DDoS 공격 탐지를 위한 확장된 블룸 필터 기반의 효율적인 목적지 주소 모니터링 기법

정회원 유 경 민*, 심 상 헌*, 한 경 은*, 소 원 호**, 종신회원 김 영 선***, 김 영 천*°

Efficient Bloom Filter Based Destination Address Monitoring Scheme for DDoS Attack Detection

Kyoung-Min Yoo*, Sang-Heon Sim*, Kyeong-Eun Han*, Won-Ho So** ***Regular Members,***
Young-Sun Kim***, Young-Chon Kim*° ***Lifelong Members***

요 약

최근 DDoS(Distributed Denial of Service) 공격이 네트워크 주요 위협요소로 부각되고 있다. 이들 공격은 주로 특정 victim에 다량의 패킷을 전송하는 특징을 가지기 때문에 발생 패킷들의 목적지 IP 주소를 모니터링하여 공격을 탐지하는 기법들이 제안되었다. 기존의 블룸 필터 탐지 기법은 구조가 간단하고 실시간 탐지가 가능한 장점을 갖지만 목적지 IP 주소의 세부 주소를 독립적으로 모니터링하므로 오탐지율이 높은 문제점을 가진다. 이러한 문제점을 해결하기 위하여 본 논문에서는 목적지 주소의 세부 주소 간 연관성을 정의하여 모니터링하는 확장된 블룸 필터 기반의 효율적인 목적지 주소 모니터링 기법을 제안한다. 제안한 기법에서는 세부 주소를 모니터링하는 테이블뿐만 아니라 세부 주소 간 연관성을 모니터링하는 추가 테이블을 유지한다. 시뮬레이션을 통한 성능 평가 결과 제안한 기법은 기존의 블룸 필터 탐지 기법보다 낮은 오탐지율을 보였다. 또한 공격 탐지 정확성 향상을 위하여 다층의 모니터링 구조를 제안하였으며, 층수와 추가 테이블의 수의 변화에 따라 정확도를 높일 수 있었다.

Key Words : DDoS, Attack detection, Packet monitoring, Bloom Filter

ABSTRACT

Recently, DDoS (Distributed Denial of Service) attack has emerged as one of the major threats and it's main characteristic is to send flood of data packets toward a specific victim. Thus, several attack detection schemes which monitor the destination IP address of packets have been suggested. The existing Bloom Filter based attack detection scheme is simple and can support real-time monitoring. However, since this scheme monitors the separate fields of destination IP address independently, wrong detection is comparatively high. In this paper, in order to solve this drawback, an efficient Bloom Filter based destination address monitoring scheme is proposed, which monitors not only separate fields but also relationship among separate fields. In the results of simulation, the proposed monitoring scheme outperforms the existing Bloom Filter based detection scheme. Also, to improve the correctness of detection, multi-layerd structure is proposed and the correctness of result is improved according to the number of layers and extra tables.

※ 본 연구는 한국전자통신연구원과 한국산업기술재단의 지역인력양성사업의 지원을 받아 수행된 연구임.
* 전북대학교 영상정보신기술연구소, ** 순천대학교 컴퓨터교육과, *** 한국전자통신연구원,
전북대학교 영상정보신기술연구소 (yckim@chonbuk.ac.kr)(°: 교신저자)
논문번호 : KICS2007-11-499, 접수일자 : 2007년 11월 6일, 최종논문접수일자 : 2008년 3월 12일

Ⅰ. 서 론

인터넷 이용자의 급속한 증가와 다양한 서비스 요구로 인하여 인터넷 환경은 점점 복잡해지고 망 트래픽도 급격히 증가되고 있지만 망 자원을 효과적으로 관리하고 서비스 품질을 보장하는 제어 기술의 발전은 아직 미진한 상태이다. 국내외적으로 활발하게 추진되고 있는 NGN (Next Generation Network)과 광대역통합망 (BcN:Broadband convergence Network) 등의 경우 이러한 기술의 개발 및 도입에 대한 요구는 더욱 증가될 전망이다. 특히 기존 네트워크 보안의 한계를 극복하는 것이 통합망을 효과적으로 운용하기 위해 선결해야 할 문제로 인식되고 있으며 이에 관한 다양한 연구가 진행 중에 있다[1,2].

