주소기반 분류기법을 통한 효과적인 침입상황 분석 도구

전남대학교 김민수 · 노봉남
국가보안기술연구소 서정택 · 박응기

1. 서 론

사이버 범죄로부터 시스템과 네트워크를 보호하기 위해 침입탐지 시스템이 연구되어 왔다. 침입탐지 시스템은 일반적으로 정해진 규칙을 사용하며 탐지 척도에 따라 다양한 결과를 나타낼 수 있다. 현재 알려진 침입탐지 시스템은 서로 다른 척도와 규칙을 사용함에 따라 침입경보가 다양하게 나타난다. 또한, 침입정보를 놓치지 않으려고 너무 많은 침입경보를 발생시킴으로써 보안 관리자에게 엄청난 부담을 주게 된다. 이러한 문제로 인하여 침입탐지 경보를 축약하는 방법과 침입상황을 쉽게 분석하는 방법에 관심이 많아지고 있다.

침입경보를 축약하고 침입상황을 분석하는 대표적인 방법은 ACC에서 찾아볼 수 있다. ACC는 침입경보의 3가지 속성(공격유형, 근원지 IP, 목적지 IP)에 대한 비교 결합으로 축약하며 축약된 정보를 상황으로 표현하여 관리자가 공격의 상황을 쉽게 인식할 수 있도록 하였다. 이러한 방법은 침입경보를 추상화된 상황 클래스로 표현함으로써 축약율과 상황 분류는 뛰어나지만, 협동 공격을 잘 표현하지 못하고 공격의 흐름을 설명하기 부족하다. 이러한 면은 관리자가 축약되기 전의 정보를 재분석해야한다는 부담을 주게 된다.

본 논문에서는 주소기반 분류기법을 제시하고 이러한 방법을 통하여 효과적으로 침입상황을 분석할 수 있음을 보여주고자 한다. 속성 비교에 의한 축약에 의존하지 않고 공격 특성별로 분류하고 주소별로 구분하여 보여줌으로써 공격 경로와 방법을 쉽게 보여줄 수 있도록 한다. 공격 사이의 관계를 흐름으로 보여주어 관리자가 쉽게 공격상황을 파악할 수 있고, 자료의 재분석의 부담을 덜어주게 된다.

2. 관련연구

2.1 침입탐지 방법과 침입경보의 축약

현재의 침입탐지 시스템은 전문가의 경험적 지식을 규칙으로 만들어 정확하게 탐지하도록 하는 오용탐지 기법을 사용한 것이 대부분이다. 오용탐지 방법은 알려지고 분석된 공격에 대하여 정확한 결과를 낼 수 있다. 그러나 비슷한 유형의 공격에 대하여 반응하지 못하거나 다양한 형태로 경보를 발생시킬 수 있다. 이러한 불특정적인 행위를 탐지하기 위해 데이터마이닝이나 통계학과 같은 이론을 적용한 비정상행위 탐지 방법도 발표되었지만 정확성이 떨어져 기피되고 있다[1].

다양한 형태의 침입탐지 시스템은 다양한 형태의 경보를 발생하게 되고 이러한 경보 사이의 호환성 문제도 침입탐지 시스템의 결과를 분석하는데 어려움을 주게 된다. 임의의 공격에 대해 각 탐지 시스템이 다수의 관련된 경보 메시지를 발생시키지만, 논리적으로 결합시키는 방법이 제시되지 않아 잘못된 탐지결과를 발생시키는 원인이 되기도 한다. 또한, DDoS와 같은 대량의 패킷을 발생시키는 공격은 침입탐지 시스템에도 영향을 끼쳐서 대량의 경보 메시지를 발생시키게 한다. 그 결과로 보안 관리자는 대량의 경보에서 침입의 상황을 분석해야만 하는 어려움에 직면하게 된다[2].

결국 대량으로 발생하는 침입경보에 대한 축약과 이종 시스템 또는 변형된 공격의 침입경보의 통합하는 문제는 현재의 침입탐지 시스템의 당면 과제가 되었다. 이러한 침입탐지시스템들의 탐지결과를 통합하고 판정하기 위한 대표적인 연구로서 TEC[3]과 EMERALD가 있다[4,5,6].

