情報保護學會論文誌
第19卷 第3號, 2009. 6

# 시각화 기반의 효율적인 네트워크 보안 상황 분석 방법*

정 치 윤,†‡ 손 선 경, 장 범 환, 나 중 찬
한국전자통신연구원

# An Efficient Method for Analyzing Network Security Situation Using Visualization*

Chi Yoon Jeong,†‡ Seon-Gyoung Sohn, Beom-Hwan Chang, Jung-Chan Na
Electronics and Telecommunications Research Institute

## 요 약

네트워크 관리자가 침입 탐지 시스템, 방화벽 등의 보안 장비에서 발생하는 경보 메시지를 통하여 네트워크에서 이상 현상이 발생하였는지를 인지하고, 이상 현상이 실제 네트워크 보안 위협인지를 판단하기 위해서는 경보 메시지와 관련된 트래픽을 검색하고 분석하는 등의 일련의 작업이 필요하다. 하지만 보안 장비에서 발생되는 경보 메시지의 양이 많을 뿐만 아니라, 네트워크 관리자가 관련 트래픽을 검색하고 분석하는데 많은 시간이 소요되는 등의 문제점이 있다. 따라서 본 논문에서는 보안 이벤트 시각화 기술을 사용하여 네트워크의 보안 상황을 보다 빠르고 효과적으로 분석할 수 있는 방법을 제안한다. 제안된 방법의 경우 전체 IP 주소 공간에서 트래픽의 흐름을 표현하기 때문에 네트워크 관리자가 현재 네트워크에서 발생되는 보안 위협을 보다 빠르게 판단할 수 있도록 도와준다.

## ABSTRACT

Network administrator recognizes the abnormal phenomenon in the managed network by using the alert messages generated in the security devices including the intrusion detection system, intrusion prevention system, firewall, and etc. And then the series of task, which searches for the traffic related to the alert message and analyzes the traffic data, are required to determine where the abnormal phenomenon is the real network security threat or not. There are many alert messages to have to inspect in order to determine the network security situation. Also the much times are needed so that the network administrator can analyze the security condition using existing methods. Therefore, in this paper, we proposed an efficient method for analyzing network security situation using visualization. The proposed method monitors anomalies occurred in the entire IP address's space and displays the detail information of a security event. In addition, it represents the physical locations of the attackers or victims by linking GIS information and IP address. Therefore, it is helpful for network administrator to rapidly analyze the security status of managed network.

**Keywords:** Information visualization, Security visualization, Network monitoring, Network situation awareness

## I. 서 론

최근 네트워크 인프라의 발전으로 인하여 인터넷이 급격하게 확산되면서 인터넷을 이용하는 사람들의 수가 급격하게 증가하고 있다. 이로 인하여 인터넷 상에서 이루어지는 네트워크 공격의 발생 빈도도 점점 더 증가하고 있으며, 네트워크 공격을 탐지하는 보안 장비에서 발생하는 경보 메시지의 수도 점점 더 늘어나

접수일(2008년 9월 25일), 수정일(2009년 4월 20일), 게재확정일(2009년 5월 25일)
* 본 연구는 지식경제부 및 정보통신연구진흥원의 IT 신성장동력핵심기술개발사업(2007-S-022-03, All-IP환경의 지능형 사이버공격 감시 및 추적 시스템)의 일환으로 수행하였습니다.
† 주저자, iamready@etri.re.kr
‡ 교신저자, iamready@etri.re.kr

고 있다. 네트워크 보안 장비에서 발생되는 경보 메시지의 경우 정상 트래픽을 네트워크 공격으로 잘못 판단하는 오탐(False positives)을 발생 시킬 수 있는 가능성이 있기 때문에 네트워크 관리자는 경보 메시지의 정보를 사용하여 대응을 하기 전에 실제 공격인지 여부를 판단 과정이 필요하다. 현재 네트워크 관리자는 공격 여부를 판단하기 위해서 경보 메시지와 관련된 트래픽을 검색한 후, 검색된 트래픽으로부터 근원지 IP의 분산도 및 각 IP별 트래픽의 집중도, 목적지 IP의 분산도 및 각 IP별 트래픽의 집중도, 근원지 및 목적지 포트 번호별 트래픽의 집중도 및 분산도 등을 분석한다. 또한 근원지와 목적지 IP의 정보를 조회하여 IP가 속한 국가, 기관 등의 정보를 추출하는 일련의 과정을 거쳐 최종적으로 공격 여부를 판단하고 대응하게 된다. 하지만 이와 같은 과정은 시스템화 되어 있지 않고 관리자의 수작업으로 이루어지는 경우가 많기 때문에 공격 여부를 판단하는데 많은 시간이 소요된다. 또한 보안 장비에서 발생하는 경보 메시지의 수가 계속 증가하고 있기 때문에 네트워크 관리자가 기존의 방법을 통하여 네트워크의 보안 상황을 분석하기에는 어려움이 있다.

최근 네트워크의 보안 상황을 신속하게 분석하기 위한 방법으로 보안 이벤트 시각화 기술에 대한 연구가 활발히 진행되고 있다. 보안 이벤트 시각화 기술은 네트워크 상에서 발생되는 방대한 양의 이벤트를 실시간으로 시각화하는 기술로써, 네트워크 관리자에게 보안과 관련된 많은 정보를 신속하고 쉽고 정확하게 전달 할 수 있는 장점이 있다. 네트워크 관리자는 보안 이벤트 시각화 기술을 사용하여 현재 네트워크에서 발생되는 트래픽 흐름 및 경보 메시지를 파악하고, 이상 현상을 유발한 트래픽의 특성을 빠르게 분석하여 이상 현상이 실제 네트워크 공격인지를 신속하게 판단할 수 있다. 또한 보안 이벤트 시각화 기술을 사용하면 서비스 거부 공격(DoS: Denial of Service), 분산 서비스 거부 공격(DDos: Distributed Dos), 인터넷 웜, 호스트 스캔 등의 네트워크 공격에 대한 패턴을 잘 표현할 수 있기 때문에 네트워크 공격을 직관적으로 인지 할 수 있다. 따라서 본 논문에서는 시각화 기반의 효율적인 네트워크 보안 상황 분석 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 보안 이벤트 시각화 기술과 관련된 연구 동향에 대해서 서술하고, 3장에서는 본 논문에서 제안한 시각화 기반의 효율적인 네트워크 보안 상황 분석 방법에 대해서 설명할 것이다. 4장에서는 제안된 방법에 대한 실험 결과를 보여주고, 5장에서는 결론을 내릴 것이다.

