하드웨어 기반의 고성능 침입탐지 기술

High-Performance Intrusion Detection Technology in FPGA-Based Reconfiguring Hardware

u-IT839의 정보보호 이슈 특집

김병구 (B.K. Kim) 네트워크보안구조연구팀 연구원
윤승용 (S.Y. Yoon) 네트워크보안구조연구팀 선임연구원
오진태 (J.T. Oh) 네트워크보안구조연구팀 팀장
장종수 (J.S. Jang) 네트워크보안그룹 그룹장

목 차

인터넷의 발전과 더불어 네트워크 상에서의 침입 시도가 갈수록 증가되고 다변화됨으로써, 이에 대한 대응으로 많은 침입탐지시스템들이 개발되었다. 그러나, 현재의 대다수 침입탐지시스템들은 갈수록 증가하는 트래픽양을 처리하는 데 어려움이 있다. 즉, 기가비트 이더넷 환경과 같은 고속 네트워크 환경이 현실화되고 있고, 이를 바탕으로 한 대용량의 데이터를 처리할 수 있는 보안 분석 기법들에 대한 필요성이 대두되고 있다. 따라서, 본 논문에서는 고속 네트워크 환경에 적합한 하드웨어 기반의 고성능 침입탐지 기술에 대해서 설명한다. 이는 대용량의 트래픽 데이터들을 실시간으로 분석하기 위한 기술로써, 점점 고속화되고 대용량화되어 가는 대규모 네트워크 환경에서의 다양한 침입을 보다 빠르고 정확하게 탐지하고 대응하기 위한 기반을 제공한다.

Ⅰ. 서론

네트워크의 고속화 및 이를 바탕으로 한 대용량 데이터의 송수신은 침입탐지시스템의 적용 환경에도 많은 영향을 미치게 되었다. 또한, 인터넷의 발전과 더불어 네트워크 상에서의 침입 시도가 갈수록 증가되고 다변화됨으로써, 기존의 저속 침입탐지 기법에 대한 변화를 요구하고 있다. 다시 말해서, 갈수록 고속화되고 대용량화되는 네트워크 환경과 보다 다양해지는 침입 시도에 적절히 대응하기 위해서는 보다 빠른 시간 내에 많은 데이터를 분석할 수 있는 기법이 요구된다. 그러나, 현재의 대다수 침입탐지 시스템들은 갈수록 증가하는 트래픽양을 처리하는 데에 어려움이 있다. 즉, 기가비트 이더넷(Gigabit Ethernet) 환경과 같은 고속 네트워크 환경이 현실화되고 있기 때문에 이를 수용할 수 있는 보안 분석 기법들이 요구되고 있다[1],[2]. 따라서, 본 논문에서는 고속 네트워크 환경에서의 침입탐지 및 대응 기능을 제공하기 위한 하드웨어 기반의 고성능 침입탐지 기술을 설명한다. 이는 기가비트 이더넷 환경과 같은 고속 네트워크 환경에 적합한 기술로써, 하드웨어가 갖는 리소스의 한계를 최대한 극복할 수 있는 침입탐지 기법을 제공한다.

본 논문의 구성은 Ⅱ장에서 침입탐지시스템에 대한 기존의 연구 결과 및 동향들에 대해서 살펴보고, Ⅲ장에서 하드웨어 기반의 고성능 침입탐지 기술의 구성요소와 수행 메커니즘에 대해서 기술한다. Ⅳ장에서는 설명된 기술의 구현 결과 및 적용 환경을 기술하며, 마지막으로 Ⅴ장은 결론 및 최신 연구 동향에 대해 기술한다.

