# 안전한 정보통신 인프라용 고성능 침해탐지 및 대응기술

한국전자통신연구원 정보보호연구단 김기영, 오진태
대구가톨릭대학교 컴퓨터정보통신공학부 전용희

차 례



## 1. 서 론

인터넷 사용의 급증으로 인한 인터넷 가입자 수의 폭발적 증가와 생활의 편의성 제공을 위한 다양한 서비스 제공으로 인하여 인터넷 트래픽 양이 지속적으로 늘어나고 있다. 하지만 인터넷은 누구나 쉽게 접근할 수 있는 개방형 환경과 편리성 제공으로 인하여 오히려 해킹, 바이러스 유포, 지적 재산권의 침해 및 사이버 범죄 등에 이용되고 있어 인터넷 활성화에 대한 역기능이 심각한 문제로 대두되고 있다.

이미 사이버공격은 해킹/웜 및 바이러스 기술의 통합화로 인하여 그 피해가 대형화되고 있으며, 공격기술 또한 고수준화 되고 있다. 또한 특정 시스템 및 중요서버를 공격대상으로 하던 초기 해킹 양상도 변화하고 있어, 불특정 다수의 시스템 및 네트워크 차원의 공격으로 변화하고 있다.

최근 발생하였던 Bot, Peep에서 볼 수 있는 바와 같이 사회공학적인 방법까지 해킹에 이용되어 날마다 새로운 방법의 네트워크 침해가 발생하고 있다. 이러한 공격의 대부분이 네트워크 인프라에 과부하를 발생하도록 하고 있어 다양한 웜 바이러스에 대한 네트워크 인프라보호가 가능한 새로운 솔루션이 절실히 요구된다.

이러한 솔루션의 일환으로 IPS (Intrusion Prevention System)가 네트워크 보안장비의 새로운 패러다임으로 자리잡고 있다. IPS는 기존의 IDS (Intrusion Detection System)가 탐지만 하고 대응을 할 수 없었던 단점을 보완하여, 탐지 정확성과 성능을 향상시키고 실시간 대응이 가능한 네트워크 보안 전용장비이다. 실제 네트워크

에 적용시 외부의 위협을 근본적으로 차단하며 성능과 품질을 보장하는 능동형 솔루션이라고 할 수 있다.

IPS는 네트워크로 입력되는 모든 트래픽의 세션 정보를 관리하여 프로토콜별로 취약점을 분석하는 기술을 기본기능으로 제공한다. 또한 세션 분석과 함께 misuse 기반 탐지를 위한 패킷 헤더 분석 및 패킷 내용까지도 100% 분석하면서 패킷의 통과 여부를 실시간으로 결정하는 기능도 제공한다.

일반적으로 CPU기반 보안장치의 경우 초당 처리 가능한 패킷 수에 한정이 있어 대부분의 공격자들이 우회 공격하기 위하여 작은 크기의 패킷을 이용하고 있다. 따라서 보안장치의 우회 공격에 대응하기 위하서는 패킷의 크기에 무관하게 성능이 보장되는 가용성을 제공하여야 한다. 그리고 알려진 공격 패턴에 대한 실시간 대응이 가능하도록 축적된 데이터베이스를 갖추고, 실시간 탐지 및 방어 기능을 제공하여야 한다.

최근 빈번히 발생하는 웜의 경우, 이를 보안장치에서 탐지하고 대응할 수 있는 공격 패턴이 알려지기 전에 급속도로 인터넷을 통해 전 세계의 컴퓨터를 감염시키기 때문에 이러한 공격 유형에 대한 실시간 탐지 및 방어 기술이 필요하다. 알려지지 않은 웜의 경우 호스트 IDS 등으로 탐지할 수 있지만, 네트워크 수준에서는 네트워크 트래픽 분석이나 프로토콜분석 등을 통한 비정상행위 탐지 기법을 이용하여야만 공격 탐지가 가능하다. 하지만 비정상행위 탐지 기술은 높은 오탐율을 가지고 있어 여기에서 제공된 탐지 결과를 대응에 바로 적용하기에는 많은 무리가 있다고 판단된다. 따라서 오탐율을 최소화하기 위해 다양한 변수를 가지고 환경에 적응하는 지능형 방어기술이 추가로 요구된다.

본 고에서는 네트워크 인프라를 위협하는 웜이나 바이러스, 알려지지 않은 공격에 대하여 보안기능을 제공하는 하드웨어 기반 고성능 침해탐지 기술과 과다 트래픽 감지기술에 대하여 알아보고, 현재 한국전자통신연구원 네트워크 보안그룹에서 개발하고 있는 보안게이트웨이 시스템(SGS : Security Gateway System)에 대하여도 알아보고자 한다.