## II. 관련 연구

보안 이벤트 시각화 기술은 네트워크에서 발생하는 방대한 양의 보안 이벤트로부터 특성 정보를 추출한 후, 정보 시각화(Information Visualization)기법을 사용하여 2차원 또는 3차원 공간상에 보안 이벤트의 내용을 표현하는 기법이다. 보안 이벤트 시각화 기술은 보안 이벤트를 전송한 네트워크의 지점 및 보안 이벤트의 종류에 따라서 구분된다. 보안 이벤트를 전송한 지점은 호스트 내부, 네트워크에 연결된 호스트, 네트워크 등으로 구분 되며[1], 보안 이벤트는 라우터, 스위치 등의 네트워크 장비에서 발생하는 트래픽 정보와 방화벽, 침입 탐지 시스템 등의 보안 장비에서 발생하는 경보 메시지로 나누어진다[2]. 트래픽 정보를 사용하여 보안 이벤트를 시각화 하는 방법은 NVisionIP[3]을 비롯하여 많은 연구[2-9]가 진행되고 있으며, 경보 메시지를 시각화하는 방법은 SnortView[10]를 포함하여 다양한 방법[10-13]들이 연구되고 있다. 본 논문에서는 보안 이벤트를 네트워크 상의 트래픽 정보로 한정하여 보안 이벤트 시각화 기술을 다룰 것이다. 또한 네트워크 공격의 의미를 트래픽 정보를 통하여 인지할 수 있는 분산 서비스 거부 공격, 서비스 거부 공격, 인터넷 웜, 호스트 스캔, 포트 스캔으로 한정하여 사용할 것이다.

네트워크에서 발생되는 트래픽 정보를 시각화하여 네트워크 보안 상황 인지 하는 기술은 VisualScope[2], NVisionIP [3], VisFlowConnect-IP[4], PortVis[5] 등이 있다. NVisionIP는 B클래스 네트워크의 서브넷을 가로축, 호스트를 세로축으로 설정하여 호스트에서 사용하는 유일한 포트의 수를 화면상에 표현하는 Galaxy View, 네트워크 관리자에서 선택된 서브넷의 호스트의 특정 포트별 플로우 수를 표현하는 Small Multiple View, 한 호스트에서 송·수신 되는 포트별 트래픽의 양을 표현하는 Machine View 등의 세 화면으로 구성된다[3]. NVisionIP는 드릴다운 기능을 통하여 전체 관리 네트워크를 감시하면서 이상 현상이 발견 되는 경우 상세한 화면으로 이동하는 기능을 제공한다. 하지만 관리 대상이 되는 B클래스 네트워크에 초점을 맞추고 있기 때문에 트래픽의 근원지 및 근원지 포트 정보를 표현하지 못한다. 또한 한 화면에서 트래픽과 관련된 모든 정보를 표현하지 못하기 때문에

원하는 정보를 얻기 위해서는 다른 화면으로의 전환이 필요하며, 이는 관리자가 이상 현상을 파악하는데 소요되는 시간을 증가시키는 요인이 된다.

VisFlowConnect-IP는 트래픽의 세션 정보에 초점을 맞추고 있으며, 데이터를 송신하는 근원지를 표현하는 축, 관리 도메인의 호스트를 표현하는 축, 데이터를 수신하는 목적지를 표현하는 축으로 구성된 평행축(Parallel Axis)을 사용하여 사전 정의된 임계치를 초과하는 트래픽에 대해서 연결선을 표현하는 방법을 사용하였다[4]. VisFlowConnect-IP는 내부 도메인과 외부의 인터넷 도메인간의 연결 정보를 보여주는 External View, 전체 외부 도메인 중 선택된 도메인과 내부 도메인간의 연결 정보를 보여주는 Domain View, 내부 도메인의 호스트 간 연결 정보를 보여주는 Internal View 등으로 구성된다. 트래픽의 흐름을 나타내는 연결선의 경우 트래픽의 양이 많아질수록 어두운 색으로 표현되며, 연결선의 색은 사전에 정의된 도메인을 의미한다. VisFlowConnect-IP는 연결 정보에 초점을 맞추고 있어서 포트별 사용량, 포트의 연속성 등의 포트와 관련된 정보를 시각화하여 보여주지 못하며, 한 평행선에 호스트 및 도메인을 표현하기 때문에 특정 호스트 및 도메인을 직관적으로 인지하기 어렵다.

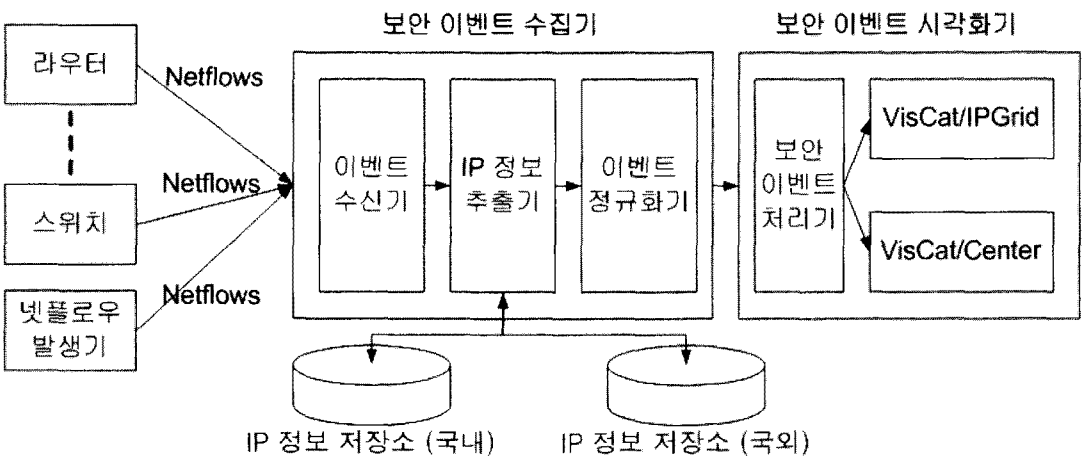
PortVis의 경우 시간에 흐름에 따른 포트 정보를 표현하는 기술로써, 특정 시간에 사용된 포트 별 트래픽의 양을 표현하는 화면을 제공한다[5]. 또한 화면에서 특정 시간의 특정 포트에 대한 트래픽의 통계 정보(세션의 수, 유일한 근원지의 수, 유일한 목적지의 수, 유일한 근원지와 목적지 쌍의 수, 유일한 근원지 국가의 수)를 선택하여 시간에 따른 흐름을 보여주는 화면을 제공함으로써, 네트워크의 비정상적인 현상을 쉽게 검출 할 수 있다. 하지만 통계 정보만을 사용하여 시각화하기 때문에 트래픽의 흐름을 보여주지 못하며, 정확한 근원지 및 목적지의 주소를 인지할 수 없다. 따라서 이상 현상의 상세한 분석을 위해서는 보안 이벤트의 원본 데이터에 접근해야 하는 문제점이 있다.