Ⅱ. 관련 연구

지금까지 최고의 보안 제품이라는 보편적인 인식하에 방화벽이 도입되었으나, 점점 다양해지는 침입 행위들에 대응하기 위해서 침입탐지시스템이나 가상 가설망 등의 보안 장비들이 부각되기 시작했다. 더 나아가 최근에는 침입방지시스템의 개념이 침입탐지시스템의 개념을 포괄하고 있다. 이는 유사한 개념이지만, 능동적 대처 능력 측면에서 차별화된다. 침입탐지시스템의 주기능이 네트워크 상에서 발생하는 악의적 침입 행위를 탐지하고, 이에 대해 사전에 정의된 정책에 따라 경고 메시지 전송 등을 수행하는 것이라면, 침입방지시스템은 침입을 탐지하는 것뿐만 아니라, 침입이 일어나는 것을 근본적으로 방어하는 것을 목적으로 하는 능동적 대응 개념을 포함하는 솔루션이다. 무엇보다도 이러한 시스템들 모두 정확한 침입탐지 능력에 바탕을 두고 있다고 할 수 있는데, 이와 같은 침입탐지시스템은 공공기관에서 높은 예산을 집행하고 있을 정도로 그 중요성이 높이 인식되고 있으며, 국내외적으로 여러 제품들이 연구 개발되고 있다. 그러나, 기존의 침입탐지시스템은 방대한 데이터 분석에 따른 성능 문제 및 오판 등과 같은 많은 문제를 가지고 있다.

현재의 침입탐지시스템이 지니고 있는 기술적 한계, 즉 문제점은 무엇보다도 패킷 분실률 및 침입 탐지율과 같은 침입탐지시스템의 성능 문제라 할 수 있다. 성능은 꾸준히 여러 개발자들에 의해서 개선되고는 있으나, 이는 돈과 시간이 많이 소요되는 작업이다. 그럼에도 불구하고 성능 개선은 무엇보다도 중요한 해결 과제이다. 또한, 점점 고속화, 대용량화되어 가는 네트워크 환경은 이에 대한 중요성을 더욱 증가시키고 있다. 여러 워킹 그룹에서 이러한 성능상의 요구를 수용하기 위한 연구가 진행되고 있으며, 실제로 많은 상업 제품들이 개발되었다. 대부분 100Mbps 이하 환경에서의 탐지 성능을 보증하고 200Mbps까지 동작 가능하며, 일부 핵심기술을 개발한 업체에선 기가비트 이더넷 환경까지 지원하고 있다. 이러한 기술들은 고속 트래픽 모니터링과 메모리 관리, 데이터베이스 관리 및 커널의 컨트롤이 가능해야 하며, 그만큼 좋은 인프라가 앞선 기술을 만들어 내고 있다고 볼 수 있다. 그러나, 이들에 대한 성능 분석 결과가 불분명하고 명확한 속도 향상 기법은 제시되고 있지 못하다. 이와 같은 필요성을 충족시키기 위한 기술로써 고속 침입탐지 기술을 하드웨어로 만들기 위한 노력들이 있었으나, 대다수

하드웨어 보안 시스템들은 제한된 리소스의 한계로 인해서 적용될 수 있는 패턴의 수에 제약을 가지고 있다. 따라서, 이에 대한 최대한의 적용이 가능하면서 실시간으로 침입탐지 기능을 수행하는 고속의 하드웨어를 만드는 것이 쉽지 않았다.

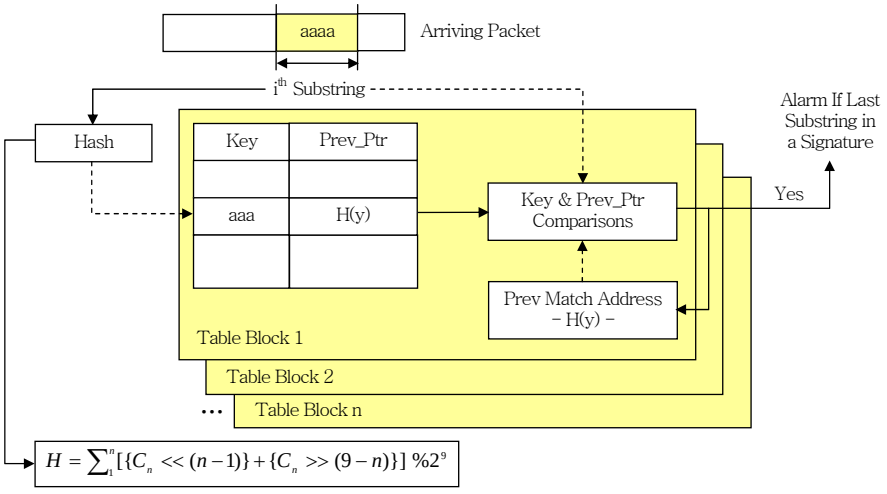
따라서, 본 논문에서는 이러한 성능 개선의 관점에서 하드웨어 기반의 고성능 침입탐지 기술을 설명하고, 이를 통한 고성능의 트래픽 분석 및 탐지 기능을 제공하고자 하였다. 소프트웨어 기반의 시스템과는 달리 하드웨어 기반의 시스템은 메모리 상의 제약을 동반하기 때문에 수많은 유해 트래픽 패턴들을 효율적으로 적용할 수 있는 기법이 요구된다. 따라서, 본 논문에서는 제한된 메모리 상에 최대한의 유해 트래픽 패턴들을 효율적으로 배치, 적용하면서도 성능 저하가 발생하지 않는 침입탐지 기술을 설명한다.