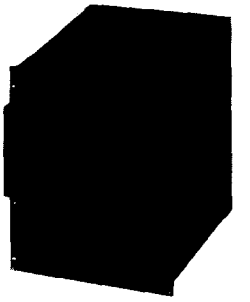


**그림 1. SGS 시스템 형상**

그림 1은 현재 ETRI에서 개발하고 있는 SGS 시스템의 형상으로 실시간 20Gbps의 처리성능을 가지는 보안전용 시스템이다.

본 고의 나머지는 다음과 같은 구성으로 기술되어 있다. II절에서 고성능 침해탐지 기술에 대하여 하드웨어기반 고성능 탐지 알고리즘과 시스템 측면에서 살펴보고, III절에서 과다트래픽 감지기술에 대하여 2단계 트래픽 분석 알고리즘과 시스템 측면에서 검토해본 다음, 이러한 기술을 이용하여 네트워크 차원의 대응이 가능한 실시간 대응 메카니즘에 대하여 IV절에서 알아본다.

## II. 고성능 침해탐지기술

지금까지 침입탐지 시스템은 침입탐지 기능을 수행하기 위하여 대부분 소프트웨어 기반의 보안기능을 제공하였으나, 이미 고속화된 네트워크에서 소프트웨어 기반의 침입탐지 기능은 성능의 한계에 봉착하고 있다. 또한 침입탐지 시스템과 같은 보안 시스템은 다양한 탐지 기술을 필요로

하며, 고속화된 네트워크를 수용하기 위하여 탐지의 고속화도 필요로 한다. 탐지 기능은 정확성 및 고속성 뿐만 아니라 misuse 기반의 탐지 룰 생성이 용이하지 않은 침해를 탐지하기 위한 비정상행위 탐지 능력을 갖는 탐지 엔진을 필요로 한다. 이미 언급한 바와 같이 이러한 기능들을 소프트웨어 기반으로 제공하는 것은 한계를 보이고 있으므로 **보안 전용 하드웨어**를 설계하여 해결하여야 할 **것이다.**

현재 네트워크 **장치에서 다양한** 접속 표준 및 새로운 기능들을 **쉽게 추가하고자** 네트워크 프로세서가 만들어**져 활용되고 있고** 이미 10G급의 처리용량을 가진 **네트워크 프로세**스가 사용되고 있다. 또한 이미 수년전부터 고성능 네트워크 프로세스를 사용하여 보안기능을 구현하고자 하는 노력들이 있어 왔다.

네트워크 프로세서를 이용한 보안 기능 구현은 대부분 소프트웨어 기반의 보안 알고리즘들을 네트워크 프로세스에 마이크로 코드 형태로 구현한다. 하지만 소프트웨어 기반의 알고리즘은 하나의 고속 프로세스를 사용하는 것을 전제로 만들어진 알고리즘으로 다중 프로세스와 하드웨어 로직들을 이용한 병렬 처리 구조에 적합하지 않다.

따라서 하드웨어에 보안 기능을 적용하기 위해서는 하드웨어의 구조에 적합한 고속 탐지 알고리즘 개발이 우선되어야 할 것이다. 사실 네트워크 프로세스를 이용하든지 또는 로직을 직접 설계하여 ASIC등으로 만드는지가 문제가 아니라 오히려 하드웨어의 특성을 이해하고 이를 적극적으로 이용할 수 있는 알고리즘이 개발되었는가가 더 중요한 문제일 것이다.

현재까지 개발된 네트워크 프로세서 중에서 최고성능의 네트워크 프로세서로도 1Gbps 급의 패킷 헤드 룩업 기능과 stateless 방화벽 정도를 겨우 구현할 수 있는 정도이며 이들 기능을 구현하면 추가적인 보안기능을 구현할 하드웨어 리소스가 거의 없어 추가적인 보안 알고리즘을 구현하기 어려운 실정이다. 따라서 지금까지 네트워크 프로세스로 구현할 수 있는 보안기능은 탐지 룰의 필드가 비교적 한정된 패킷 라우팅 기능과 stateless 방화벽 등에 적용 가능한 헤더룩업 정도를 구현할 수 있는 것으로 보인다.