## III. 시각화 기반의 효율적인 보안 상황 분석 방법

네트워크상에서 발생되는 공격으로는 서비스 거부 공격, 분산 서비스 거부 공격, 인터넷 웜, 호스트 스캔, 포트 스캔 등이 있으며, 이들 공격 중 대부분은 보안 이벤트를 구성하는 요소 중 5-tuple(근원지 IP 주소, 근원지 포트, 프로토콜, 목적지 포트, 목적지 IP 주소)을 변화시키면서 공격하기 때문에 다양한 공격을 모두 인지 하기 위해서는 5-tuple을 효과적으로 시각화하는 것이 필요하다. 분산 서비스 거부 공격 또는 서비스 거부 공격의 경우 근원지 IP 주소와 목적지 IP 주소의 분포, 공격에 사용되는 목적지 포트, 특정 목적지 IP에 대한 트래픽의 집중도 등이 공격을 판단하는 데 있어 중요한 정보가 되며, 인터넷 웜의 경우 근원지 IP에서 발생시키는 트래픽의 양, 목적지 IP 주소의 분포, 목적지 포트 번호 등이 중요한 정보가 된다. 호스트 스캔의 경우 목적지 포트 번호 및 목적지 IP 주소의 분포가 중요한 정보가 되며, 포트 스캔의 경우 근원지 및 목적지 포트의 분포가 네트워크 공격 여부를 판단할 때 중요한 정보가 된다. 따라서 앞에서 기술한 공격들을 신속하게 인지하기 위해서는 5-tuple의 모든 정보를 한 화면에 효과적으로 표현하여 네트워크 관리자의 직관적인 인지력을 향상 시키는 방법이 필요하다. 하지만 기존의 방법들은 5-tuple 중 몇 가지 정보만을 사용하여 시각화하였기 때문에, 5-tuple 구성 요소간의 연결 정보를 통하여 파악할 수 있는 공격들을 신속하게 분석하는 것이 어려웠다. 또한 5-tuple의 모든 정보를 한 화면에 표현하는 경우 화면의 복잡해져 오히려 네트워크 관리자의 직관적인 인지력을 저하시키는 경우도 있다. 따라서 본 논문에서는 5-tuple의 정보와 IP 정보로부터 추출한 부가 정보를 효과적으로 시각화하여 다양한 네트워크 공격을 직관적으로 인지 할 수 있는 방법을 제안한다.

본 논문에서 제안하는 방법은 보안 이벤트를 구성하는 5-tuple 정보를 추출하여 보안 이벤트의 흐름을 한 화면에 시각화함으로써, 네트워크 관리자가 이상 현상을 유발하는 트래픽을 직관적으로 인지하고 분석하여 네트워크의 보안 상황을 보다 빠르고 정확하게 판단 할 수 있도록 하는 것이다. 또한 5-tuple을 구성하는 IP 주소로부터 지리적 위치, 소속 기관, 소속 국가 등의 부가 정보를 추출하여 트래픽 정보와 같이 표현함으로써 네트워크 관리자가 공격자 및 피해자의 상세 정보를 보다 빠르고 쉽게 인지 할 수 있도록 한다. 본 논문에서 제안하는 시각화 기반의 효율적인 네트워크 보안 상황 분석 방법의 구성도는 [그림 1]과 같다.

제안된 네트워크 보안 상황 분석 방법은 네트워크 장비 및 넷플로우 생성기로부터 트래픽 정보를 수집하여 부가 정보를 추출하는 보안 이벤트 수집기와 수집된 보안 이벤트의 5-tuple 정보와 부가 정보를 시각화하는 보안 이벤트 시각화기로 구성된다. 보안 이벤



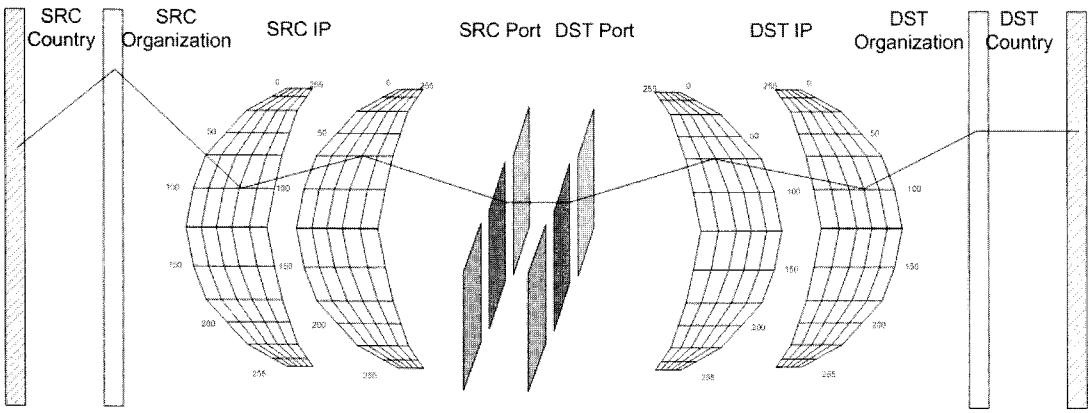

〔그림 1〕 제안된 네트워크 보안 상황 분석 방법 구조도

트 수집기는 UDP 통신을 통하여 넷플로우 정보를 수집하여 5-tuple 정보를 추출한 후, IP 정보와 IP 정보 저장소 저장되어 있는 IP 대역 정보를 매핑하여 관련된 정보를 추출하는 기능을 한다. IP 정보 저장소는 IP 대역별로 구분되어 있으며, IP 대역이 존재하는 물리적 위치(위도, 경도), IP 대역의 소유 국가, IP 대역의 ISP 등의 정보가 저장되어 있다. 제안된 방법은 IP 정보 저장소를 통하여 IP와 지리 정보를 매핑하게 된다. IP 정보 저장소의 경우 일반적으로 국외의 GeoIP〔14〕, IP2Location〔15〕 등의 데이터베이스가 많이 사용되고 있지만, 국내 IP 대역의 정보는 정확하지 못한 단점이 있다. 따라서 제안된 방법은 국내의 경우 자체 제작한 고정밀 데이터베이스〔16〕를 사용하며 IP정보와 지리 정보를 매핑하였으며, 국외의 경우 GeoIP 데이터베이스를 사용하여 지리 정보와 매핑하였다. 5-tuple 정보와 지리 정보를 비롯한 IP의 부가적인 정보는 정규화 되어 보안 이벤트 시각화기로 전달된다.