Ⅲ. 고성능 침입탐지 기술

1. 패턴 매칭 기법

하드웨어 기반의 고성능 침입탐지 기술은 기본적으로 고속의 패턴 매칭 기술을 기반으로 이루어진다. 가령, 특정 패턴을 갖는 단일 패킷을 침입으로 판정할 수도 있으나, 특정 패턴을 갖는 여러 패킷을 분석하여 침입으로 판정할 수도 있다. 또한, 침입 판정에 대한 정확도를 높이기 위해서 세션 상태 정보와 같은 여러 종류의 정보를 활용하기도 한다. 이와 같은 패턴 매칭 기법은 패킷 헤더와 페이로드에 대한 분석을 수행하며, 기 적용되어 있는 공격 시그니처에 기반하여 해당 패킷이 공격 패킷인지 아닌지의 유무를 판단하게 된다. 즉, 침입탐지 기능을 수행하기 위해서는 이와 같은 공격 시그니처들을 하드웨어 메모리 상에 적재하고 있어야 한다. 기본적으로 이와 같은 시그니처들은 대부분 페이로드 정보를 가지고 있으며, 이 부분에 대한 패턴 매칭 수행은 대부분의 침입탐지시스템에서의 성능 저하를 유발한다[3],[4]. 따라서, 이에 대한 효율적인 메모리 배치 및 매칭 기법이 요구된다.

(그림 1)은 상기의 목적을 위해서 패킷 페이로드에 대한 스트링 패턴 매칭 기법을 보인다. 이는 기본적으로 해시 값에 기반한 매칭 기법이며, 일정 단위의 서브 스트링 단위로 스트링 매칭을 수행한다. (그림 1)에서와 같이, 우선 각 시그니처 페이로드는 일정 단위의 서브 스트링 단위로 나뉘어 하드웨어 메모리에 적재되며, 메모리에 적재되는 위치는 해당 서브 스트링의 해시 값을 키로 사용한다. 이후, 패킷이 유입되면 유입 패킷의 페이로드 부분을 해당 크



(그림 1) 스트링 패턴 매칭 기법

기의 서브 스트링 단위로 이동해 가면서 해시 값을 구하고, 해당 해시 값을 키로 하여 저장되어 있는 서브 스트링 정보와 바로 매칭하는 방식으로 스트링 패턴 매칭을 수행한다. 이와 같은 수행은 메모리 블록마다 동시에 수행되며, 이를 통해서 즉각적인 매칭 유무를 알아내게 된다.

<표 1>은 이와 같은 스트링 패턴 매칭 기법을 사용한 본 연구진의 ATPS 시스템과 다른 기법들과의 성능 비교를 나타낸다[5]-[8]. <표 1>에서와 같이, ATPS 시스템은 "Logic Cells/Char"의 값이 0.9로 다른 기법들에 비해서 메모리 사용 측면이 월등히 좋음을 알 수 있다. 비록, 성능에서는 떨어지는 결과를 나타내고 있으나, 이는 125MHz의 클럭 속도에 맞추어 개발된 프로토타입이기 때문이며 기술적으로는 10.7Gbps의 성능까지 제공될 수 있다.

이외에, 패킷 헤더 부분에 대한 패턴 매칭 기법은 (그림 2)에서와 같이, TCP/IP 프로토콜 헤더를 구성하는 필드들의 크기에 따라 8비트, 16비트, 32비트의 TCAM을 기본으로 하여 매칭을 수행한다[9]. 이는 최종적으로 256비트의 매칭 결과를 출력하기 때문에 최대 256개의 헤더 조합에 대한 매칭을 수행할 수 있다. 이에 대한 결과는 스트링 패턴 매칭 수행과 유기적으로 상호 동작하며, 이를 통해서 최종 침입 유무를 판단하게 된다.