TEC(Tivoli Enterprise Console)은 호스트 및 네트워크 기반의 침입탐지 시스템의 결과를 통합(aggregation)하고 각 탐지결과 메시지의 관련성을 분석하여 관리자에게 압축된 결과를 보고하는 체계를 갖는 시스템이다. TEC은 침입 데이터의 수집, 형식화 및 분석, 진단, 그리고 탐지결과 메시지를 보이는 기능을 하는 프로브(probe)가 있으며, 통합 및 관련성 분석 콘솔(Aggregation & Correlation Console : ACC)은 프로브 결과의 수집, 분석, 압축된 탐지결과 메시지를 관리자에게 제시하는 기능을 한다. TEC은 통합탐지를 통한 경보의 보고를 줄이고 오판율을 감소하기 위해 경보

들의 관련성을 호스트 주소, 목적지주소, 경보를 이용하여 7가지의 상태로 그룹화한다. 그룹화하는 단계는 경보에 대한 기본 정보를 생성하는 프로브 계층, 다중의 목적지 주소를 갖는 메시지를 분석하는 목적지 계층, 메시지 발생의 호스트 주소가 실제 주소인지 분석하는 근원지 계층, 목적지의 서비스 이용을 분석하는 상세 목적지 계층으로 이루어진다. 각 계층 그리고 계층 사이에는 중복된 관계인지 또는 이전의 사건과 연결되는 관계인지를 보이는 방법으로 분석하고 있으며, 사용자 세션에 대한 행위 프로파일 분석이 필요하다.

EMERALD는 네트워크 서비스의 실시간 보호를 제공하기 위해 통계학적인 프로파일과 서명 분석을 결합한 능률적인 침입탐지 기능을 제공하며, 광범위한 침입탐지 기능과 네트워크에서 일어날 수 있는 중요한 공격에 대한 대응 능력을 제공하기 위해 분산되어 있는 모니터의 분석을 종합하는 프레임워크 개념을 도입하여 개발하고 있다. EMERALD는 각 다중 탐지 시스템들의 탐지 메시지의 교환을 위해 경보 템플리트(alert template)를 이용하고 있으며, 이 템플리트에는 탐지 시스템의 유형, 위치, 공격의 목표, 그리고 정상 및 비정상의 행위 표시 필드를 포함하고 있다. 또한, 메타 경보(meta alert)에서는 공격에 대하여 다른 길이의 패턴 비교, 비교된 특징의 수량 및 질, 비교된 횟수, 경보의 특성을 비교하여 경보들 간의 유사성을 정의하고 있다. EMERALD의 특징은 메타메시지의 통합에 의해 기존의 경보와 새로운 경보 사이의 유사가능성(expectation of similarity)을 찾아 관련 정도를 표현한다. 각 경보의 유사가능성은 비교되는 특징들의 정도에 의해 나타나게 되며, 두 개의 경보 사이의 유사가능성은 베이지안 통계에 의해 표현한다. EMERALD는 경보의 관련성을 사건의 클래스에 따른 유사가능성으로 표현하였으며, 이를 위한 메타 경보의 구성 및 사건의 분류는 호스트의 감사로그, TCP 연결 등의 저수준 사건을 통합하고, 다음 단계에서는 동일한 행위에 대해 하나의 탐지센서가 다른 탐지센서의 상태를 인지하여 다수의 경보를 하나의 메시지로 통합하며, 마지막으로 각 센서의 탐지 메시지를 통합하는 단계의 절차를 수행한다.

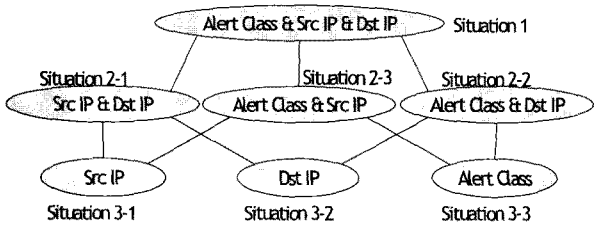


그림 1 ACC에서 사용한 집단화 레벨과 상황 클래스

2.2 침입상황 분석 방법

대량의 경보가 발생하는 상황에서 침입상황을 쉽게 분석하기 위해서 여러 가지 축약 방법이 제시되었다. ACC에서는 7가지 상태를 정의하고 그 특성에 따라 축약하여 침입 상황을 보여준다. 즉, 그림 1에서 볼 수 있듯이 경보의 클래스, 목적지 주소(destination address), 발신지 주소(source address)에 따라 결합을 수행하여 단순화된 상황으로 보여준다. 이러한 방법은 빠른 시간 내에 대량의 경보를 상황으로 분류하여 현재 발생한 침입 경보의 성향 파악을 쉽게 한다.