보안 이벤트 시각화기는 UDP 통신을 통하여 보안 이벤트 수집기로부터 정규화된 이벤트를 실시간으로 수신하며, VisCat/IPGrid와 VisCat/Center를 사용하여 이벤트를 표현하는 기능을 수행한다. 보안 이벤트 시각화기는 윈도우즈 환경에서 OpenGL을 사용하여 구현되었으며, 표현되는 이벤트의 관리는 원형 큐를 사용하여 큐의 저장공간이 부족할 때는 제일 먼저 입력되는 데이터가 삭제 되도록 하였다. VisCat/IPGrid와 VisCat/Center에서 화면의 갱신은 사용자가 설정한 갱신 시간과 이벤트의 수를 사용하여 갱신 시간이 초과되거나 설정된 수만큼의 이벤트가 입력되면 화면이 갱신되도록 하였으며, VisCat/IPGrid와 VisCat/Center에 대해서는 다음 장에서 자세히 살펴 볼 것이다.

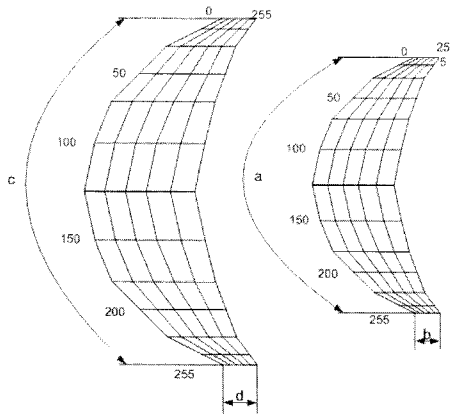
### 3.1 VisCat/IPGrid

기존의 보안 이벤트 시각화 기술은 주로 목적지 관리 도메인의 호스트 또는 B클래스 네트워크 내의 호스트를 대상으로 네트워크를 감시하였기 때문에, 근원지의 IP 주소 정보에 대한 정보를 제공해주지 못하였다. 또한 전체 관리 도메인을 표현하는 화면에서 호스트에 대한 정보는 통계 값으로 표현되기 때문에 이상 현상이 발생한 호스트를 찾기 위해서는 호스트의 정보를 상세하게 보여주는 또 다른 화면으로의 전환이 필요하였으며, 이는 네트워크 관리자가 보안 상황을 분석하는데 소요되는 시간을 증가시키는 요인이 되었다. 그리고 호스트 스캔과 같이 호스트 별로 소량의 트래픽을 생성되는 공격을 인지 할 수 없는 단점이 있었다. 따라서 본 논문에서는 근원지와 목적지의 전체 IP 주소 공간에서 트래픽 흐름을 감시하여 네트워크의 이상 현상을 보다 신속하게 분석할 수 있는 VisCat/IPGrid를 제안하였다. 제안된 방법은 근원지와 목적지의 전체 IP 주소 공간에서 발생하는 트래픽의 흐름을 시각화하여 호스트 스캔, 네트워크 스캔 등의 공격을 직관적으로 인지 할 수 있다. 또한 IP 주소로부터 추출된 소속 국가, 소속 기관의 정보를 화면상에 표현함으로써 네트워크 공격의 공격자 및 피해자에 대한 상세 정보를 한 화면에서 인지 할 수 있는 장점이 있다. VisCat/IPGrid의 화면 구성은 〔그림 2〕

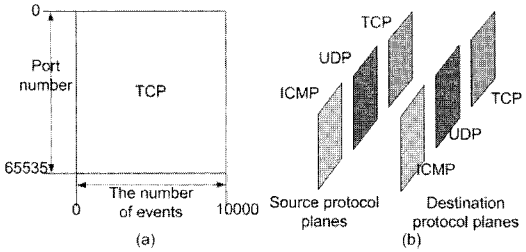



〔그림 2〕 VisCat/IPGrid 화면 구성

와 같다. 화면의 좌측은 근원지 IP 주소의 소속 국가, 소속 기관, IP 주소, 포트 정보를 나타내며, 화면의 우측은 목적지 IP 주소의 포트 정보, IP 주소, 소속 기관, 소속 국가 정보를 표현한다. 하나의 보안 이벤트는 근원지 국가부터 시작하여 목적지 국가까지 10개의 점, 9개의 선으로 매핑되며, 선의 색상은 보안 이벤트에서 사용된 목적지 포트 번호에 매핑된다. IP 주소 a.b.c.d를 표현하기 위해서 B클래스 네트워크(a.b)를 나타내는 그리드와 B클래스 네트워크에 매칭되는 한 호스트(c.d)를 나타내는 그리드를 사용하여 전체 IP 주소를 표현하였으며, 전체 IP 주소를 나타내는 IP 그리드는 〔그림 3〕과 같다. B클래스 네트워크를 나타내는 그리드 상의 한 점을 선택하거나, 호스트를 나타내는 그리드의 한 점을 선택하면 해당 B클래스 네트워크의 트래픽만을 필터링하며 화면상에 표시한다. 제안된 방법은 전체 IP 주소 공간에서 발생하는 보안 이벤트를 한 화면에서 감시함으로써, 호스트 스캔, B클래스 네트워크 스캔 등의 공격을 직관적으로 인지하고, 해당 보안 이벤트의 근원지 IP, 소속 국가, 소속 기관 및 사용되는 포트 등의 공격과 관련된 상세 정보들을 신속하고 정확하게 인지 할 수 있다. 본 논문에서는 다양한 프로토콜에서 발생하는 포트 별 이벤트를 모두 감시하기 위하여 다수의 프로토콜 평면으로 구성된 프로토콜 큐브를 제안하였으며, 〔그림 4〕와 같다. 〔그림 4(a)〕의 프로토콜 평면에서 세로축은 포트 번호를 의미하고 가로축은 해당 포트 번호에서 발생한 보안 이벤트의 수를 의미한다. 따라서 특정 포트 번호를 사용하는 공격 이벤트가 다수 발생하는 경우에, 프로토콜 평면에서 가로축으로 실선이 생기게 된다. 또한 포트 번호를 변경하는 포트 스캔 공격의 경우 세로축으로 실선이 생기게 됨으로 네트워크 관리자는 포트와 관련된 다양한 공격들을 직관적으로 인지할 수 있게 된다. 일반적으로 1024이하의 잘 알려진 포트 번호가 많이 사용되기 때문에, 1024 이하의 포트를 잘 보기 위하여 포트 번호를 나타내는 축은 지수함수적으로 증가하게 되어 있다. 〔그림 4(b)〕의 프로토콜 큐브는 근원지의 TCP, UDP, ICMP 프로토콜