최근 네트워크 주요 위협 요소로 부각되고 있는 DDoS (Distributed Denial of Service) 공격의 경우 취약성이 노출된 여러 호스트에 에이전트 프로그램을 설치한 후 원격으로 조정하여 특정 시스템으로 동시에 많은 패킷을 전송하는 특성을 가진다. 그러나 기존의 네트워크 보안 기법들은 MAC spoofing이나 IP snipping 등과 같이 단일 시스템에서의 지역적인 보안 방식만을 수행하고 있어 분산 공격 상황을 실시간으로 감지하기 어렵다. 또한 공격에 대응하기 위해서 라우팅 프로토콜에 의존하므로 대응 시간이 느리며 복잡도가 증가하는 문제점을 가진다. 따라서 이러한 문제점을 해결할 수 있는 효율적인 공격 탐지 기법이 요구되고 있다.

현재 널리 사용되고 있는 Netflow나 MRTG (Multi Router Traffic Grapher)와 같은 네트워크 모니터링 툴은 패킷의 특성을 분석하여 네트워크가 유발하는 트래픽 중 TCP, UDP나 ICMP트래픽의 양을 측정하여 가장 많은 트래픽을 유발하는 IP를 정렬하는 기능을 제공한다. 이러한 링크 리스트 구조를 이용하는 탐지 기법들은 패킷의 패턴을 모니터링하기 위해 동적 메모리 할당의 추가적인 처리가 필요하며 패킷의 종류가 증가할수록 시스템 자원을 많이 소모하는 문제점이 있다.

한편 패킷들의 목적지 주소를 모니터링하여 공격 트래픽을 판별하는 기법들이 제안되었는데 이는 앞서 언급한 바와 같이 DDoS 공격이 특정 시스템으로 대량의 패킷을 전송하는 특성을 이용한 것이다. 기존에 제안된 MULTOPS는 그 구조상 동적으로 메모리를 관리하기 때문에 목적지 주소의 수가 증가할수록 추가적인 메모리 공간이 필요하며 메모리 할당에 따른 복잡도가 증가하는 문제점이 있다. 이를 해결하기 위해 블룸 필터 기반의 탐지 기법이 제안되었다[3,4]. 블룸 필터 기반의 탐지 기법은 구조가 간단하고 실시간 탐지가 가능하지만 IP 주소를 세부 주소로 분리하여 각각을 독립적으로 모니터링함으로써 오탐지율이 높은 문제점이 있다.

그러므로 본 논문에서는 기존 목적지 주소 모니터링 기법들의 문제점을 해결하기 위해 확장된 블룸 필터 기반의 목적지 주소 모니터링 기법을 제안한다. 제안된 기법에서는 간단한 테이블 구조를 이용하므로 실시간 모니터링을 제공할 수 있을 뿐만 아니라 IP 주소를 구성하는 세부 주소들의 연관성을 정의하여 모니터링하는 추가 테이블을 이용하기 때문에 보다 정확하게 공격 트래픽을 탐지할 수 있다. 또한 다층 구조를 설계하여 공격 패킷과 정상 패킷을 분리하여 모니터링함으로써 보다 정확한 공격 탐지를 수행할 수 있다.