침입 탐지 엔진에서 사용되는 대부분의 탐지 룰들은 패킷의 헤더 필드와 페이로드에 포함된 특정 패턴의 조합에서 침입을 탐지할 수 있어야 하며, 헤더 필드 비교만으로 침입을 판단할 수 있는 탐지 룰은 그리 많지 않다. 또한 misuse기반의 패턴 매칭 정도의 기술도 현재의 네트워크 프로세서에서 적용하기는 쉽지 않다. 앞에서 설명하였듯이 소프트웨어 기반의 침입탐지 기능을 네트워크 프로세스를 이용하여 구현하는 경우 각각의 탐지 룰들을 마이크로 코드 형식으로 코딩하여야 한다. 네트워크 프로세스의 물리적인 한계로 인하여 이미 수천 개가 넘는 많은 탐지 룰들을 하나의 프로세스에서 구현하는 것은 불가능한 것으로 여겨진다. 기존에 네트워크 프로세스를 이용하여 탐지엔진을 구현한 예에서도 몇 개의 탐지 룰들만을 구현하여 탐지엔진의 구현 가능성만을 보인정도로 평가되고 있다. 또한 네트워크 프로세스를 이용하는 경우 새로운 탐지 룰을 추가하기 위해서는 해당 탐지 룰에 대한 마이크로 코드를 새로 추가하여야 하므로 룰 추가가 매우 힘들다고 할 수 있다.

이상에서 살펴본 바와 같이 네트워크 프로세스를 이용하여 보안 기능을 구현 할 때 침입탐지 장치의 가장 기본적인 misuse기반의 탐지엔진도 네트워크 프로세서로 구현하는 것도 현재 네트워크 프로세서 기술로는 어려워 보인다.

또한 현재 대부분의 보안 시스템은 L7까지 모든 계층에 걸쳐 보안 검사를 요구하고 있어 네트워크 프로세서에 의한 완벽한 해결책은 기대하기

어렵다고 보여진다. 이미 국내 여러곳에서 네트워크 프로세서를 적용하여 보안제품을 개발하고자 노력하였으나 탐지엔진 구현의 어려움과 성능 한계로 인한 어려움을 겪고 있다. 이러한 고속탐지엔진은 많은 수의 룰들을 동시에 비교할 수 있는 하드웨어 알고리즘을 필요로 하며, 이러한 검색 알고리즘 없이 단순한 소프트웨어의 하드웨어화로는 해결되지 않는다.

이미 IPS기술의 우위를 선점하고 있는 티핑포인트 유니트윈, NA의 맥아피 인터루쉴드 등의 회사에서도 보안전용 ASIC을 개발하여 적용한 시스템을 출시하였으며, 네트워크 프로세서에 기반한 고성능 제품을 찾아보기 어렵다. 따라서 고성능 알고리즘 개발을 통한 보안 전용 FPGA 및 ASIC 솔루션이 현재까지는 유일한 해결책으로 보인다.

이렇게 하드웨어로 구현된 고성능 침해탐지기술을 제공하기 위하여 고속의 네트워크에서 송수신되는 유해패킷들에 대한 탐지의 정확성을 보장하여야 하며, 이러한 탐지의 정확성 보장을 위하여 패턴매칭과 휴리스틱 분석기능 등이 필요하고, Stateful Packet Inspection, IP defragmentation, TCP Reassembly와 같은 Packet Preprocessing이 제공되어야 한다. 이러한 Packet Preprocessing 기능을 자세히 살펴보면 다음과 같다.

### • SPI(Statefule Packet Inspection) 기능

일반적으로 인터넷 프로토콜은 TCP와 같이 3-way handshaking을 통해 연결을 설정하고 통신하는 프로토콜과 UDP나 ICMP등과 같이 연결을 위한 준비단계가 없이 바로 패킷을 전달하는 프로토콜로 나누어 볼 수 있다. SPI 기능은 3-way handshaking을 통해 연결을 설정하고 연결이 설정된 후 본격적인 통신을 하는 TCP 프로토콜의 패킷에 대하여 침해를 탐지하는 기술이다. SPI기능으로 탐지 할 수 있는 탐지 기능은 일반적으로 TCP 패킷을 이용하여 네트워크를 공격하는 유형의 공격들이 연결을 설정한 후에 본격적인 공격코드가 전달된다는 것을 이용하여 침입을 좀더 정확히 찾아내며, session의 특정한 부분에서만 공격코드가 교환된다는 점 등을 이용하여 공격을 정확히 찾아내기도 한다. 또한 TCP를 이용하는 공격의 경우 TCP가 가지는 session이 IETF 등의 국제 표준화 기관에서 권고하는 특정 state를 벗어난 state 천이를 발생하여 공격지의 시스템이 비정상적인 버퍼 오버플로우를 발생하도록 하는 등의 이상 상태 천이를 찾는데 적용될 수 있는 기술이다.