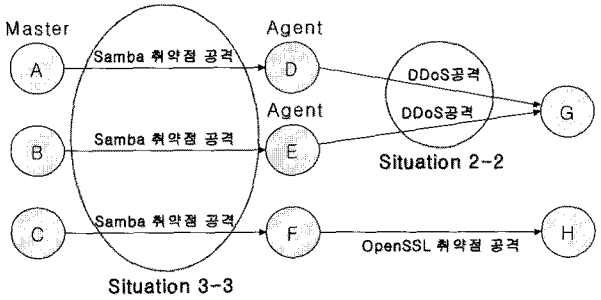


그림 2 DDoS 공격에 숨어있는 징검다리 공격

단순한 결합에 의한 상황 분류 방법은 침입상황을 간단한 형태로 보여주는 장점이 있지만 복합적인 공격을 분석하거나 공격 흐름을 파악하기에는 추가적인 노력을 필요로 하게 된다. 즉, 결합에 의해 축약되기 전의 원래 경보를 분석해야만 된다는 것이다. 예를 들어, 그림 2의 경우처럼 G 시스템으로의 Samba 취약점에 의한 R2L 공격으로 DDoS 에이전트를 설치하고 마지막에 G 시스템으로 DDoS 공격을 하는 상황과 H 시스템으로 OpenSSL 취약점에 의한 R2L 공격이 동시에 발생하였다고 하자. 즉, DDoS로 관리자의 눈을 현혹시키고 실질적으로는 H 시스템에 침입하고자 하는 상황이다. 이 예에서 ACC와 같은 방식은 Samba 취약점을 이용한 공격을 하나로 결합하고 DDoS 공격을 하나로 결합한 결과만을 보여주게 된다. 즉, H 시스템에 침입하는 공격 흐름은 다른 상황으로 포함되어 버리는 결과로 나타난다. 물론 결합되기 전의 정보를 살펴보면 공격을 찾을 수도 있겠지만, 그 정보를 분석하려고 쉽게 결정하기 않을뿐더러 추가적인 비용이 요구된다. 따라서 이러한 예에서도 공격흐름을 정확히 집어낼 수 있는 방법이 필요하게 된다.

3. 공격흐름 분석 방법 제안

3.1 IP 주소 기반의 방법

공격자를 파악하기 위해서는 일반적으로 공격자 IP

주소를 찾아가는 방식을 사용한다. 흔히 징검다리 공격(stepping stone attack)은 공격자가 최종 목적지에 침투하기 위해 여러 시스템을 징검다리처럼 점령해 나가는 것을 말한다. 이러한 공격 흐름 파악은 징검다리가 된 시스템 사이의 침입 경보를 분석함으로써 이루어질 수 있다. IP 기반으로 공격흐름을 파악하는 또하나의 장점은 Probe나 DoS와 같은 공격 행위도 ACC에서 집단화에 사용한 것처럼 IP 기반 특성으로 쉽게 분류할 수 있다는 것이다.

본 논문에서는 기존 연구의 문제점을 보완하면서 목적지 주소 중심의 상황분석 방법을 제안한다. 제안한 방법은 중요한 공격 흐름 정보를 보장하기 위하여 최소한 침입경보 속성 3개가 일치하는 상황 클래스만을 적용하여 침입경보 축약을 수행한다. 침입경보 중에서 공격 이름, 발신지 주소, 목적지 주소, 서비스 종류 중에서 3가지가 일치하는 경우를 집단화 가능하다고 판단하고 집단화를 수행한다. 더 적은 상황 클래스를 이용하여 집단화를 수행함에 따라 다소 축약율이 떨어지지만, 데이터마이닝의 연관규칙을 이용하여 공격타입이 서로 다른 침입경보도 축약이 가능하도록 함으로써 축약율 감소를 보완한다.

3.2 공격 사이의 관련성 분석

데이터마이닝의 연관규칙은 알려진 사실로부터 연관된 패턴을 찾는데 유용한 기법으로 알려져 있으므로, 공격타입이 서로 다른 침입경보에 대해 연관성 분석을 수행한다면 다수의 침입경보를 대체하는 축약 효과가 있고 상황분석에 용이한 고수준의 침입정보 생성이 가능하다. 연관성 분석은 미리 오프라인에서 학습 데이터를 통하여 축약을 수행하는 연관규칙을 생성하고, 실시간으로 발생되는 침입경보에 대해 연관규칙을 적용하여 이루어진다. 또한, 연관성 분석에 데이터마이닝 기법을 사용하므로, 변형된 공격에 대한 연관성 분석도 용이하다.