본 논문의 구성은 다음과 같다. 먼저 Ⅱ장에서는 기존의 목적지 IP 주소 모니터링 기반 공격 탐지 기법들을 소개한다. Ⅲ장에서는 본 논문에서 제안한 확장된 블룸 필터 기반의 목적지 주소 모니터링 기법의 구조와 공격 탐지 알고리즘을 소개하고 탐지 정확도를 향상시키기 위한 다층 구조에 대해 기술한다. 또한 제안한 기법의 성능 평가를 위해 오탐지율 관점에서 수행한 시뮬레이션 결과들을 Ⅳ장에서 분석한다. 마지막으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 연구

DDoS 공격 탐지를 위하여 엔트로피, Chi-Square 분석 그리고 목적지 IP 주소 등을 이용한 여러 기법이 제시되었다[5,6]. 본 논문에서는 목적지 주소 기반의 탐지 기법에 초점을 맞추었다.

목적지 주소를 기반으로 한 탐지 기법들은 근원지 라우터를 통해 전송되는 패킷들의 목적지 주소를 모니터링함으로써 실시간 공격 탐지를 그 목적으로 하며, 대표적인 방법으로 MULTOPS (Multi-Level Tree for Online Packet Statistics)와 블룸 필터 기반의 탐지 기법이 있다.

MULTOPS는 각 subnet prefix에 대한 입력 패킷 비율과 출력 패킷 비율을 기록하는 노드들의 트리 구조로 IPv4 전체 주소를 표현하기 위해 4-레벨 256-배열로 운영된다. 트리의 각 노드는 256개의 레코드 테이블로 구성되고 각 레코드는 3개의 필드 (입력 비율, 출력 비율, 자식노드를 지칭하는 포인

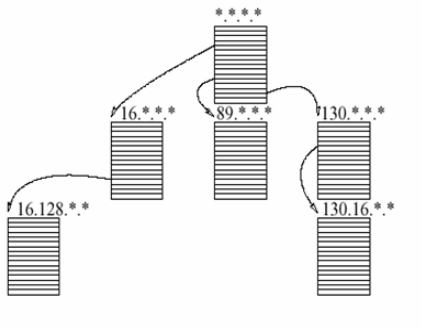

그림 1. MULTOPS의 트리 구조

터)로 구성되어 있다. 그리고 트리의 레벨에 따라 모든 패킷 비율과 공통적으로 0-bit, 8-bit, 16-bit 또는 24-bit의 선행 비트를 가지는 입력 IP 주소와 출력 IP 주소에 대한 모든 패킷 비율을 테이블에 저장한다. 즉, 트리의 레벨이 높아질수록 패킷 비율은 긴 선행 비트를 가지게 된다. 또한 루트 노드(root node)는 패킷 비율과 주소를 통합하여 가지고 있어야 한다. 예를 들어 그림 1에서 보는 바와 같이 루트 노드의 90번째 레코드는 8-bit의 선행비트 89를 가진 주소와 패킷 비율들을 가지고 있고, 포인터 노드는 89 선행 비트를 가진 주소(즉, 89.0.*.*, 89.1.*.*, 89.2.*.*, 등)들의 패킷 비율들이 모여 계속적으로 정보를 추적한다. 하지만 MULTOPS는 목적지 IP 주소를 트리 구조로 구현하여 모니터링하는 시스템이기 때문에 새로운 목적지 주소가 발생할 때마다 지속적으로 동적인 메모리를 할당해야 하며 목적지 주소의 종류가 증가할수록 트리 분할에 따른 처리의 복잡성이 증가하는 문제점이 있다.

한편 블룸 필터 기반의 공격 탐지 기법은 그림 2와 같은 구조를 이용하여 패킷을 모니터링함으로써 공격을 탐지하는 방법으로 2차원의 배열 구조[k][m]을 이용한다. k는 세부 주소의 수를 나타내는 값으로 현재 사용하는 IPv4의 주소 체계가 32비트 체계로 각 1바이트 사이에 도트로 분리되어 총 4개의 세부 주소로 나눌 수 있으므로 그림 1의 예시는 k가 4인 경우이다. m은 세부 주소의 모니터링을 위한 bin의 수를 나타내는 값으로 세부 주소 각각이 가질 수 있는 값의 범위가 8비트의 경우 0~255이므로 그림 1의 예시는 m이 256인 경우이다. 결과적으로 배열의 구성 요소인 bin 각각은 해당 세부 주소의 발생 횟수를 세는 카운터이다.