SPI기능은 기존의 stateless 침해 탐지기능과 조합되어 탐지의 정확성을 향상하는 역할을 수행한다. SPI에서는 기존의 stateless 패턴 매칭 기술이 하나의 패킷 내용만을 보고 침입여부를 판단하는 것과는 달리 TCP 스트림의 session에 대한 상태를 추적하면서 보다 정확하게 침입여부를 판단하여 False Positive 경보를 줄이는 특징이 있다.

특히 SPI 기술을 적용하여야 stick이나 snot와 같은 IDS 우회 공격용 Tool들에 의해 발생하는 다량의 False Positive Alert을 줄일 수 있다. 또한 SPI기능에 서 동시에 연결할 수 있는 session 수는 최소 100만개 이상은 되어야 하며, SYN Flooding등의 TCP session을 시작하는 DoS 공격에 자체 시스템을 방어할 수 있는 메카니즘을 필요로 한다.

SPI 기술은 도착한 패킷이 Session Table Entry에 존재하지 않으면, 즉 Unestablished connection에서 받은 패킷이면 정책에 따라 해당 패킷을 처리할 수 있는 Session 추적기능, 이전 패킷의 Sequence Number, data size와 Window size 정보를 이용하여 현재 패킷의 Expected Maximum Sequence Number를 구하는 Sequence Number Tracking기능, 서버와 클라이언트의 Last Ack를

계속 추적하여 현재 패킷의 Acknowledged Number를 check하는 Acknowledge Number Tracking기능, 동일 세션에 속한 패킷들의 hop count를 check하는 TTL tracking기능이 필요하다.

- **PR(Packet Reassembly) 기능**

Packet Reassembly 기능은 fragmented IP 패킷을 이용한 침입탐지 장치 우회 공격을 탐지하기 위한 IP defragmentation 기능과 조각난 TCP 패킷에 의한 침입탐지 장치 우회 공격을 탐지하기 위한 TCP reassembly 기능으로 구성되어 침해탐지엔진의 정확성을 향상하는 역할을 수행한다.

IP Defragmentation 기능은 IP Header의 DF (don't Frag), MF(more frag)와 Frag offset값에 의해 fragment된 패킷을 재조합하여 패킷을 검사하는 기능을 수행하여야 한다. 또한 TCP Reassembly 기능은 source/destination IP, 포트, 프로토콜 정보와 sequence number, window size, data size등의 정보를 이용하여 동일한 session에 속한 TCP 패킷들을 재조합하는 기능을 제공하여 IDS evasion 공격을 탐지하도록 한다.

- **PAA(Protocol Anomaly Analysis) 기능**

비정상 프로토콜 해석 기능은 Packet Preprocessing 기능의 하나로 정상적인 프로토콜에 명시한 규약을 위반하여 서버의 버퍼를 오버 플로우 시키는 등의 공격을 탐지하는 기능을 수행한다. 인터넷의 패킷들은 IETF등의 표준화 기관의 RFC 문서에 근거하여 패킷을 발생하도록 되어 있다. Protocol Anomaly 기능은 각 프로토콜에 대하여 RFC 문서에 근거하여 패킷의 적합성 검사를 수행하며 이를 통해서 공격 여부를 탐지하는 기능을 제공한다. 헤더 룰 체크 모듈에서 매칭된 모든 패킷들을 Protocol Anomaly 기능에서 전달받아 anomaly여부를 검사하며, HTTP, SMTP, FTP, POP, DNS 등의 프로토콜에 대하여 적합성 검사를 거쳐 버퍼 오버플로우성 공격에 대한 탐지를 수행한다.

현재 SGS시스템은 FPGA 로직을 통하여 입력 패킷에 대하여 Stateful packet Inspection, IP Defragmentation, TCP Reassembly 및 Protocol Anomaly 기능들을 전처리 기능들을 수행하고 규칙기반 패턴 매칭 기능으로 침입을 탐지하는 메카니즘을 제공한다.

규칙기반의 패턴 매칭 기능은 이미 snort 2.0과 같이 기 정의된 침입 탐지규칙에 따라 입력되는 패킷의 헤더와 데이터 내용을 검사함으로써 수행되며, 침입으로 판정된 패킷에 대해서는 패킷 Drop, 세션 종료 등의 대응기능까지 수행할 수 있다. 실시간 탐지를 위해 하드웨어에 적합한 탐지 알고리즘이 개발되어 구현되었으며, snort 등에서 제공하는 침입 탐지규칙들을 적용하여 침입에 대한 실시간 분석과 실시간 대응을 수행할 수 있는 하드웨어를 제공함으로서 고속의 네트워크에서 효율적인 탐지 기능을 제공한다.