또한 본 논문에서는 침입상황에 대한 파악이 용이하도록 축약과 연관성 분석으로 생성된 고수준의 침입정보를 이용하여 상황분석을 수행한다. 상황분석 단계에서는 목적지 주소별로 침입경보를 그룹화하고, 그룹화된 침입경보를 9가지의 공격유형으로 나눈다. 9가지 공격유형은 IP 스캔, 포트 스캔, 취약점 스캔, 서비스 거부 공격(DoS: Denial of Service), 분산 서비스 거부 공격(DDoS: Distributed DoS), 웜 바이러스 공격, 원격 공격(R2L: Remote-To-Local), 정보유출 공격, 추측 공격이다. 이렇게 분류된 침입경보의 출발지 주소를 따라 관련된 침입경보를 연결시키고, 침입흐름을 제시한다.

3.3 공격의 흐름 분석

상황분석을 통해 우선적으로 파악하고자 하는 것은 공격하는 호스트와 공격당하는 호스트의 구분이다. 이뿐만 아니라 어떠한 공격성향으로 공격을 가하는 가도 중요하다. 상황분석이 요구되는 경우는 다음과 같다.

- 실시간 침입경보 분석시, 위험도가 높은 침입경보가 나왔을 때
- 통계자료 분석시, 이상 현상이 발견되었을 때
- 임의의 조건에 의한 침입경보 리스트에서 높은 위험도가 발견되었을 때

위와 같은 상황분석의 대상들은 Viewer에서의 조건 입력으로부터 범위가 정해진다. 이는 위의 경우에 따라 시간, 출발지 주소, 목적지 주소 등을 입력하여 관제센터에 해당 범위 내의 정보를 요구한다. 이를 통해 Viewer로 전해지는 데이터는 첫째로 목적지 주소를 기준으로 한 IP 주소와 그룹핑된 갯수를 나열한다. 이들은 상황분석의 기준이 되는 항목으로 어떠한 호스트가, 얼마나 공격당하고 있는가를 나타내기도 한다. 이러한 목적지 IP 리스트는 여러 개의 침입경보 그룹으로 나열된 것으로 하나의 리스트 항목을 선택하였을 때 통합된 침입경보들의 세부 리스트를 볼 수 있다. 이들은 또한 각각 출발지 주소 정보를 가지고 있다.

즉, 이를 통하여 전체적으로 출발지 주소와 목적지 주소를 파악함으로써 공격의 흐름을 파악할 수 있다. 또한 이들의 시그너처를 동시에 보여줌으로써 어떠한 공격으로 침입이 진행되고 있는가를 알 수 있다.

4. 상황분석 모듈의 구현

4.1 시스템 구조

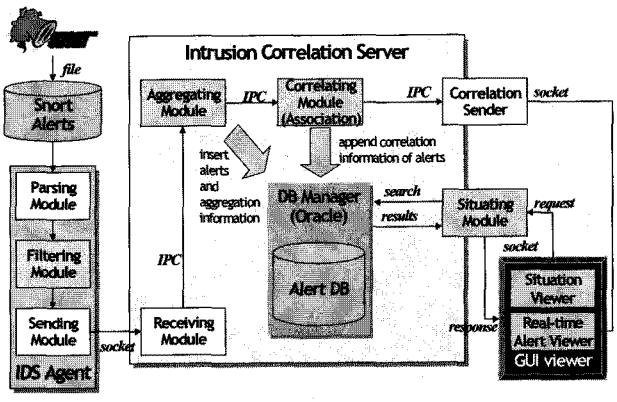


그림 3 본 논문에서 제안하는 시스템 구조

그림 3은 본 논문에서 제시하는 방법을 적용하여 구현한 시스템의 구조도이다. 사용한 침입탐지 시스템은 Snort [7]이며 필터링(filtering), 집단화(aggregating), 연관

성(correlating) 모듈을 통하여 축약된 정보를 바탕으로 상황분석(situating) 모듈에서 공격의 흐름을 파악하고 GUI viewer를 통해 보여준다. 침입 연관성 서버(intrusion correlation server)에서 상황분석 모듈은 독립적으로 구동되어 GUI viewer로부터 요청이 있을 때에 DB를 검색하여 공격 상황을 분석하게 된다. 침입 연관성 서버에서는 GUI viewer로부터 분석 범위(기간, IP 대역)를 전달받아 해당 범위에 맞는 침입경보를 DB에서 검색한다. 상황분석 모듈에서는 각 모듈에서 발생한 침입경보 뿐만 아니라 해당 침입경보에 연관된 모든 침입 경보를 보내게 된다. 이러한 경보는 어느 모듈에 의해 축약되어 있는지 어떠한 분류 기준에 속하는지가 구분된다.