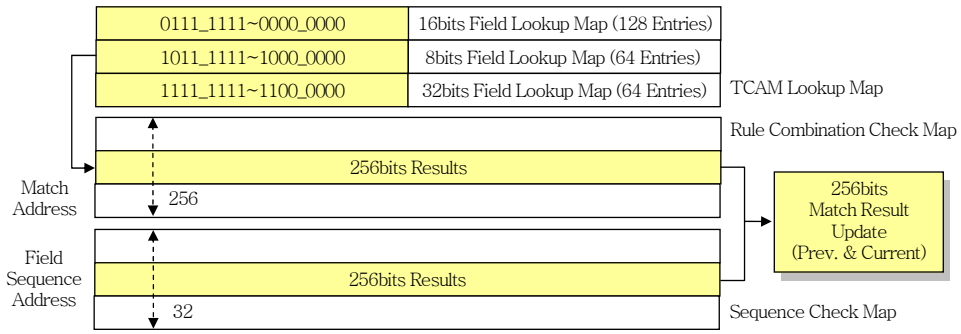
2. 휴리스틱 분석 기법

휴리스틱 분석 기법을 이용한 고성능 침입탐지 기술은 패킷량과 시간 임계치에 기반한 유해 트래픽 감지 기법이다. 일반적으로 서비스 거부 공격이나 포트 스캔 공격과 같은 네트워크 상의 이상 유해 트래픽은 다량의 패킷 발생을 특징으로 하기 때문에 [10], 하나의 패킷이 공격 패턴에 일치되더라도 이를 공격으로 판정하기는 어렵다. 따라서, 동일한 패턴의 패킷이 다량으로 유입되었을 때 침입으로 판정하는 것이 보다 높은 정확도를 제공하게 된다. 여기에서 동일한 패턴에 대한 패킷 분석은 앞서 설명한 패턴 매칭 기법을 동일하게 사용한다.

(그림 3)은 상기의 목적을 위해서 패킷량과 시간 임계치에 기반한 휴리스틱 분석 기법을 개략적으로 도시한 개념도이다.

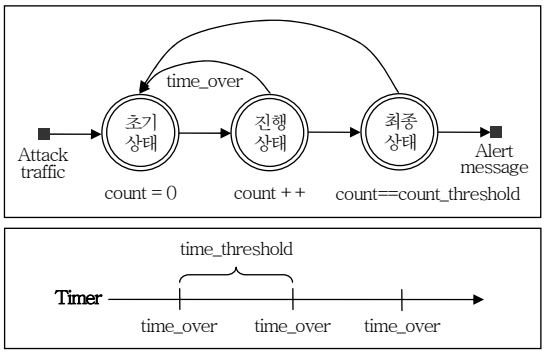
〈표 1〉 패턴 매칭 기법 성능 비교

Description	Input Bits	Device	Throughput (Gbps)	Logic Cells/Char
State Tables	64	Altera EP20K400E	10.1	15
Pre-decoded CAMs	32	Virtex2 6000	9.7	3.56
Granidt	32	VirtexE 1000	2.2	15.2
Parallel Comparators	32	Altera EP20K	2.9	10.6
ATPS[ETRI]	32	Virtex II Pro	2.0	0.9



(그림 2) 헤더 패턴 매칭 기법

(그림 3)에서와 같이, 공격 패턴에 일치하는 패킷이 최초 유입되면 초기 상태에서 패킷량에 대한 카운트가 증가되면서 진행 상태로 전이된다. 여기에서, 공격 패턴에 일치하는 패킷이 계속적으로 유입되어 카운트가 기 정의된 임계치에 도달하면 최종 상태로 전이되어 경보가 발생하게 된다. 그러나, 카운트에만 의존한 상태 전이는 소량의 패킷에 대한 장기간의 카운트에 의한 경보 발생 가능성이 있기 때문에 시간 임계치에 따른 상태 전이가 요구된다. 따라서, 타이머에 의한 시간 임계치를 측정하고, 시간 임계치에 도달한 경우에 진행 상태를 초기 상태로 재 전이한다. 이와 같은 방식은 서비스 거부 공격 및 포트 스캔 공격과 같은 네트워크 상의 이상 유해 트래픽에 대한 탐지 정확도를 높일 수 있도록 도와준다.