블룸 필터 기반 공격 탐지 기법에서는 패킷이 발생하면 목적지 IP 주소의 세부 주소를 이용해 테이블의 인덱스 값으로 변환하고 해당 bin의 카운터 값을 1씩 증가시킨다. 즉, 그림에서 보는 바와 같이 Hash_i() 함수를 이용하여 IP 세부 주소를 테이블의 인덱스 값으로 변환하고 인덱스 값에 의해 결정된 bin의 카운터를 1씩 증가시킨다. 최종적으로 4개의 세부 주소에 대한 bin의 값을 모두 증가시킨 후 모든 bin의 값이 임계값을 초과할 경우 그 목적지 IP 주소로 향하는 패킷을 공격 트래픽으로 간주한다.

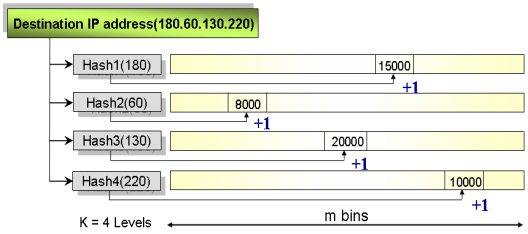

그림 2. 블룸 필터 기반 목적지 주소 모니터링 구조

그러나 각 세부 주소를 독립적으로 관리함으로써 하나의 bin이 유일한 IP 주소에 의해서 증가되는 것이 아니라, 서로 다른 IP 주소이지만 같은 위치에 동일한 세부 주소를 가지는 경우 여러 IP 주소에 의해 특정 bin의 카운터 값이 빠르게 증가되는 문제점이 발생한다. 예를 들어 100.xxx.xxx.xxx, xxx.50.xxx.xxx, xxx.xxx.200.xxx 그리고 xxx.xxx.xxx.150 에 해당하는 목적지 IP 주소들이 많이 발생하였다고 하자. 이 때 100.50.200.150 값을 가지는 IP 주소는 처음 발생하였다 하더라도 각 세부 주소의 카운터 값들이 증가되어 있어 임계값을 초과하게 되면 공격 트래픽으로 탐지되는 것이다.

이러한 문제점을 해결하기 위해 본 논문에서는 기존의 블룸 필터 기반 공격 탐지 기법을 개선하여 실시간 모니터링을 제공하면서도 오탐지율을 줄일 수 있는 확장된 블룸 필터 기반의 효율적인 패킷 모니터링 기법을 제안한다.

Ⅲ. 확장된 블룸 필터 기반 목적지 주소 모니터링 기법

3.1 확장된 블룸 필터 기반의 공격 탐지 구조

기존의 블룸 필터 기반 공격 탐지 기법은 목적지 IP 주소를 세부 주소로 분리하여 개별적으로 모니터링하기 때문에 오탐지율이 높다. 따라서 본 논문에서는 오탐지율을 낮추기 위해 확장된 블룸 필터 기반의 목적지 주소 모니터링 기법을 제안한다. 제안된 기법의 모니터링 구조는 그림 3에 제시된

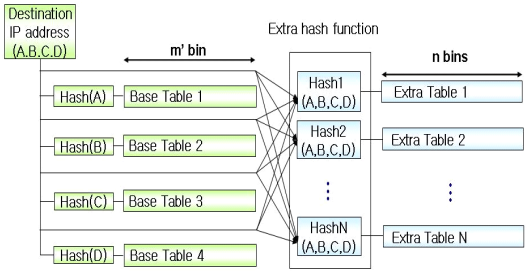

그림 3. 확장된 블룸 필터 기반의 목적지 주소 모니터링 구조

것과 같이 크게 기본 테이블(Base table)과 추가 테이블(Extra table)로 구성된다. 먼저 기본 테이블은 기존의 방식과 같이 4개의 테이블로 구성되며 운영 방식도 동일하게 적용하되 더 작은 수의 bin들을 사용한다. 추가 테이블은 세부 주소간의 연관성을 모니터링하는 테이블로써 네트워크 상황에 따라 1개부터 N개까지 다양한 형태로 구성할 수 있다.