표 1 분류 번호에 따른 위험도

분류	의미	위험수준	구분 색상
0	unclassified	0	흰색
1	IP scan	1	회색
2	port scan	2	노랑
3	vulnerability scan	3	진노랑
4	DoS	6	파랑
5	DDoS	7	남색
6	worm virus	5	청록
7	R2L	9	빨강
8	information leakage	8	자주
9	guessing	4	녹색

GUI viewer에서는 침입 연관성 서버에세 받은 정보를 목적지 주소를 기준으로 분류한다. 이 결과로 목적지 주소로 그룹핑된 리스트 정보가 보여진다. 각 목적지 주소에는 침입경보 수와 위험수준(severity)이 같이 표현된다. 위험수준은 그룹핑된 침입경보 중에서 가장 위험도가 높은 것으로 표현되며 목적지 주소의 피해 정도를 한눈에 파악할 수 있게 해준다. 표 1은 분류 번호에 따른 위험도를 표현하고 있으며 GUI viewer에서 색상으로 구분한다.

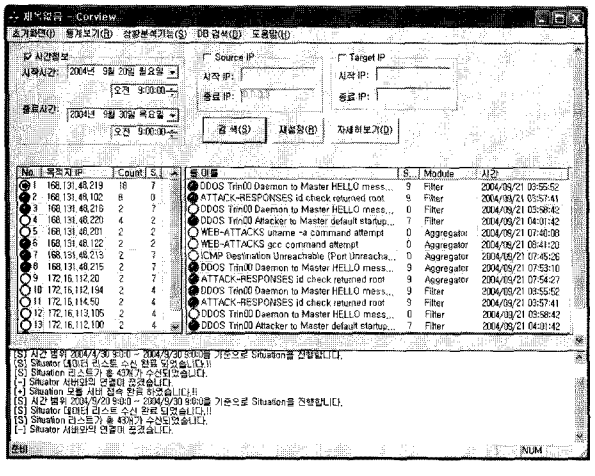


그림 4 상황분석을 위한 GUI viewer

그림 4는 상황분석을 위한 GUI viewer를 보여주고 있다. 이 GUI viewer에서는 목적지 주소를 클릭하면 우측 리스트에 목적지 주소로 그룹핑된 침입경보들이 나열된다. 여기에는 경보 이름, 위험도, 발생한 모듈, 시간 등의 정보를 나타내고, 경보 이름 앞에 색상 아이콘으로 위험수준을 알려준다. 또한, 좌측 리스트에서는 선택한 주소에 ➡표시를 하고 그 주소의 발신지 주소를 ◉로 표시하여 관련된 공격 흐름을 보여줄 수 있도록 한다. 이러한 방법으로 공격자와 공격당한 호스트를 구별할 수 있게 된다.

그림 5는 GUI viewer를 이용하여 임의의 호스트로부터 스캔에서 R2L까지를 수행하는 공격 방법과 경로를 파악하는 방법을 보여준다. 먼저, 공격수행 시간을 입력하여 목적지 주소 리스트를 얻는다. 이 리스트 중 분석의 대상이 되는 것은 위험수준이 높은 것이다. 위험수준이 5 이상인 공격은 반드시 분석할 필요가 있는 것이다. 그림 5에서는 도가 5 이상인 공격은 위험수준이 높은 것으로 반드시 분석할 필요가 있다. 그림 5에서 72.16.112.20 사이트에 위험수준이 9로써 168.131.48.215로부터 R2L 공격을 받았음을 알 수 있다. 따라서 168.131.48.215를 다시 조사하면 168.131.48.219로부터 R2L 공격을 받았음을 추적할 수 있다. 결국 168.131.48.219를 조사해 보면 DDoS Trin00 데몬을 설치하기 위해 여러 호스트를 조사하고 있다는 것을 확인할 수 있다. 이러한 방식으로 공격 흐름을 추적할 수 있으며 그래프로도 표현할 수 있다.

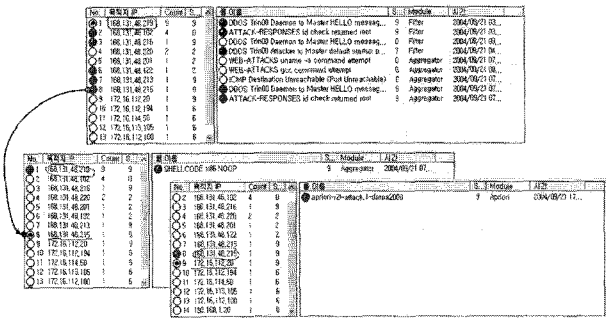


그림 5 GUI viewer를 이용한 공격 흐름분석 예제

4.2 IP 주소기반 상황 분석 방법의 성과

본 논문에서 주장하는 방법의 차이점을 설명하기 위해 그림 2와 같은 상황을 재현하여 실험하기로 한다. 그림 6은 DDoS 공격과 R2L 공격이 동시에 발생하는 상황을 도식화 한 것이다. 168.131.48.22에서 침입자는 몇몇 시스템에 DDoS용 마스터와 에이전트 시스템을 설치하고 DDoS 공격 준비를 하고 동료 침입자는 168.131.48.102에서 168.131.48.208 시스템에 침투하기 위한 준비를 한다. 모든 상황이 준비되면 DDoS 공격을