〔그림 3〕 IP 그리드



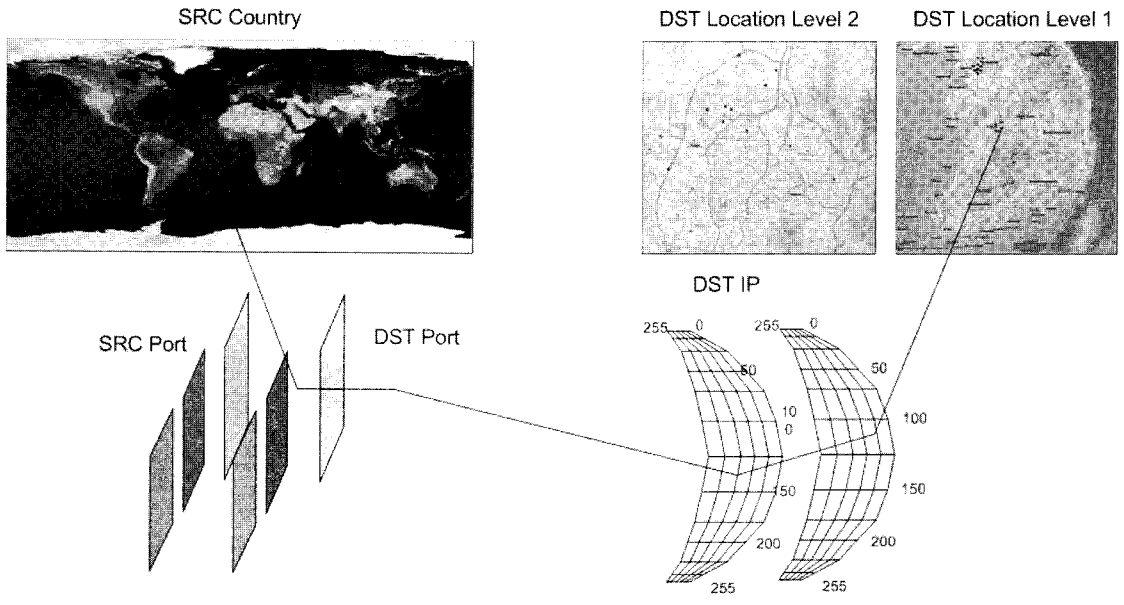

〔그림 4〕 (a) 프로토콜 평면 (b) 프로토콜 큐브

을 나타내는 세 개의 프로토콜 평면과 목적지의 TCP, UDP, ICMP 프로토콜을 나타내는 세 개의 프로토콜 평면으로 구성되어 있다. VisCat/IPGrid는 네트워크 관리자에게 화면의 전환 없이 보안 이벤트로부터 얻을 수 있는 모든 정보를 표현할 수 있으며 할 수 있으며, 이상 현상을 분석함에 있어 네트워크 관리자가 국가, B클래스 네트워크, 포트 번호, 이벤트 타입, 도메인 등을 선택하여 상세하게 분석할 수 있는 방법을 제공함으로써 네트워크의 보안 상황을 분석에 소요되는 시간을 줄일 수 있다.

### 3.2 VisCat/Center

전국 규모의 도메인을 관리하는 네트워크 관리자는 이상 현상이 일어난 지점을 파악하고 대응하기 위해서는 이상 현상이 발생한 지점의 논리적 위치인 IP 주소뿐만 아니라 실제 호스트가 존재하는 물리적 위치를 파악하는 것이 중요하다. 하지만 기존의 보안 이벤트 시각화 기술은 숫자로 구성된 IP 주소만을 화면에 표현하였기 때문에 네트워크 관리자가 이상 현상이 발생한 물리적 지점 및 논리적 지점을 파악하기가 어려웠다. 따라서 본 논문에서는 두 단계의 계층적인 지리 정보를 통해 호스트의 물리적인 위치를 표현함으로써 이상 현상이 발생한 호스트의 물리적 위치와 논리적 위치를 직관적으로 인지 할 수 있는 VisCat/Center를 제안하였다.

VisCat/Center는 [그림 5]와 같이 IP 그리드와 두 단계의 계층적인 지리 정보를 통하여 한 화면에서 관리 도메인 내의 호스트의 IP 주소 및 물리적인 위치를 모두 표현할 수 있다. 제안된 방법의 경우 근원지를 세계 지도에 매핑하여 어떤 국가에서 보안 이벤트가 발생되었는지를 표현하였다. 이는 일반적인 네트워크 관리자의 경우에는 이상 현상을 유발한 공격자 보다 네트워크 공격으로부터 관리 도메인의 피해를 줄이기 위해서 관리 도메인 내의 피해 호스트에 더 관심을 갖기 때문이다. VisCat/Center에서 근원지와 목적지의 포트 정보를 표현하기 위해 VisCat/IPGrid에서 사용한 프로토콜 큐브를 사용하였으며, 목적지의 IP 주소를 표현하기 위해서 IP 그리드를 사용하였다. 따라서 VisCat/IPGrid에서 탐지 할 수 있었던 호스트 스캔, 포트 스캔 등의 다양한 네트워크 공격을 네트워크 관리자가 직관적으로 인지 할 수 있다. 또한 목적지 IP 주소의 물리적인 위치는 두 단계의 레벨로 위치를 표현하여, 레벨 1의 지도에서 전체 관리 도메인의 현황을 보여주고 레벨 2의 지도에서는 레벨 1에서 선택된 특별시 및 광역시도의 지역을 상세하게 보여줌으로써 호스트의 물리적 위치에 대한 네트워크 관리자의 직관적인 인지력을 향상 시킬 수 있었다. 또한 목적지 기관의 물리적 위치와 기관의 명칭을 화면상에 표현함으로써, 네트워크 관리자는 이상 현상이 발생한




[그림 5] VisCat/Center 화면 구성

호스트의 물리적 위치를 보다 신속하고 정확하게 인지 할 수 있다. VisCat/Center는 한 화면에서 관리 도메인의 논리적 위치 정보인 IP 주소와 물리적 위치 정보인 지리 정보를 동시에 표현함으로써, 네트워크 관리자로 하여금 네트워크 공격이 발생한 피해자의 물리적 위치와 논리적 위치를 신속하게 인지 할 수 있다는 장점이 있다.

## IV. 실험 결과

이 장에서는 본 논문에서 제안된 시각화 기반의 효율적인 네트워크 보안 상황 분석 방법의 성능을 확인하기 위해여 다음 〔표 1〕의 데이터를 사용하여 시험하였다. 시험에 사용된 데이터는 트래픽 미터링 데이터인 Netflow(v5) 데이터로써, 한국과학기술정보연구원의 Kreonet 망에서 각각 5분 동안 수집한 데이터이다.