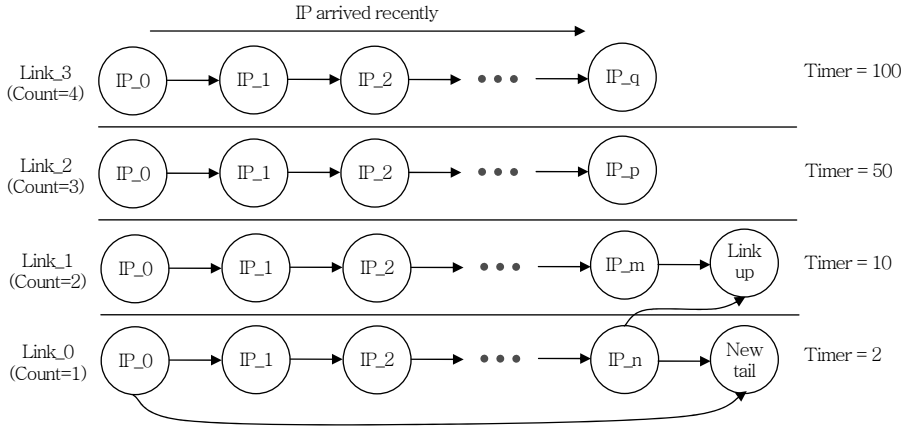
(그림 3) 휴리스틱 분석 기법

마지막으로, (그림 4)는 상기의 휴리스틱 분석 기법에 쓰이는 목적지 IP 엔트리 관리 기법을 보여준다.

서비스 거부 공격과 포트 스캔 공격은 단일 목적지 IP에 대해서 이루어지기 때문에 한정된 하드웨어 메모리 상에서 각 목적지 IP를 전부 추적하기는 어렵다. 때문에, 타이머 및 공격 패턴에 일치된 패킷의 빈도에 따라 지속적으로 목적지 IP 엔트리를 관리해 줄 필요가 있으며, 이를 통해서 제한된 메모리 상에서의 효율적인 공격 탐지가 가능하다.

3. 세션 관리 기법

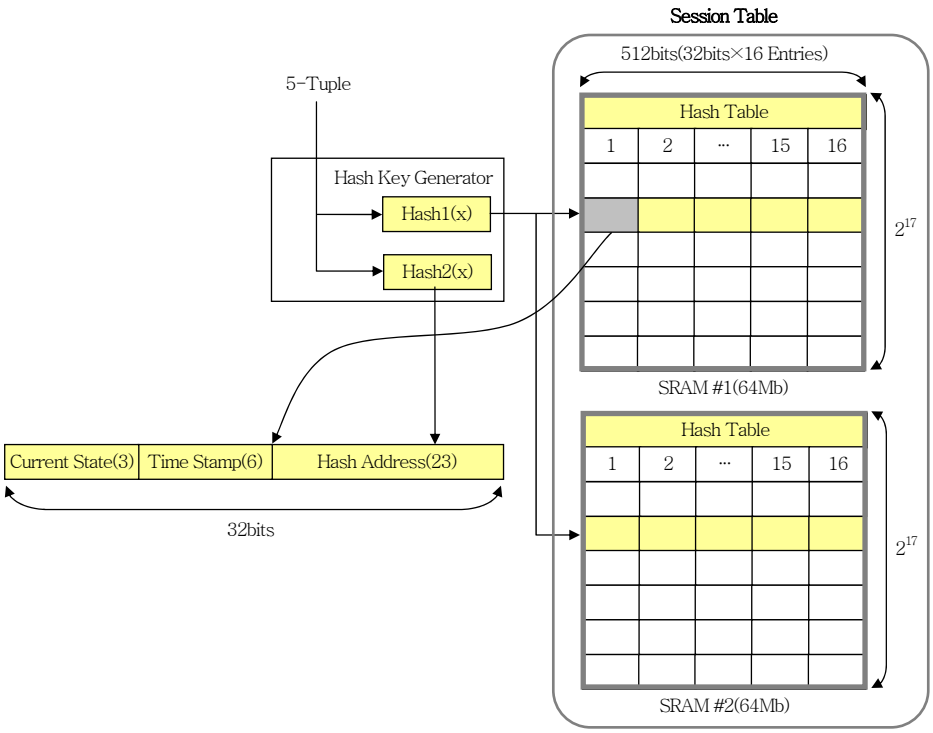
침입탐지시스템이 가지고 있는 문제점 중 하나가 오탐률이라고 앞장에서 기술한 바 있다. 지금까지 오탐률을 줄이기 위한 많은 방법들이 연구되어 왔는데, SPI 기술은 침입탐지에 세션 상태 정보를 이용하여 오탐률을 상당히 줄일 수 있는 기술이다. SPI 기능이 없는 침입탐지시스템은 stick이나 snot과 같은 툴에 의해 엄청난 잘못된 경보가 발생하여 제대로 된 기능을 수행하기가 어렵다. SPI 기능을 제대로 수행하기 위해서는 효율적인 세션 관리 기법이 필수적인데, 기가비트 네트워크 환경에서 패킷 지연이나 손실 없이, 즉 성능저하 없이 100만 세션 이상을 관리 및 추적하여 패턴 매칭과 같은 침입탐지 기법에 필요한 상태정보를 실시간으로 생성해 낼 수 있어야 한다.