수행하고 그 사이에서 R2L 공격으로 시스템에 침투하는 시나리오이다. 이렇게 두 시스템이 공격을 받는 상황에서 본 논문에서 주장하는 방법과 기존의 상황분석 방법의 차이를 알아본다.

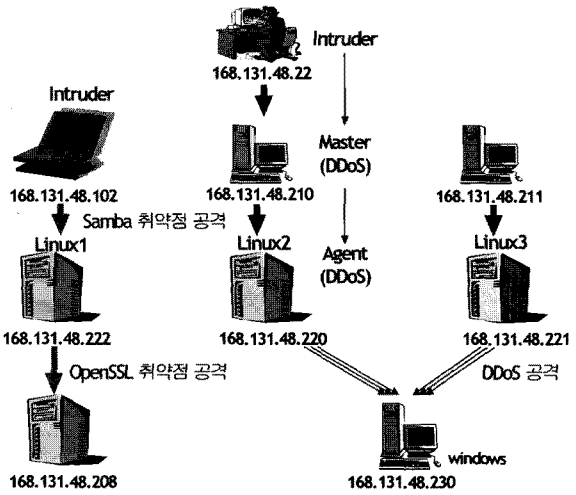


그림 6 상황분석 테스트를 위한 공격 시나리오

그림 7에서는 그림 6의 시나리오로 수행한 결과를 분석한 내용을 보여준다. 그림 7(a)는 168.131.48.220으로 R2L 공격을 통해 DDoS 에이전트를 설치한 결과를 볼 수 있다. 마찬가지로 그림 7(b)는 168.131.48.221에 DDoS 에이전트를 설치한 결과를 보여준다. 그림 7(c)에서는 또 다른 공격이 168.131.48.222로 있었음을 알 수 있고 그림 7(d)에서는 168.131.48.222에서 168.131.48.208로 침투가 있었음을 보여준다.

그림 7과 같은 과정을 수행함에 따라 자동으로 그림 8과 같은 그래프가 생성되며 공격의 흐름을 한눈에 보여주게 된다. 침입경보의 위험수준에 따라 시스템 사이의 화살표 선 색을 다르게 표현한다. 그림 8에서는 R2L 공격을 붉은색 실선으로 표시했고 DDoS 공격을 파란색 점선으로 표현했다. 실제로 DDoS 공격에 대한 경보는 주로 ICMP에 대한 메시지 형태로 발생되기 때문에, 메시지 흐름이 반대로 나타나게 되어 그래프로 표현할 때 방향을 바꾸는 과정이 추가로 필요하게 된다.

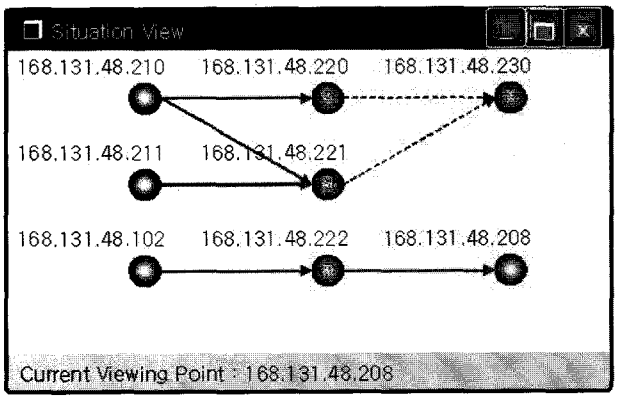
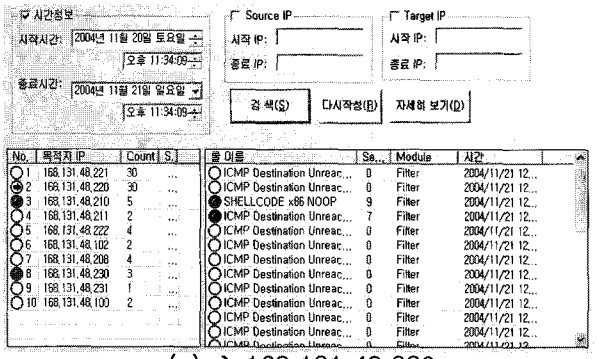
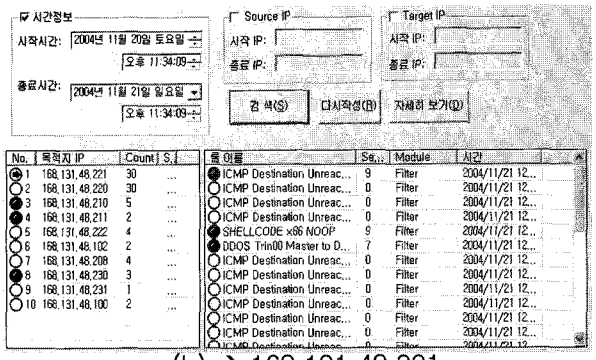