제안된 기법의 전체적인 공격 탐지 동작은 그림 4의 알고리즘을 따른다. 먼저 목적지 IP 주소가 A.B.C.D인 패킷이 발생되면 도트로 구분된 각 세부 주소들은 해쉬 함수, Hash()에 의해 각 기본 테이블의 인덱스 값으로 변환된다. 이에 따라 변환된 인덱스 값에 해당되는 bin 값을 1씩 증가시킨다. 또한 추가 테이블의 인덱스 값을 구하기 위해 추가 해쉬 함수, Hashi()를 사용하여 추가 테이블의 인덱스 값을 생성한다. 이에 따라 변환된 인덱스 값에 해당되는 bin 값을 1씩 증가시킨다. 최종적으로 기본 테이블 4개와 추가 테이블의 해당 bin 값들이 모두 증가되면 미리 결정된 임계값과 비교하여 모든 bin 값이 임계값을 초과하는 경우 목적지 주소, A.B.C.D를 가진 패킷은 비정상 트래픽으로 결정된다. 사용되는 해쉬 함수는 빠른 계산을 위해 간결한 비트 연산을 이용한다.

앞서 기술된 구조와 알고리즘을 기반으로 제안된 기법의 특성을 다음과 같이 정리할 수 있다. 먼저 실시간성으로 본 기법은 고정된 크기의 공간을 사용하기 때문에 링크 리스트(linked list)나 트리(tree) 구조처럼 동적 할당이 필요 없으므로 처리 시간이 짧고, 해쉬 함수를 비트 논리 연산으로 정의하기 때문에 빠른 연산이 가능하다.

예를 들면, 패킷의 평균 크기를 1,000 byte로 했을 경우 약 2 Gbps의 망에서 실시간 탐지가 가능하다. 또한 테이블의 수와 테이블 당 bin의 수를 네트워크 상황에 따라 조절할 수 있으므로 확장성이 높다. 따라서 본 기법은 추후 IPv6 환경의 모니터링

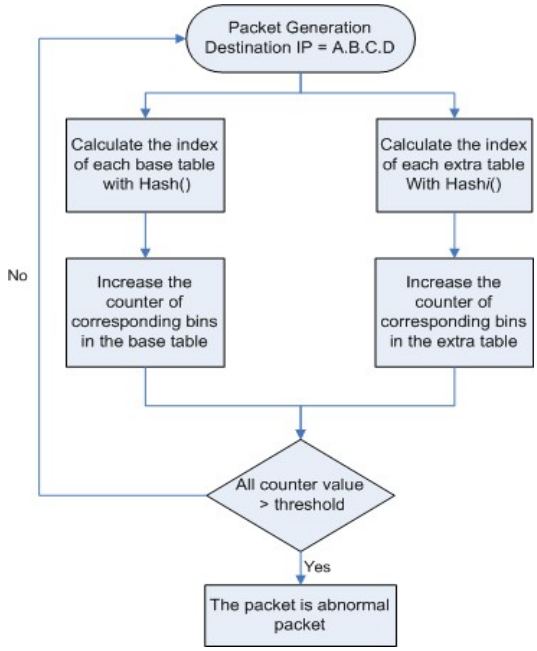

그림 4. 제안된 모니터링 기법의 공격탐지 알고리즘

기법 설계 시에도 적용될 수 있다.