(그림 4) 목적지 IP 엔트리 관리 기법

실시간 세션 상태 기반 침입탐지 기능을 수행하기 위해서는 효율적인 세션 테이블 관리 기법이 필수적이다. 이를 위해 본 논문에서는 2중 해시 구조와 N-way set associative table 구조를 사용하고 있다. 우선 패킷이 입력되면 패킷 파서를 거쳐 세션 테이블에 필요한 필드들을 미리 추출한다. 추출된 5-tuple(프로토콜, 소스와 목적지의 IP 주소, 포트 번호) 정보를 입력으로 받아 2중 해시기는 Hash1(x)와 Hash2(x) 함수를 이용하여 해당 세션 엔트리를 인덱스하고 관리한다. 여기서 사용되는 Hash1(x)와 Hash2(x) 함수는 XOR 함수나 CRC 함수 등 임의의 적합한 함수일 수 있다. 첫번째 해시 함수인 Hash1(x)는 보다 빠른 세션 테이블 검색을 위해, hash collision을 허용하는 각각의 hash set을 포인트하는 인덱스를 생성하는 데 사용된다. 두번째 해시 함수인 Hash2(x)는 Hash1(x)에 의해 포인트된 hash set 안에서 각각의 세션 엔트리를 구별하는 데 사용되는 hash address를 생성하는 데 사용된다. 세션 테이블의 각 hash set 안에는 N개의 세션 엔트리를 포함할 수 있어, N-way set associative session table 구조를 하고 있다. (그림 5)의 세션 테이블은 하나의 세션 엔트리가 32bit length를 갖는 32-way set associative session table을 구성한 것이다.

하나의 세션 엔트리에는 current state, time stamp, hash address를 포함하고 있다. Current state는 현재 해당 세션의 연결 상태 정보를 포함하고 있고, time stamp는 세션 테이블이 full이 되었을 때 어떤 세션 엔트리를 삭제할 것인가를 결정하는 데 이용되고, hash address는 동일한 hash set 안에서 각각의 세션 엔트리를 구별하기 위해 사용된다. 여기서 time stamp는 내부 타이머에 의해 해당 세션이 접근될 때마다 갱신된다. 세션 테이블의 hash set이 full이 되어 더 이상 해당 hash set에 새로운 세션을 할당할 수 없을 때, 현재 타이머의 시간과 세션 엔트리의 time stamp를 비교하여 가장 오래된 세션을 새로운 세션으로 대체한다. 즉 LRU 알고리듬을 적용한다. 또한 TCP 세션 중에는 RST이



(그림 5) 세션 테이블 구조

나 FIN 패킷을 보내지 않고 종료되는 경우가 발생하는데, 이러한 세션은 세션 테이블에서 적극적으로 제거해줘야 한다. 이 때에도 세션 엔트리의 time stamp를 이용하여 관리자가 정해놓은 특정 time-out 임계치(threshold)를 넘으면 해당 세션 엔트리를 바로 삭제한다.