침입탐지를 위해 misuse 기반의 침입탐지엔진은 regular expression search 기능을 포함하고 있다. regular expression search 기능은 패킷 헤더의 조합을 실시간으로 검사하는 기능인 순차적 룩업을 이용한 packet header lookup 기능과 패킷의 데이터 내용을 실시간으로 검사하는 패턴 매칭 기능으로 구분할 수 있다.

침입 탐지 룰들에 정의된 패킷 헤더의 다양한 조합은 수천 개의 룰 수에 비하여 적은 수백 개 이내의 조합으로 정리될 수 있다. 하지만 각 조합은 패킷 헤더의 모든 필드들을 비트별 don't care 처리 가능한 조합을 요구하고 있어 매우 복잡하다. 물론 이러한 헤더 룩업 기능을 로직으로 구현하여 하드코딩 할 수도 있으나 이 경우 새로운 탐지 룰을 추가 하고자 하는 경우 문제가 발

생한다. 이를 처리하기 위하여 TCAM을 사용 할 수도 있으나, IP헤드 20바이트 및 TCP 헤더 20 바이트 등 많게는 40바이트 이상의 입력 데이터를 요구하여 구현비용이 비싸지는 단점이 있다.

현재 SGS에서는 룩업 순서에 따라서 헤드 룩업의 결과를 조합 할 수 있는 FPGA의 로직으로 만든 작은 크기의 TCAM을 이용하도록 하는 알고리즘을 사용한다. 즉, 작은 크기의 TCAM만으로도 다양한 헤더 조합의 룩업 기능이 가능하도록 구현하였으며, 패킷의 데이터 내용을 검사하기 위한 알고리즘도 함께 제공하여 실시간 탐지가 가능하도록 하였다.

지금까지 기술한 패턴매칭, 휴리스틱분석 및 전처리기능 등의 침입탐지 기능이 기본적으로 제공하여야 하는 기능들을 요약하면 다음과 같다.

- 침입 유형별 탐지 및 차단 기능
- 웜, 바이러스 탐지 및 차단 기능
- 인라인모드 지원을 통한 정책기반 자체 차단기능
- 침입탐지 내역 및 차단 현황에 대한 로그 및 보고 기능
- 유연하고 실시간성이 보장되는 정책 Update 기능
- 실시간네트워크 트래픽 분석 기능
- 알려지지 않은 공격 탐지를 위한 Anomaly 분석 기능

위와 같은 기능들은 오탐으로 인한 서비스 제한 방지를 위한 탐지기능의 정확성과 수기가급의 네트워크에서 wire-speed를 보장하는 고성능화를 보장하면서 제공되어야 한다.

## Ⅲ. 과다트래픽 감지기술

과다트래픽 감지기술은 네트워크에서 선로 속도의 flow 분류 및 실시간 트래픽 측정을 통해 다양한 DoS/DDoS 공격과 웜/바이러스와 같이 과도한 트래픽을 발생하여 네트워크에 부하를 가하는 유형의 공격을 탐지하기 위한 기능이다.

현재 네트워크 트래픽 분석을 위하여 Netflow, Cflow와 같은 트래픽 미터링 툴들이 활용되고 있다. 하지만 이러한 툴들은 실시간으로 기가급 이상의 트래픽을 모두 분석하기 어려워 샘플링 메카니즘을 사용하여 트래픽을 측정하고 있다. 물론 샘플링에 의한 트래픽 측정이 네트워크상의 비정상적인 행위를 가진 트래픽을 찾을 수 있다고는 하지만, 측정된 정보를 소프트웨어로 다시 분석하여야 하는 부담이 있어 실시간 처리에 어려움이 있는 것으로 분석되고 있다. Netflow 같은 제품의 경우. 측정된 데이터를 분석하여 다양한 공격들을 찾을 수는 있지만 이와 같은 모든 기능을 수행하기 위해서는 실시간성을 포기해야 하는 tradeoff가 발생한다.

과다 트래픽을 생성하는 공격은 단시간에 많은 트래픽을 발생하여 네트워크 폭주를 유발하도록 한다. 이러한 네트워크 폭주상태로 인하여 네트워크를 사용하는 정상 사용자들의 서비스에 장애를 겪게 되고, 마침내는 네트워크 전체가 마비된다. 지금까지 네트워크 폭주를 방지하기 위한 기술로는 큐잉기술, 침입탐지/방어 시스템, 트래픽 볼륨기반 분석에 기반한 대역폭 제한 기술 등이 제안되어 있으며, 이러한 기술들을 살펴보면 다음과 같다.