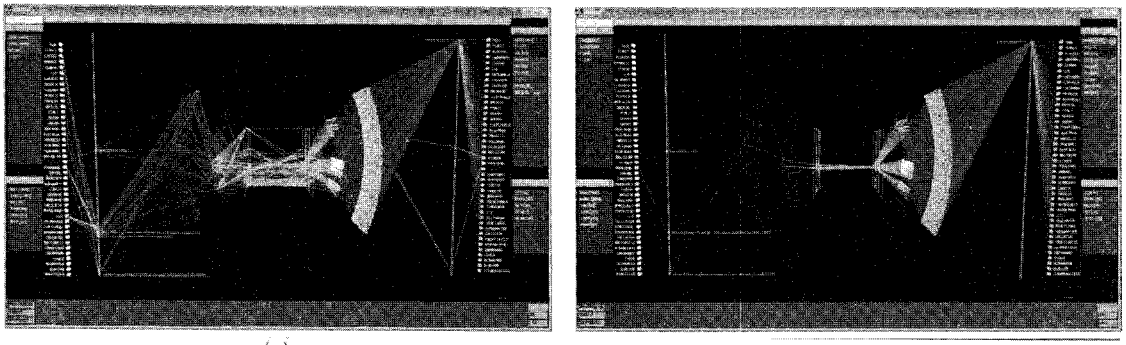
〔표 1〕 실험 데이터

| 파일명 | 이벤트 수 | 파일 크기 | 설명 |
|---|---|---|---|
| N07270701 | 703,331 | 55M | 1434 슬래머 웜 |
| N07200703 | 73,572 | 6M | 호스트 스캐닝 |

〔그림 6〕은 N07200703 데이터를 사용하여 제안된 방법으로 시각화한 모습이다. 〔그림 6(a)〕를 보면 녹색으로 매핑된 1434 포트를 사용하는 트래픽이 다양한 B클래스 네트워크의 전체 호스트로 향하고 있음을 인지 할 수 있다. 〔그림 6(b)〕는 목적지 포트가 1434인 트래픽 데이터만 필터링하여 시각화한 화면의 모습이다. 목적지 포트 1434를 가지는 트래픽의 경우 두 개의 호스트에서 발생함을 확인 할 수 있으며, 호스트의 소속 기관 및 소속 국가도 알 수 있다. 이와 같이 특정 몇몇의 호스트로부터 전체 IP대역으로 방대한 양의 트래픽이 발생하는 것은 웜으로 판단 할 수 있다. 기존의 NVisionIP, VisFlowConnect-IP 경우 전체 IP 주소 공간을 감시하지 않고 특정 B클래스 네트워크만을 감시하기 때문에 특정 호스트에서 전체 네트워크로 랜덤하게 발생되는 웜 트래픽의 패턴을 인지 할 수 없으며, PortVis의 경우 1434 포트에 대한 통계 정보를 사용하여 이상 현상의 여부를 알 수 있지만 웜 트래픽인지를 확인 할 수 없는 단점이 있다.

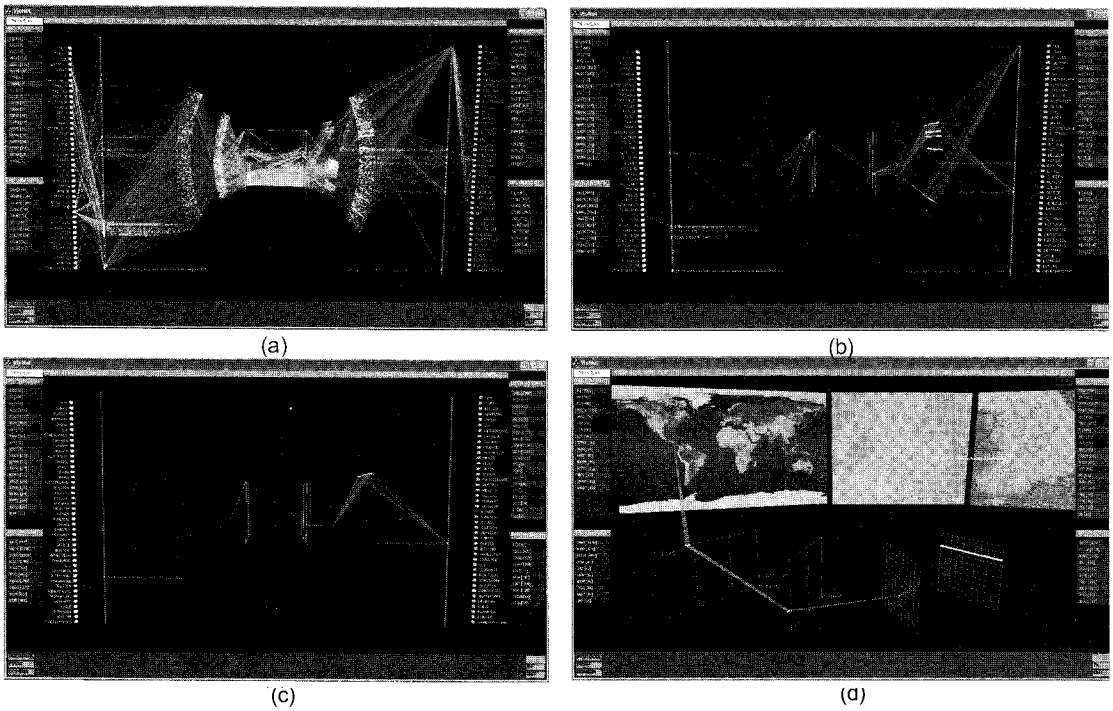
〔그림 7〕은 N07270701 데이터를 시각화한 모습으로써, 〔그림 7(a)〕를 보면 다양한 공격이 혼재하고 있음을 알 수 있다. 시각화 화면의 우측에 표현되는 빈도수가 높은 목적지 포트 창에서 현재 트래픽 중에서는 목적지 포트 2048이 가장 많이 사용되고 있음을 알 수 있다. 해당 포트를 선택하면 〔그림 7(b)〕와 같이 해당 포트를 사용하는 트래픽만을 필터링하여 시각화하며, 현재 호스트 스캐닝 공격이 이루어지고 있음을 인지할 수 있다. VisNet/IPGrid 또는 VisNet/Center 화면에서 IP 주소를 표현하는 IP 그리드에서 일렬로 선이 생기는 것은 IP 주소 대역을 순차적으로 변경하면서 동일한 트래픽을 유발하는 것임으로 호스트 스캔이라고 할 수 있다.