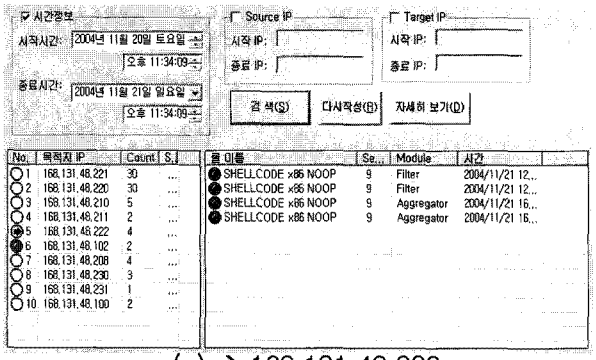
그림 8 공격 상황 그래프 보기



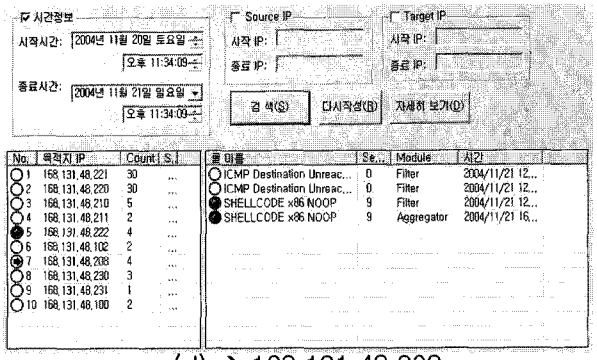
(a) → 168.131.48.220



(b) → 168.131.48.221



(c) → 168.131.48.222



(d) → 168.131.48.208

그림 7 테스트 시나리오 결과 분석 화면

그림 6과 같은 테스트 시나리오를 수행한 결과를 분석해 보면 표 2처럼 ACC 방식은 몇가지 공격을 하나의 상황 클래스로 표현하고 있음을 알 수 있다. 또한, 그 클래스 내부의 침입정보를 보면 Situation 3-3과 Situation 2-2에서 발신지 주소를 확인할 수 없다. 물론 이러한 상황 클래스로 축약되기 전을 분석하면 알 수 있겠지만 추가적인 부담을 주게 된다. 본 논문에서 제안한 방법은 각각의 상황을 독립적인 경보로 구분하여 보여주며 발신지 주소와 목적지 주소를 정확히 보여주고 그 사이의 연결까지 보여준다. 따라서 본 논문에서 제안한 방법은 각 호스트 사이의 공격흐름을 적절히 분석할 수 있도록 축약된 경보를 생성하며 그래프 형태로 공격 흐름을 보여줌으로써 관리자가 쉽게 침입상황에 대응할 수 있도록 도움을 줄 수 있다.

표 2 제안한 방법과 ACC의 상황인식 방법의 차이

		210→220	211→221	102→222	220→230	221→230	222→208
ACC		Situation 3-3			Situation 2-2		Situation 1
제안 방법		R2L	R2L	R2L	DDoS		R2L
ACC의 상황 클래스		Situation 3-3		Situation 2-2		Situation 1	
침입정보	공격 타입	ShellCode x86 Noop		ICMP Destination Unreachable		ShellCode x86 Noop	
	발신지 주소	*		*		168.131.48.222	
	목적지 주소	*		168.131.48.230		168.131.48.202	

5. 결 론

침입탐지 시스템에 직면한 현재의 문제점은 경보가 너무 많이 발생하거나 잘못된 경우가 있다는 것이다. 이러한 점은 관리자의 실시간 대처 능력과 공격 흐름 분석을 어렵게 한다. 또한 기존의 상황 분석 방법은 단순한 척도의 비교로 추상화함으로써 간결한 결과를 얻을 수 있으나 정교한 공격을 파악하기 어렵다. 이것은 침입경보를 축약시키는데 효과가 있으나 공격 흐름 분석에는 부적절하다. 즉, 기존의 방법에서 제시한 상황 분석은 여러 경보를 단순한 상황 클래스로 축약함에 따라 축약율에서 성과는 좋으나 공격 흐름을 파악하기에는 어려움이 있다.