● 큐잉기술

네트워크 폭주시 또는 네트워크 폭주를 방지하기 위하여, 차단할 패킷을 결정하는 기술이다. 차단할 패킷을 결정하는 방법에 따라서 FIFO, FQ, RED 등이 제안되었다. 이러한 종래의 큐잉 기술은 네트워크의 상태에 순응하는 트래픽, 즉 네트워크가 폭주라는 것을 감지하면 전송 양을

줄이는 트래픽의 경우에는 네트워크 폭주를 차단하거나 방지하는 데에 큰 효과가 있지만, 폭주상태에서도 과다 트래픽을 계속 생성하거나 또는 많은 종류의 인위적인 플로우를 생성하는 DoS 공격에서는 그 과다 트래픽을 근본적으로 차단할 수 없는 문제가 있다.

● 침입탐지 및 방어 시스템

비정상적인 패킷을 생성하거나 비정상적인 플로우를 생성하여 목적지 시스템을 스캔, 해킹, 그리고 마비시키는 등의 행위들을 네트워크상에서 탐지할 목적으로 제안되었다. 침입탐지 시스템은 공격으로 판단된 트래픽들을 방화벽과 연계하여 차단하기도 하고 또는 침입탐지 시스템 자체가 직접 차단하기도 한다. 하지만 정상 트래픽을 공격 트래픽으로 오판할 경우 정상적인 트래픽까지 차단하는 문제점을 제공하고 있다.

● 트래픽 볼륨 분석기반에 의한 대역폭제한 기술

대역폭 제한기술은 측정한 트래픽 볼륨과 기준치를 비교하여 패킷을 전송하거나 폐기함으로써 DoS 공격을 차단하는 기술이다. 기준치는 가입자의 트래픽을 직접 측정해서 통계치를 이용하여 얻도록 한다. 어떠한 트래픽도 기준치를 초과할 수 없어 DoS 공격을 차단하는 효과가 있지만, 기준치를 정확하게 측정하는 것이 거의 불가능하다. 기준치가 부정확하게 측정된 경우 정상 트래픽을 차단할 수 있는 문제점을 내포하고 있다.

일반적으로 네트워크에서 한 보안 장치를 사용하여 네트워크의 모든 침해 문제를 해결 할 수는 없다고 말하고 있다. 과다 트래픽 감지 기능 또한 마찬가지로 이 기능만 가지고 네트워크의 모든 형태의 침해를 찾을 수 있는 것으로 기대하기는 어렵다. 따라서 과다 트래픽 감지 기능을 이용한 anomaly 분석 기법과 misuse 기반의 침입탐지 기능 등이 통합된 형태의 장치를 필요로 한다.

일반적으로 과다 트래픽을 발생하는 flow는 평상시의 정상적인 트래픽 flow에 비해 상대적으로 큰 대역폭을 사용한다는 특징이 있다. SGS 시스템에서는 이러한 비정상적인 과다 flow 특징을 이용하여, 입력 flow에 대한 실시간 대역폭 측정 기술과 이미 측정된 flow들을 대역폭 크기 순으로 정렬하여 변화를 추적하는 기술을 하드웨어로 제공한다. 그리고 하드웨어 장치에서 발생하는 분석데이터들을 소프트웨어에서 처리하는 과다트래픽 감지 알고리즘도 아울러 제공한다.

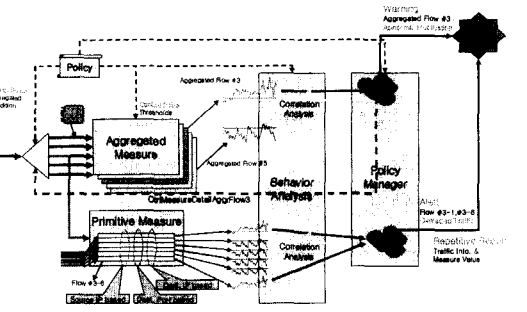



**그림 2. SGS시스템의 2단계 트래픽 측정**

그림 2에서는 SGS 시스템에 적용된 2단계 flow 분석 메카니즘을 보여주고 있다. SGS에서는 기존의 샘플링에 의한 데이터 측정에서 제공하는 실시간 데이터처리 문제와 정상 트래픽 수집에 의한 처리 데이타 양의 문제점을 해결하도록 하였으며, 측정된 데이터를 다시 소프트웨어에서 가공하여 처리하는 데이터양의 문제점을 해결하고자 Source IP별 flow와 Destination IP 및 destination port별 flow에 대해 트래픽을 1차로 측정하도록 한다.