〔그림 7(c)〕는 동시에 발생되고 있는 호스트 스캐닝 공격 중 그 피해 호스트가 한국인 경우만을 보여주며, 네트워크 관리자는 해당 공격을 수행하는 공격자의 IP 주소, 소속 기관, 소속 국가, 사용하는 근원지 포트 등 네트워크 공격 여부를 판단하기 위해서 필요한 모든 정보들을 얻을 수 있다. 〔그림 7(d)〕는 동일 공격을 VisNet/Center의 화면으로 시각화한 모습이다. VisNet/Center의 화면을 통해서 네트워크 관리자는 현재 진행 중인 호스트 스캔 공격이 어떤 IP



(a) (b)

〔그림 6〕 1434 슬래머 웜 (a) VisNet/IPGrid 화면 (b) VisNet/IPGrid의 1434 근원지 포트 선택 화면



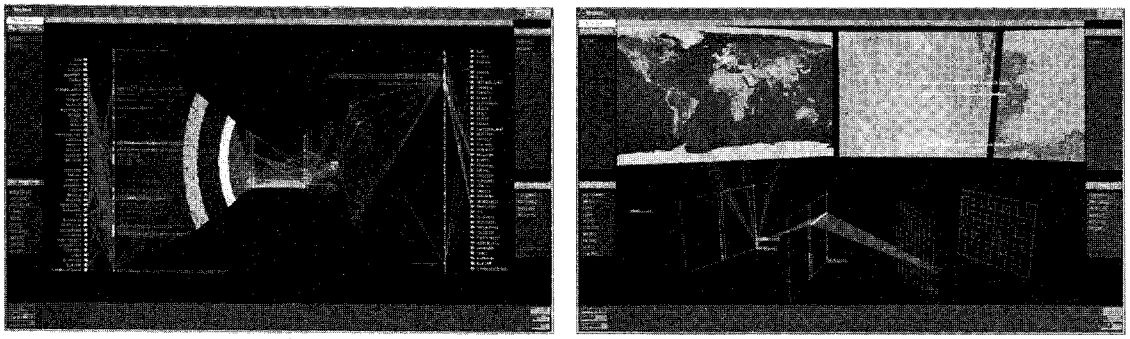

〔그림 7〕 호스트 스캔 공격 탐지 (a)VisNet/IPGrid 화면 (b) VisNet/IPGrid의 2048 포트 선택 화면
(c) VisNet/IPGrid의 근원지 국가 선택 화면 (d) VisNet/Center 화면

범위를 스캔 하는지, 해당 IP가 속한 기관과 기관의 물리적 위치 등을 직관적으로 인지 할 수 있다. NVisionIP의 경우 근원지 IP와 목적지 IP간의 연결 정보를 표현하지 않기 때문에 동일한 공격자로부터 발생되는 트래픽임을 확인하는 별도의 과정이 필요하여 호스트 스캔으로 판정하는 데 시간이 많이 소요된다. VisFlowConnect-IP의 경우 Global View를 통하여 호스트 스캔이 현재 네트워크에서 발생하고 있음을 확인할 수 있지만, 호스트 스캔의 공격자 IP 주소를 알기 위해서는 Global View에서 Domain View로 화면을 전환해야하는 문제점이 있다. PortVis의 경우도 특정 시간에 따른 포트 별 트래픽의 양을 표현하기 때문에 호스트 스캔 현상을 직관적으로 인지하기 어려우며, 보다 상세한 분석을 위하여 원본 트래픽 데이터에 접근해야한다는 문제점이 있다.

〔그림 8〕은 네트워크 공격 패킷 생성 툴로 분산 서비스 거부 공격 패킷을 생성하였을 때 제안된 방법에서 표현되는 네트워크 트래픽의 모습이다. 〔그림 8(a)〕를 보면 분산 서비스 거부 공격의 경우 근원지 IP의 경우가 랜덤하게 생성되고, 특정 호스트들로 트래픽이 집중되기 때문에 근원지 IP를 나타내는 평면이 흰색으로 가득 차 있고, 두 ISP의 특정 호스트로 트래픽이 집중되고 있음을 알 수 있다. 〔그림 8(b)〕를 보면 분산 서비스 거부 공격 트래픽을 나타내는 적색 선들이 향하는 목적지의 IP 주소 뿐만 아니라 해당 IP가 존재하는 물리적 위치까지 직관적으로 인지 할 수 있다.

NVisionIP의 경우 근원지 IP와 목적지 IP간의 연결 정보를 표현하지 않기 때문에 어떤 공격자로부터 트래픽이 발생하는지를 인지 할 수는 없지만, 네트워크에 이상 현상이 발생한 것을 알 수 있다. 하지만 네트워크 공격자를 찾기 위해서는 트래픽 데이터를 검색하는 과정이 필요하다. VisFlowConnect-IP의 경우 Global View를 통하여 분산 서비스 거부 공격이 현재 네트워크에서 발생하고 있음을 확인 할 수 있지만, 피해자의 IP 주소를 알기 위해서는 Global View에서 Domain View로 화면을 전환해야하는 문제점이 있다. PortVis의 경우도 특정 포트로 트래픽이 과다하게 흐르고 있음을 직관적으로 인지 할 수는 있지만, 분산 서비스 거부 공격으로 판단하기에는 근원지 IP 주소의 분포를 알 수 없기 때문에 어려움이 있다.

제안된 방법은 네트워크 관리자가 현재 네트워크에



(a) (b)

〔그림 8〕 분산 서비스 거부 공격 탐지 (a) VisNet/IPGrid 화면 (b) VisNet/Center 화면

서 발생하고 있는 이상 현상을 신속하게 인지하고 네트워크 공격 여부를 판단할 수 있도록 하기위하여 네트워크에서 발생하는 트래픽의 흐름을 직관적으로 인지할 수 있도록 시각화하였다. 또한 IP 정보 이외에 소속 기간, 소속 국가 및 물리적 위치를 화면상에 같이 표현하여 네트워크 관리자가 피해자의 정보를 빠르게 인지하고 네트워크 공격에 신속하게 대응함으로써 공격에 대한 피해를 최소화 시킬 수 있다. 하지만 제안된 방법의 경우 트래픽의 흐름을 표현하기 때문에 5-tuple간의 정보를 연결하기 위한 선이 많이 생겨 프로토콜 큐브에서 특정 호스트에 대해서 소량의 트래픽이 발생되는 포트 스캔이 연결선에 가려져서 인지하기 어려운 단점이 있다. 또한 근원지 IP 주소까지 표현함으로써 네트워크 공격자의 IP 주소를 직관적으로 인지 할 수 있다는 장점이 있지만, IP 주소를 스푸핑하면서 수행되는 네트워크 공격의 경우 네트워크 관리자가 근원지 IP 주소를 인지하는 것이 의미가 없을 수 있다.

## V. 결 론

네트워크 관리자가 침입 탐지 시스템, 방화벽 등의 보안 장비에서 발생하는 경보 메시지를 통하여 네트워크에서 이상 현상이 발생하였는지를 인지하고, 이상 현상이 실제 네트워크 보안 위협인지를 판단하기 위해서는 경보 메시지와 관련된 트래픽을 검색하고 분석하는 등의 일련의 작업이 필요하다. 본 논문에서는 네트워크 관리자가 트래픽을 검색하고 분석하여 네트워크의 보안 상황을 분석하는데 소요되는 시간을 줄일 수 있는 시각화 기반의 효율적인 네트워크 보안 상황 분석 방법을 제안하였다. 제안된 방법은 전체 IP 주소 공간을 감시하는 VisNet/IPGrid와 지리 정보와 연계해 관리 호스트의 물리적 위치까지 표현하는 VisNet/Center로 구성되어 있으며, 기존의 방법들과 달리 보안 이벤트를 구성하는 5-tuple의 정보를 IP 주소를 표현하는 IP 그리드와 프로토콜 및 포트 번호 별 빈도수를 표현하는 프로토콜 큐브를 사용하여 한 화면상에 표현함으로써 네트워크 관리자가 보안 상황을 분석하는데 있어 필요한 모든 정보를 제공해 준다. 또한 네트워크 관리자가 다양한 네트워크의 공격 패턴을 직관적으로 인지 할 수 있도록 시각화하며, 네트워크 공격의 공격자 및 피해자에 관련된 정보, 관리 도메인 내 존재하는 피해자의 물리적 위치 정보 등의 정보를 신속하게 파악 할 수 있는 장점이 있다. 본 논문에서 제안된 방법을 사용하면 네트워크 관리자는 관리 네트워크에서 발생되는 보안 위협을 보다 빠르게 판단하여 공격에 대응하는 시간을 줄일 수 있을 것으로 기대된다.