세션 테이블이 full이 되어, 즉 해당 hash set이 full이 되어 기존의 세션 중에 아직 종료가 되지 않은 것이 새로운 세션으로 대체되면 잘못된 세션 상태 정보를 생성하게 되므로 세션 테이블 관리 기법에 있어서 세션이 full out 될 확률은 아주 중요하다. 이것은 침입탐지 오탐률로 직결되기 때문이다. 세션 테이블 각각의 hash set에 할당되는 세션의 개수 분포는 식 (1)과 같은 정규분포를 따른다.

$$f(x) = \frac{1}{\sqrt{2\pi}} \exp\{-\frac{1}{2\sigma^2}(x-\mu)^2\} \quad (1)$$

$$Z = \frac{X-\mu}{\sigma} \quad (2)$$

$$P(a < X < b) = P(\frac{a-\mu}{\sigma} < Z < \frac{b-\mu}{\sigma}) \quad (3)$$

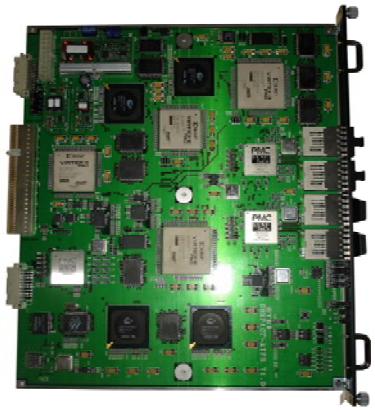
이를 (2)와 (3)을 이용하여 표준화한 후, 32-way set associative session table에서 세션이 full out 될 확률을 계산하면 P{X>32} = P{Z>8.3} 이다. 이것은 8.3 시그마로 거의 0%에 가깝다.

결국, 본 논문의 2중 해시 구조와 N-way set associative table 구조를 이용한 세션 테이블 관리 기법은 최소한의 하드웨어 리소스를 사용하면서도 원하는 기능과 성능을 모두 만족시킬 수 있는 장점을 갖는다.

Ⅳ. 시스템 구현 및 적용

본 논문에서 설명한 하드웨어 기반의 고성능 침입탐지 기술은 기존의 침입탐지시스템이 지닌 성능 문제를 개선하고자 개발되었다. 즉, 기가비트 이더넷 환경과 같은 고속 네트워크 환경에서의 보다 정확한 고속 침입탐지 기능을 제공하고, 이를 통해 보다 빠른 대응이 가능하도록 하고자 하였다. 본 연구진에서는 이를 바탕으로 한 프로토타입으로써 ATPS 시스템을 개발하였다. 기본적으로 ATPS 시스템의 하드웨어 로직은 Xilinx FPGA 상에서 동작하도록 구현되었으며[11], CPU를 통해 침입 패턴이 탐지 정책으로써 적용되도록 하였다.

(그림 6)은 ATPS 시스템의 일환으로 제작된 프로토타입 보드를 나타내며, 이를 여러 도메인으로 구성된 시험 망 내에 설치하여 지속적으로 시험 운용하고 있다. 본 논문에서 기술된 고성능 침입탐지 기술을 적용한 ATPS 시스템은 고속의 네트워크 환경에 적용되는 것을 목표로 시험되고 있으며, 수많은 패턴의 공격 유형들과 서비스 거부 공격 및 포트 스캔 공격과 같은 이상 유해 트래픽들에 대한 빠른 징후 포착 및 대응을 수행할 수 있도록 해준다는 측면에서 대규모 네트워크 환경에 적용되어 보안 제어를 용이하게 해줄 수 있는 장점을 가지고 있다.



(그림 6) ATPS 보드

Ⅴ. 결론 및 최신 연구 동향

본 논문에서는 기가비트 이더넷 환경과 같은 고속 네트워크 환경에 적합한 보안 제어 기능을 제공하기 위한 기반 기술로써, 하드웨어 기반의 고성능 침입탐지 기술을 설명하였다. 또한, 이러한 기술의 필요성과 수행 기법들에 대해서 간략히 설명하였다. 무엇보다도, 이러한 기술을 바탕으로 자체 개발한

ATPS 시스템을 통해서 여러 유형의 침해 행위들과 이상 유해 트래픽에 대한 고성능의 침입탐지 기능을 제공하고자 하였다. 또한, 이와 같은 유해 트래픽에 대한 이상 징후를 보다 빨리 탐지해 냄으로써 패킷 처리에 대한 고속화를 추구함과 동시에 네트워크를 통한 침해 행위로부터의 피해를 최소화하고자 노력하였다.