정상적인 트래픽에 대해서도 모든 데이터를 수집하여야 한다는 기존 측정방법의 단점을 해결

하고자 1차 측정에서 과다한 트래픽 변화를 발생하는 flow에 대하여만 분석을 하도록 한다. 1차적으로 분석된 flow에 대하여 프로토콜 및 5-tuple을 기준으로 2차적 분석 기능을 제공한다. 이러한 단계별 측정 및 분석방법으로 과다트래픽에 의한 네트워크 침해를 효율적으로 찾을 수 있도록 설계하였다.

## Ⅳ. 실시간 대응 메카니즘

현재 SGS에서 실시간 대응 메카니즘은 고성능 침해탐지 기술과 과다 트래픽 분석기능에서 판단된 정보와 정책기반 차단 규칙에 의해 판단된 정보, 침입 유형 분석기능에서 판단된 정보를 기준으로 최종 대응하는 기능을 제공한다.

SGS 시스템에서는 알려진 취약점에 대해 정의된 규칙에 의하여 대응하는 정책기반 대응과 알려지지 않은 네트워크 차원의 공격에 대하여 실시간 트래픽 분석을 통한 자동화된 대응 메카니즘으로 분리하여 제공한다. 각각의 기능을 살펴보면 다음과 같다.

- 정책기반에 의한 대응
  1. 접근제어정책
  2. 패턴매칭 정책
  3. 휴리스틱 분석 정책
  4. 대역폭 제어 정책

- 자동화된 대응 메카니즘에 의한 대응
  1. 알려지지 않은 공격에 대한 세션블럭과 대역폭제어 정책
  2. Anomaly 분석기반 정책 : 프로토콜, Flow 기반 트래픽 분석
  3. 트래픽 분석과 탐지 정보 연관성 분석에 의한 대응정책 생성
  4. 알려지지 않은 공격에 대한 탐지 룰 자동생성

지금까지 기술한 실시간 대응 메카니즘은 그림 3과 같은 구조로 제공된다.

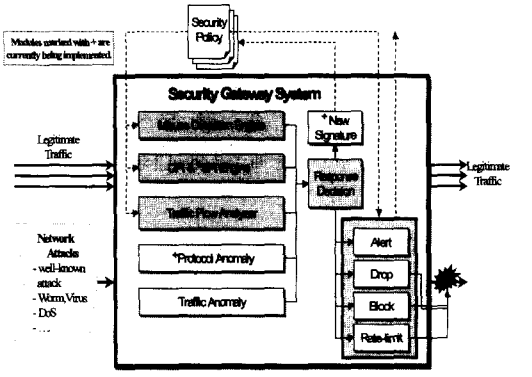



**그림 3. SGS시스템의 실시간 대응 구조**

## Ⅴ. 결 론

사이버 공격 유형이 분산화, 지능화, 통합화, 대규모화, 자동화, 은닉화의 경향으로 발전하고, 인터넷이 사회생활 전 영역에서 필수적인 요소로 자리를 잡음에 따라 보다 안전하고 신뢰할 수 있는 정보통신 인프라의 구축이 절실하게 요구되고 있다.

이를 위해서는 IPS라는 새로운 패러다임이 네트워크 측면에서 개별 트래픽에 대한 기밀성, 무결성, 가용성을 보장할 수 있는 수단을 제공하여야 하며, 일관성 있는 감시, 관리 및 제어 정책의 집행이 가능하여야 한다.

본 논문에서는 이러한 IPS 개발의 일환으로 한국전자통신연구원에서 설계 및 구현중인 SGS 시스템의 개발 내용에 대하여 살펴보았다. SGS 시스템은 하드웨어 기반의 고성능 침입탐지 및

과다 트래픽 감지 엔진으로 구성되어 있으며, 보안 엔진들에서 탐지 및 감지된 결과의 연관성 분석을 통하여 실시간 대응이 가능하다. 또한 알려진 공격뿐만 아니라 알려지지 않은 공격을 정확히 찾고 대응하기 위한 알려지지 않은 공격에 대한 탐지 룰 생성 기능을 제공한다. 현재까지 제공되는 anomaly 분석 기능들은 높은 false positive 발생으로 인하여 적절한 대응이 어려움이 있다. 하지만 SGS에서 실시간 탐지룰 생성기능을 이용하여 이러한 부분에 대해 대응이 가능하도록 한다.

본 시스템은 향후 BcN등의 차세대 인터넷 보안장치로 적용되어 보다 안전한 네트워크 인프라 제공에 기여 할 것으로 기대한다.