본 논문에서는 침입탐지 경보사이의 관계를 주소기반으로 분류하고 공격 특성에 따라 유형을 분류하였다. 먼저, 모든 침입경보를 사용하여 상황 분석을 하는 경우 시간이 많이 걸리고 보여주는 데이터가 많게 되므로 적절한 축약과정을 거쳐야 한다. 본 논문에서는 침입 경보의 특성 사이의 유사성에 따라 집단화를 수행하고 경보 이름 사이의 연관성을 학습하여 축약을 수행한다. 이러한 과정을 거침으로써 ACC와 비슷한 정도의 축약 효과를 볼 수 있었다. 이러한 축약된 정보를 가지고 IP 주소에 따라 그룹핑하고 9가지 분류 기준에 따라 해당 경보의 위험수준을 파악할 수 있도록 하였다.

이러한 결과를 바탕으로 공격 사이의 관련성을 찾아갈 수 있으며 그 결과를 그래프로 표현하여 관리자가 공격 흐름을 쉽게 파악할 수 있도록 하였다. ACC와 같은 방법은 포괄적으로 공격 상황을 파악하기에 용이하지만 본 논문에서 제시하는 방법은 세부적인 공격 경로까지도 파악할 수 있으므로 관리자가 침입에 대한 결과를 보고하거나 침입 받은 시스템을 정비하고자 할 때 더 유용하다고 할 수 있다.

참고문헌

[1] Ning, P., "Techniques and Tools for Analyzing Intrusion Alerts," ACM Transactions on Information and System Security, Vol.7 No.2, pp 274-318, 2004.

[2] Moh, W., Kim, M., Cheong, I., Noh, B., Seo, J., Park, E. and Park, C., "An Analysis on the Correlation of Network-based Alerts with Association Rule Algorithm," WISA 2004, pp.705-712, 2004.

[3] Debar, H. and Wespi, A., "Aggregation and Correlation of Intrusion-Detection Alerts," RAID 2001, Oct., 2001.

[4] Porras, P. and Neumann, P., "EMERALD : Event Monitoring Enabling Responses To Anomalous Live Disturbances," Proc. of the 20th National Information Systems Security Conference, pp 1-13, 1997.

[5] Valdes, A. and Skinner, K., "An Approach to Sensor Correlation," RAID 2000, Oct., 2000.

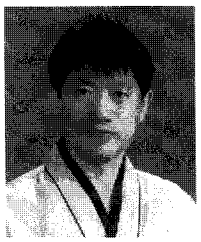
[6] Valdes, A. and Skinner, K., "Probabilistic Alert Correlation," RAID 2001, Oct., 2001.

[7] Beale, J., Foster, J., Posluns, J. and Caswell, B., Snort 2.0 Intrusion Detection, SynGress, 2003.

김 민 수

1993 전남대학교 전산통계학과
1995 전남대학교 전산통계학과(석사)
2000 전남대학교 전산통계학과(박사)
2000~2001 한국정보보호진흥원 선임연구원
2001~2004 전남대학교 객원교수
관심분야 : 침입탐지시스템, 운영체제보안, 데이터마이닝
E-mail : phoenix@athena.jnu.ac.kr

노 봉 남



1978 전남대학교 수학교육과(학사)
1982 한국과학기술원 전산학과(석사)
1994 전북대학교 전산통계학과(박사)
1983~현재 전남대학교 전자컴퓨터정보통신공학부 교수
관심분야 : 컴퓨터 네트워크 보안, 사이버 사회와 윤리
E-mail : bbong@jnu.ac.kr

서 정 택

1999 충주대학교 컴퓨터공학과(학사)
2001 아주대학교 컴퓨터공학과(석사)
2000~현재 국가보안기술연구소 정보보증연구부 선임연구원
관심분야 : 시스템 및 네트워크 보안, 정보보증
E-mail: seojt@etri.re.kr

박 응 기

1986 중앙대학교 전자계산학과(학사)
1988 중앙대학교 전자계산학과(석사)
1988~1999 한국전자통신연구원 선임연구원
2000~현재 국가보안기술연구소 정보보증연구부 책임연구원(팀장)
관심분야 : 시스템 및 네트워크 보안, 정보보증
E-mail : ekpark@etri.re.kr