캔 공격(시간 흐름에 따라 상대방 IP주소가 특정 네트워크 상에서 일률적으로 증가하고 프로토콜과 포트번호가 고정됨 -ICMP Echo Request(8)는 netflow에서는 2048로 해석), Fig. 8.은 포트스캔 공격(특정 상대방 IP주소에 대해 포트번호만 일률적으로 증가함), Fig. 9는 인터넷 웜의 일종인 MS-SQL Slammer(UDP:1434) 웜 공격, Fig. 10은 FTP 서버에 대한 DDoS 공격에 대한 시각화 형상이다. 공격을 포함한 대부분의 네트워크 이상 현상들은 종단간의 세션 패턴들이 발산 또는 수렴 형태를 보이므로 이상 현상들은 호스트평면과 포트평면 상에 표시되는 점들의 분포와 형태, 발생 빈도 수, 시계열 형상 등을 통해 감시할 수 있다.

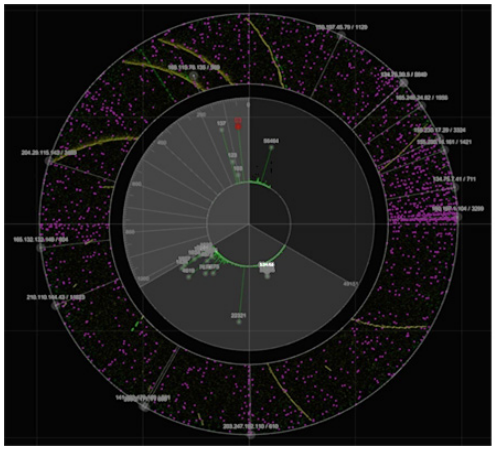

Fig. 6. Normal web server

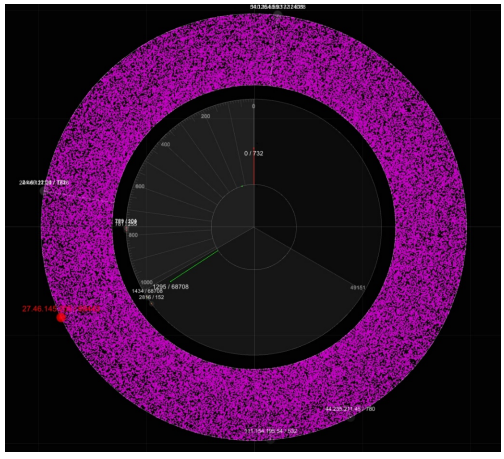

Fig. 9. Internet worm

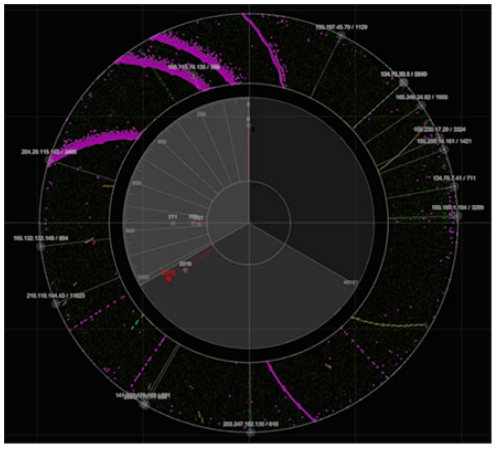

Fig. 7. Host scan attack

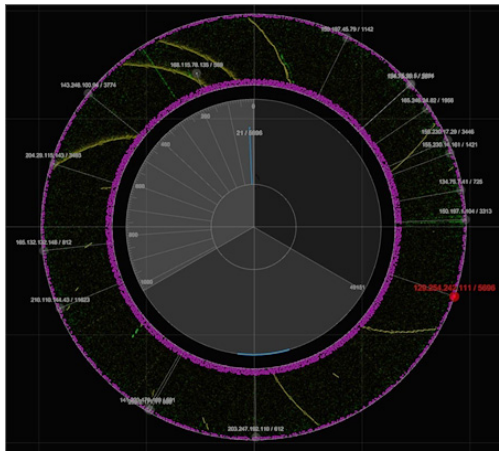

Fig. 10. DDoS attack

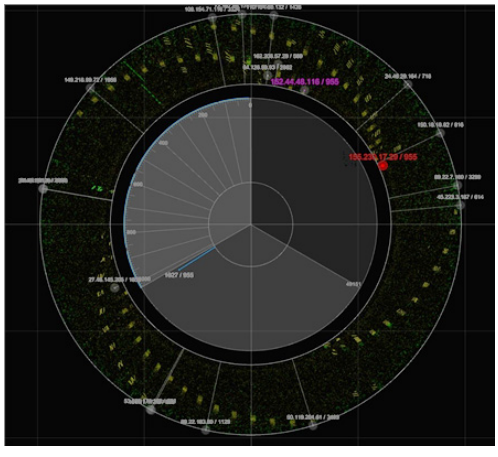

Fig. 8. Port scan attack

5. 결론

본 논문에서는 시계열 방사축과 원통좌표계를 이용하여 네트워크 공격을 감시할 수 있는 시계열 트래픽 시각화 인터페이스를 설계하고 구현하였다. 네트워크 트래픽 데이터는 시간 방사축에 따라 원통좌표계 상에 호스트 점좌표들과 포트 점좌표들로 표출된다. 시간 방사축을 따라 시각화된 점좌표들의 형태, 즉 호스트들의 분포와 프로토콜별 포트 이용 현황을 관찰함으로써 사용자는 전체 공격 및 개별 공격들의 종류, 진행경과, 연속성, 지속성 등을 직관적으로 인지할 수 있다. 기존 FlowScan에서 호스트들간의 자세한 연결 정보 및 보안 정보를 표시 못하는 단점과 NVisionIP에서 시간이 지남에 따라 변칙적

인 행동들을 한 화면에 표시 못하는 단점을 개선했다.