## 참 고 문 헌


[1] David Newman, Joel Snyder and Rodney Thayer, "Crying wolf: False alarms hide attacks," Network World, Jun. 2002.

[2] Jaeyeon Jung, Vern Paxson, Arthur W. Berger, and Hari Balakrishnan In Proc. IEEE Symposium on Security and Privacy, Oakland, CA, May, 2004

[3] Hyang-Ah Kim, Brad Karp, "Autograph : Toward Automated, Distributed Worm Signature Detection," USENIX Security Symposium July. 2004.

[4] 신승원, 강동호, 김기영, 장종수, "DPI(Deep Packet Inspection) 기술 분석," 전자통신동향분석. 2004.04.

[5] 허영준, 류걸우, 장종수, "Abnormal Traffic Detection for Network Intrusion Detection," SAM.2004.

[6] Packeteer, "Detect and limit DoS attacks," white paper, http://support.packeteer.com/.../prevent-dos-attacks.html

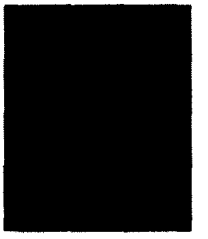
[7] Cisco Systems, "Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks," white paper, .http://www.cisco.com/warp/./newsflash.html, Feb. 2000.

[8] S. Northcutt, M. Cooper, M. Fearnow, and K. Frederick, "Intrusion Signature and Analysis," new riders, 2000.

[9] 안개일, 김기영, 류걸우, 장종수, "비정상 트래픽의 대역폭 제한 결정 메커니즘", JCCI 2004.04.

[10] 전용희, 류걸우, 장종수, "침입탐지시스템과 침입방지시스템의 기술 비교 및 동향", 정보통신연구진흥원 2004.6.9.

[11] 전용희, 김기영, 장종수, "네트워크-기반 침입방지 시스템 성능평가 기술 동향", 정보통신연구진흥원 2004.8.11.


김 기 영

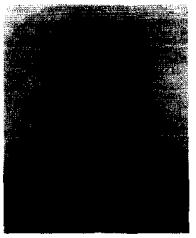
1984년 2월 ~ 1988년 2월 : 전남대학교 전산통계학과

1991년 2월 ~ 1993년 2월 : 전남대학교 전산통계학과 석사

1999년 2월 ~ 2002년 2월 : 충북대학교 대학원 전자계산학과 박사

1988년 2월 ~ 현재 : 한국전자통신연구원 책임연구원, 정보보호연구본부 보안게이트웨이연구팀 팀장

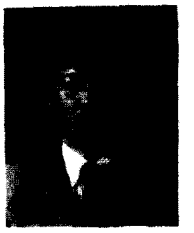
<관심분야> 네트워크 보안, 고성능 네트워크 침입탐지 및 대응



**오 진 태**

1986년 3월 ~ 1990년 2월 : 경북대학교 전자공학과 공학사
1990년 3월 ~ 1992년 2월 : 경북대학교 전자공학과 석사
1992년 2월 ~ 1998년 2월 : 한국전자통신연구원 선임연구원
1998년 2월 ~ 1999년 1월 : MinMax Tech. in St. Louis 연구원
1999년 2월 ~ 2001년 10월 : Engedi Networks Inc. in St. Louis Director
2001년 10월 ~ 2003년 1월 : Winnow Networks Inc. in St. Louis CTO, 부사장, Cofounder
2003년 3월 ~ 현재 : 한국전자통신연구원 선임연구원, 보안게이트웨이연구팀 과책

<관심분야> 네트워크보안, 비정상행위탐지기술, 고성능침입탐지엔진기술, 고속 classification 기술



**전 용 희**

1971년 3월 ~ 1978년 2월 : 고려대학교 전기공학과
1985년 8월 ~ 1987년 8월 : 미국 플로리다공대 대학원 컴퓨터공학과
1987년 8월 ~ 1992년 12월 : 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 1월 ~ 1978년 11월 : 삼성중공업(주)
1978년 11월 ~ 1985년 7월 : 한국전력기술(주)
1989년 1월 ~ 1989년 6월 : 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 7월 ~ 1992년 9월 : 미국 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA
1992년 10월 ~ 1994년 2월 : 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 3월 ~ 현재 : 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001년 3월 ~ 2003년 2월 : 대구가톨릭대학교 공과대학장 역임
2004년 2월 ~ 현재 : 한국전자통신연구원 정보보호연구단 보안게이트웨이연구팀 초빙연구원

<관심분야> 네트워크 보안, 인터넷 웜 탐지 및 대응