본 논문에서 제안된 방법의 경우 보안 이벤트의 정보를 3D 화면상에서 선을 통하여 시각화하기 때문에 초당 처리할 수 있는 이벤트 수의 제약이 있으며, 이에 대한 개선이 필요하다. 또한 보안 장비로부터 발생된 경보 데이터 중 5-tuple의 정보가 완전하지 않는 경우에도 경보 데이터를 시각화할 수 있는 방법에 대한 연구가 더 필요하다.

## 참 고 문 헌

〔1〕 G. Fink, R. Ball, N. Jawalkar, C. North, and R. Correa, "Network Eye: End-to-End Computer Security Visualization," Submitted for Consideration at ACM CCS

Workshop on Visualization and Data Mining for Computer Security (VizSec/DMSec), Oct. 2004.

[2] 장범환, 나중찬, 장종수, "보안 이벤트 시각화를 이용한 보안 상황 인지 기술," 정보보호학회지, 16(2), pp. 18-25, 2006년 4월.

[3] K. Lakkaraju, W. Yurcik, and A.J. Lee, "NVisionIP: Netflow Visualizations of System State for Security Situational Awareness," In Proc. of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, ACM Press, New York, NY, USA, pp. 65-72, Oct. 2004.

[4] X. Yin, W. Yurcik, and A. Slagell, "The Design of VisFlowConnect-IP: A Link Analysis System for IP Security Situational Awareness," Third IEEE Int'l Information Assurance Workshop, University of Maryland, pp. 23-24, Mar. 2005.

[5] J. McPherson, K. Ma, P. Krystosek, T. Bartoletti, and M. Christensen, "PortVis: A Tool for Port-Based Detection of Security Events," Proc. of VizSEC'04, ACM Press, pp. 73-81, Oct. 2004.

[6] S. Lau, "The Spinning Cube of Potential Doom," Communications of the ACM, vol. 47, no. 6, pp. 25-26, June 2004.

[7] K. Abdullah, C. Lee, G. Conti, J. Copeland, and J. Stasko, "IDS RainStorm: Visualizing IDS Alarms," Proc. of VizSEC'05, IEEE, pp. 1-7, Oct. 2005.

[8] S. Krasser, G. Conti, J. Grizzard, J. Gribschaw, and H. Owen, "Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization," Proc. of sixth IEEE Systems, Man and Cybernetics Information Assurance Workshop, pp. 42-49, June 2005.

[9] G. Conti and K. Abdullah, "Passive Visual Fingerprinting of Network Attack Tools," Proc. of VizSEC'04, ACM Press, pp. 45-54, Oct. 2004.

[10] H. Koike and K. Ohno, "Snortview: Visualization system of snort logs," Proc. of VizSEC'04, ACM Press, pp. 143-147, Oct. 2004.

[11] SecureScope, http://www.SecureDecisions.com/

[12] R. Erbacher, K. Christensen, and A. Sundberg, "Designing Visualization Capabilities for IDS Challenges," Proc. of VizSEC'05, IEEE, pp. 121-128, Oct. 2005.

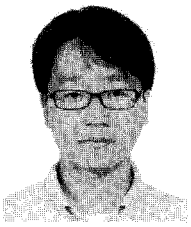
[13] A. Oline and D. Reiners, "Exploring Three-Dimensional Visualization for Intrusion Detection," Proc. of VizSEC'05, IEEE, pp. 113-120, Oct. 2005.

[14] GeoIP, MaxMind's IP Intelligence Solution, http://maxmind.com/

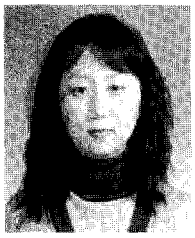
[15] IP2Location, http://www.ip2location.com

[16] 장범환, 정치윤, 손선경, 나중찬, "고정밀 수치지형도를 활용한 네트워크 보안상황인지 기술," 제12회 차세대 통신소프트웨어 학술대회, pp. 210-215, 2008년 12월.

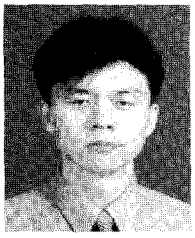
## 〈著者紹介〉



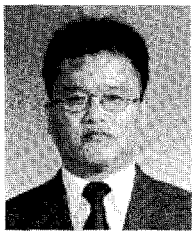
정 치 윤 (Chi Yoon Jeong) 정회원
2002년 2월: 포항공과대학교 전자전기공학과 졸업
2004년 2월: 포항공과대학교 전자전기공학과 석사
2004년 3월~현재: ETRI 보안관제기술연구팀 연구원
〈관심분야〉 네트워크 보안, 네트워크 트래픽 분석, 컴퓨터 비전



손 선 경 (Seon Gyoung Sohn) 정회원
1999년 2월: 전남대학교 전산학과 졸업
2001년 2월: 전남대학교 전산학과 석사
2001년 3월~현재: ETRI 보안관제기술연구팀 선임연구원
〈관심분야〉 네트워크 보안, 네트워크 트래픽 분석, 보안 상황인지



장 범 환 (Beon Hwan Chang) 정회원
1997년 2월: 성균관대학교 전자공학과 졸업
1999년 2월: 성균관대학교 전자및컴퓨터공학과 석사
2003년 2월: 성균관대학교 전자및컴퓨터공학과 박사
2003년 3월~현재: ETRI 보안관제기술연구팀 선임연구원
〈관심분야〉 네트워크 보안, 보안 상황인지, 네트워크 공격상황 분석



나 중 찬 (Jung Chan Na) 정회원
1986년 2월: 충남대학교 계산통계학과 졸업
1989년 2월: 숭실대학교 전자계산학과 석사
2004년 2월: 충남대학교 컴퓨터과학과 박사
1989년 3월~현재: ETRI 보안관제기술연구팀 팀장
〈관심분야〉 네트워크 보안 관리, 보안 상황인지, 네트워크 트래픽 분석