3.2 다층 구조의 확장된 블룸 필터 기반 목적지 주소 모니터링 기법

탐지 결과의 정확도가 낮고 오탐지 비율이 높을 경우, 오탐지된 결과에 의해 정상적인 패킷이 차단되어 서비스의 질이 저하될 수 있다. 본 논문에서 제안한 확장된 블룸 필터 기반의 탐지 기법은 한정된 공간을 이용하기 때문에 공격 트래픽과 유사한 세부 주소를 갖는 정상적인 패킷이 중복 카운트되어 임계값을 초과할 수 있다. 이러한 문제점을 해결하기 위해 다층 구조 블룸 필터 기반 모니터링 기법을 제안한다. 다층 구조에서는 공격 패킷으로 의심되는 패킷과 정상적인 패킷을 분리하여 모니터링하는 구조를 이용한다. 제안한 탐지 구조의 동작 과정은 그림 5와 같다. 먼저 전체 임계값(T)을 부분 임계값(st_1, st_2, st_3, ..., st_n)으로 나누어 첫 번째 부분 임계값(st_1)을 초과한 패킷은 다른 패킷들과 분리하여 상위층(2 layer)에서 모니터링된다. 이때 각 층에 대한 해쉬 함수를 다르게 설정하여 중복 카운트되는 경우를 피하도록 하였다. 만일 패킷이 두 번째 부분 임계값(st_2)을 초과할 경우 다시 상위층(3 layer)에서 모니터링되며 최종적으로 전체 임계값(T)을 초과하는 패킷은 마지막 층(N layer)에서 모니터링되어 공격 여부를 결정하게 된다.

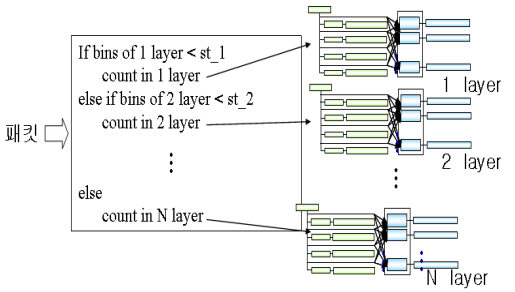

그림 5. 다층 구조의 확장된 블룸 필터 기반 모니터링 기법

부분 임계값 (Sub_threshold) : st_i
전체 임계값 (Total threshold) : T = st_1 + st_2 + …+ st_n

결과적으로 공격 패킷과 정상적인 패킷이 서로 다른 층에서 카운트되도록 함으로써 오탐지의 비율을 줄일 수 있다. 이러한 다층 구조는 메모리 공간이 증가되는 문제점이 있지만 한 층이 차지하는 메모리 공간은 약 10Kbyte이므로 전체 메모리 공간에 비해 상대적으로 낮은 비율을 차지한다.

Ⅳ. 성능 평가 및 분석

제안된 확장된 블룸 필터 기반 목적지 주소 모니터링 기법의 성능 평가를 위해 시나리오 1과 시나리오 2로 나누어 시뮬레이션을 진행하였다. 시나리오 1은 오탐지율 관점에서 기존 블룸 필터 기반 목적지 주소 모니터링 기법과 제안된 기법의 성능 비교를 위한 시뮬레이션이고, 시나리오 2는 제안한 기법에서 추가 테이블의 개수에 따른 성능 변화에 관한 시뮬레이션이다.

4.1 시나리오 1

기존의 블룸 필터 기반 모니터링 기법은 256개의 bin을 갖는 4개의 테이블을 이용하였으며, 제안된 기법은 128개의 bin을 갖는 4개의 기본 테이블과 256개의 bin을 갖는 2개의 추가 테이블을 이용하여 구성하였다. 시뮬레이션은 펜티엄 4 CPU를 탑재한 PC를 이용하였으며, 탐지 주기 T 시간 동안 다음과 같은 3종류의 패킷, 총 50,000개가 발생하도록 시나리오를 작성하였다.

1) 백그라운드 (Background) 패킷 : 0~255사이의 세부 주소를 랜덤하게 발생시켜 백그라운드 트래픽을 형성하도록 하였으며 총 38,000번 발생하도록 설정하였다.