앞으로는 여러 시험을 통해서 나오는 문제점들을 보완하고, 보다 정확한 침입탐지 기능을 제공하기 위한 기법들을 연구해 나가고자 한다. 즉 고속화되어 가는 네트워크 환경에서의 보다 나은 성능 향상과 오탐률을 낮추기 위해서, 보다 효율적인 패킷 처리 메커니즘을 추가적으로 고려하고자 한다. 이러한 연구는 보다 많은 데이터를 고속으로 정확하게 처리함으로써 간혹 놓치기 쉬운 여러 위협으로부터 자신의 네트워크를 보호하는 데 도움을 줄 것이다.

이외에, 최근에는 기존의 시그니처 기반의 공격 탐지 방법으로는 어려운, 즉 공격 패턴이 알려지지 않은 zero-day attack과 같은 공격이 이루어지는 상황에서 네트워크의 상태를 파악하기 위한 이상상태(anomaly) 분석 방법에 대한 연구도 활발히 진행되고 있으며, 이를 통한 시그니처 자동 생성 기법들도 활발히 논의되고 있다.

약 어 정 리

ATPS	Adaptive Threat Prevention System
FPGA	Field Programmable Gate Array
LRU	Least Recently Used
SPI	Stateful Packet Inspection

● 용 어 해 설 ●

서비스 거부 공격: 시스템의 정상적인 동작을 방해하는 공격 수법으로, 대량의 데이터 패킷을 통신망으로 보내거나 이메일로 보내는 식의 공격

FPGA: 이미 설계된 하드웨어를 반도체로 생산하기 직전 최종적으로 하드웨어의 동작 및 성능을 검증하기 위해 제작하는 중간 개발물 형태의 집적 회로(IC). 반도체 제조업자 측에서 보면 양산되어 일반적 용도로 사용되므로 범용 IC의 범주에 속하고, 사용자 측에서 보면 사용자 요구에 맞게 프로그래밍하여 사용할 수 있으므로 주문형 반도체(ASIC) 범주에 속한다.

참 고 문 헌

[1] Byoung-Koo Kim, Jong-Su Jang, Sung-Won Sohn, and Tai M. Chung, "Design and Implementation of Intrusion Detection System Base on Object-Oriented Modeling," *in Proc. of the Int'l Conf. on Security and Management*, June 2002, pp.10-15.

[2] C. Kruegel, F. Valeur, G. Vigna, and R. Kemmerer, "Stateful Intrusion Detection for High-Speed Networks," *in Proc. of the IEEE Symp. on Security and Privacy*, 2002, pp.266-274.

[3] M. Roesch. "Snort-Lightweight Intrusion Detection for Networks," *in Proc. of the USENIX LISA '99 Conf.*, Nov. 1999.

[4] S. Kumar and E. Spafford, "A Pattern Matching Model for Misuse Intrusion Detection," *in Proc. of the 17th National Computer Security Conf.*, Oct. 1994, pp.11-21.

[5] M. Aldwairi, T. Conte, and P. Franzon, "Configurable String MatchingHardware for Speeding Up Intrusion Detection," *in ACM SIGARCH Computer Architecture News*, Mar. 2005, pp.99-107.

[6] I. Sourdis and D. Pnevmatikatos, "Pre-decoded CAMs for Efficient and High-Speed NIDS Pattern Matching," *in Proc. of 12th IEEE Symp. on Field Programmable Custom Computing Machines*, Apr. 2004.

[7] M. Gokhale, D. Dubois, A. Dubois, M. Boorman, S. Poole, and V. Hogsett, "Granidt: Towards Gigabit Rate Network Intrusion Detection Technology," *in Proc. of the Int'l Conf. of Field Programmable Logic and Applications*, 2002.

[8] Y. Cho, S. Navab, and W. Mangione-Smith, "Specialized Hardware for Deep Network Packet Filtering," *in Proc. of Int'l Conf. on Field Programmable Logic and Application*, Sep. 2002.

[9] W. Richard Stevens, TCP/IP Illustrated Volume I: The Protocols, Addison Wesley, 1994.

[10] Thomas Ptacek and Timothy Newsham, "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection," Secure Networks Inc., 1998.

[11] http://www.xilinx.com