제안하는 기술은 네트워크 트래픽을 감시하는 네트워크 관리 분야, 그리고 각종 네트워크 이상 상황을 탐지하고 대응 및 예보하는 보안관제와 보안상황 인지 분야에 많은 기여가 있을 것으로 생각된다. 또한 일반적인 대용량 시계열 이벤트의 분석 등에도 활용도가 높을 것으로 예상된다. 향후에는 제안하는 시각화 기술과 머신러닝 기술을 접목하여 공격 탐지 및 공격 유형 판별이 자동화되도록 연구를 진행할 계획이다.

REFERENCES

[1] E. L. Malécot, M. Kohara, Y. Hori & K. Sakurai. (2006, Nov.). Interactively Combining 2D and 3D Visualization for Network Traffic Monitoring. *3rd International Workshop on Visualization for Computer Security.* (pp. 123-127). Alexandria, Virginia, USA.

[2] A. Giani, I. G. D. Souza, V. Berk & G. CybenkoI. (2006, Oct.). Attribution and Aggregation of Network Flows for Security Analysis. *2006 CERT FloCon Workshop.* (pp. 1-4). Vancouver, Washington, USA.

[3] E. W. Bethel, S. Campbell, E. Dart, K. Stockinger & K. Wu. (2006, Oct.). Accelerating Network Traffic Analytics Using Query-Driven Visualization. *2006 IEEE Symposium on Visual Analytics Science and Technology.* (pp. 115-122). Baltimore, MD.

[4] R. Ball, G. Fink & C. North. (2004, Oct.), Home-Centric Visualization of Network Traffic for Security Administration. *Workshop on Visualization and Data Mining for Computer Security.* (pp. 55-64). Washington DC, USA.

[5] B. H. Chang. (2012). A Method for Detection and Classification of Normal Server Activities and Attacks Composed of Similar Connection. *Journal of the Korean Institute of Information Security and Cryptology, 22(6),* 1315-1324.

[6] B. H. Chang. (2016). Monitoring Network Security Situation Based on Flow Visualization. *Convergence security journal, 16(5),* 41-48.

[7] S. W. Han. (2016). *A Study on Periodic data visualization via Media Design Focusing on Periodic Mass Extinction.* Doctoral dissertation. Seoul National Universisty, Seoul.

[8] B. H. Chang. (2018). Monitoring and Tracking of Time Series Security Events using Visualization Interface with Multi-rotational and Radial Axis. *Convergence security journal, 18(5),* 33-43.

[9] B. H. Chang. (2015). Network Attacks Visualization using a Port Role in Network Sessions. *Journal of the Korea Society of Digital Industry and Information Management, 11(4),* 47-60.

[10] CAIDA. (Accessed Nov. 5, 2018). *FlowScan - Network Traffic Flow Visualization and Reporting Tool.* [Online]. www.caida.org/tools/utilities/flowscan/

[11] K. Lakkaraju, W. Yurcik & A. J. Lee. (2004, Oct.). NVisionIP: Netflow Visualizations of System State for Security Situational Awareness. *2004 ACM Workshop on Visualization and Data Mining for Computer Security.* (pp. 65-72). Washington, DC, USA.

[12] X. Yin, W. Yurcik & A. Slagell. (2005, Mar.). The Design of VisFlowConnect-IP: A Link Analysis System for IP Security Situational Awareness. *3rd IEEE International Workshop on Information Assurance.* (pp. 141-153). College Park, MD, USA.

[13] T. Taylor, D. Paterson, J. Glanfield & et al. (2009, Mar.). FloVis: Flow visualization system. *Cybersecurity Applications & Technology Conference For Homeland Security.* (pp. 186-198). Washington, DC, USA.

[14] C. Kintzel, J. Fuchs & F. Mansmann. (2011, July). Monitoring Large IP Spaces with ClockView. *8th International Symposium on Visualization for Cyber Security.* (Article No.: 2, pp. 1-10). Pittsburgh, PA, USA.

[15] T. Nunnally, K. Abdullah, A. Uluagac, J. Copeland & R. Beyah. (2013, Oct.). NAVSEC : A Recommender System for 3D Network Security Visualizations. *Tenth Workshop on Visualization for Cyber Security.* (pp. 41-48). Atlanta GA, USA.

장 범 환(Beom-Hwan Chang) [정회원]

· 1997년 2월 : 성균관대학교 전자공학과(공학사)
· 1999년 2월 : 성균관대학교 전기전자컴퓨터공학과(공학석사)
· 2003년 2월 : 성균관대학교 전기전자컴퓨터공학과(공학박사)
· 2003년 3월 ~ 2012년 2월: 한국전자통신연구원 선임연구원
· 2012년 3월 ~ 현재 : 호원대학교 컴퓨터학부 교수
· 관심분야 : 네트워크 보안, 빅데이터 시각화, 인공지능
· E-Mail : bchang@howon.ac.kr

최 윤 성(Younsung Choi) [정회원]

· 2006년 2월 : 성균관대학교 정보통신공학부(공학사)
· 2007년 8월 : 성균관대학교 전기전자컴퓨터공학부(공학석사)
· 2015년 8월 : 성균관대학교 전기전자컴퓨터공학부(공학박사)
· 2016년 2월 ~ 현재 : 호원대학교 컴퓨터학부 교수
· 관심분야 : 정보보호, 빅데이터 시각화, 네트워크 포렌식
· E-Mail : yschoi@howon.ac.kr