2) 의심 (Suspicious) 패킷 : 공격 탐지의 정확성을 검증하기 위해 공격 트래픽으로 오탐지될 확률이 높은 의심 패킷을 발생시켰다. 따라서 정상 패킷이지만 과다 트래픽의 성질을 갖는 트래픽을 의심 패킷으로 정의하고 본 실험에서는 총 10,000개의 의심 패킷을 발생시켰다. 의심 패킷은 탐지 주기 T 시간 동안 미리 설정한 공격 IP 주소의 세부 주소 각각에 대해 총 500번 발생하도록 설정하였다.

3) 공격(Attack) 패킷 : 공격을 목적으로 발생된 패킷으로 탐지 주기 T 동안 하나의 목적지 IP 주소에 대해 1,000개가 발생되는 패킷을 공격 패킷으로 정의하였으며, 이에 따라 공격 탐지를 위한 임계값 (Threshold)을 1,000으로 설정하였다. DDoS 공격 환경을 설정하기 위해 2개의 서로 다른 공격 IP 주소를 이용하여 각 1,000개씩 총 2,000개의 공격 패킷을 발생시켰다.

표 1은 앞서 말한 시나리오에 따라 시뮬레이션을 수행한 결과 기존의 블룸 필터 기반 목적지 주소 모니터링 기법의 공격 탐지 결과 얻어진 공격 대상 목적지 IP 주소들이다.

표에서 확인할 수 있는 것과 같이 시나리오에서 발생시킨 두 개의 공격 대상 목적지 IP 주소 이외에도 정상 패킷임에도 불구하고 18개의 목적지 IP 주소가 추가로 공격 대상으로 탐지되어 결과의 90%가 오탐지임을 확인할 수 있다. 표 2는 본 논문에서 제안된 기법을 이용한 공격 탐지 결과 얻어진 공격

표 1. 기존 블룸 필터 기반 모니터링 기법의 공격 탐지 결과

탐지된 공격 대상 목적지 IP 주소	
150.200.100.110 (x)	129.200.100.170 (x)
60.210.230.150 (x)	129.200.230.150 (x)
150.200.230.170 (x)	150.200.100.120 (x)
60.210.230.170 (x)	129.1.100.150 (x)
60.210.190.150 (x)	150.1.100.170 (x)
60.210.190.140 (x)	60.210.190.110 (x)
150.200.100.140 (x)	150.200.100.160 (x)
60.210.190.130 (x)	60.210.230.160 (x)
150.200.100.130 (x)	60.210.190.120 (x)
129.1.230.170 (o)	150.200.100.150 (o)

표 2. 제안된 기법의 공격 탐지 결과

탐지된 공격 대상 목적지 IP 주소	
150.200.100.140 (x)	129.1.230.170 (o)
150.200.100.150 (o)	

대상 목적지 IP 주소들이다. 제안된 기법에서는 2개의 공격 대상 목적지 IP 주소가 정확히 탐지되었을 뿐만 아니라 0.3% 정도로 오탐지율이 극히 낮음을 알 수 있다.

4.2 시나리오 2

시나리오 2에서는 추가 테이블 개수의 변화에 따른 성능 평가를 수행하였다. 먼저 시나리오 1과 같이 128개의 bin을 갖는 4개의 기본 테이블을 이용하였고 256개의 bin을 갖는 추가 테이블 수를 변화시키면서 탐지 주기 T 시간 동안 3종류의 패킷이 총 1,000,000개가 발생되도록 하였다. 그리고 백그라운드 패킷과 의심 패킷의 비율을 각각 80%와 20%로 설정하여 시뮬레이션을 수행하였다. 공격 패킷은 하나의 목적지 IP 주소마다 5,000개가 발생되는 패킷을 공격 패킷으로 정의하였고 이에 따라 공격 탐지를 위한 임계값을 5,000으로 설정하였다. 또한 다중 DDoS 공격 환경을 설정하기 위해 5개의 공격 대상 목적지 IP 주소를 설정하여 임의의 시간에 5,000개가 초과되어 발생되도록 하였다.

다음 그림 6은 시나리오 2 환경에서 추가 테이블 수 변화에 따른 오탐지 수를 보인다. 그림에서 보는 바와 같이 추가 테이블 수가 증가할수록 세부 주소 간의 연관성을 다양하게 모니터링하므로 오탐지 수가 줄어들게 되나 6개 이상의 추가 테이블을 이용하는 경우 성능에 큰 변화가 없음을 확인할 수 있다.

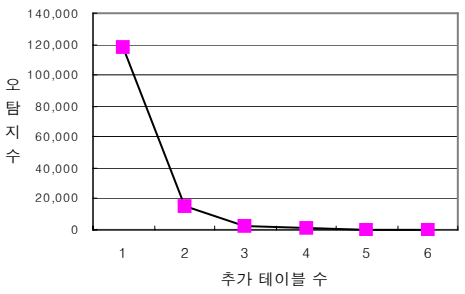

그림 6. 추가 테이블 수 변화에 따른 오탐지수 변화

4.3 다층 구조의 확장된 블룸 필터 기반 모니터일 기법의 성능 평가

확장된 블룸 필터 기반 모니터링 기법의 탐지 정확성을 향상시키기 위한 다층 구조 성능 평가를 위하여 시나리오 2 환경에서 시뮬레이션을 수행하였다. 실험은 층수와 추가 테이블 수를 변화시키면서 오탐지 결과를 분석하였다.

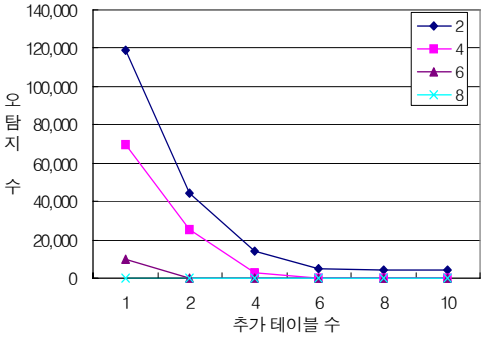

그림 7. 층수와 추가 테이블 수에 따른 오탐지 수

그림 7은 층수와 추가 테이블 수의 변화에 따른 오탐지 결과를 보인다. 결과를 분석해 보면 층수가 증가함에 따라 복잡도가 증가할 뿐만 아니라 기억 공간도 증가하는 문제점이 있으나 여러 단계로 모니터링을 수행하기 때문에 오탐지 수가 감소함을 보인다. 한편 동일한 층수를 사용하는 경우에도 추가 테이블 수를 증가시키면 세부 주소간 다양한 연관성을 모니터링하게 되므로 오탐지가 감소함을 알 수 있었다. 이러한 결과들을 종합해 볼 때 층수와 추가 테이블수의 적절한 결정에 따라 요구되는 오탐지 수준을 유지할 수 있다.

V. 결 론

본 논문에서는 확장된 블룸 필터 구조를 이용하여 패킷의 목적지 주소를 기반으로 DDoS 공격을 탐지하는 기법을 제안하였다. 기존 블룸 필터 기반 공격 탐지 기법은 각 패킷에 대한 목적지 세부 주소를 독립적으로 모니터링하기 때문에 오탐지율이 높은 단점을 가진다. 이러한 문제점을 해결하기 위하여 제안된 기법에서는 패킷의 목적지 IP 주소의 세부 주소 간 연관성을 갖는 테이블을 추가함으로써 보다 기존의 블룸 필터 기반 공격 탐지 기법보다 정확하게 공격 패킷을 탐지할 수 있었다. 또한 제안한 기법의 정확성을 향상시키기 위하여 추가 테이블의 변화에 따른 성능 평가를 수행하였다. 그 결과 추가 테이블의 수에 따른 성능 변화를 확인할 수 있었다. 이를 기반으로 요구되는 정확성 또는 확장성에 따라 적절한 추가 테이블의 개수를 결정할 수 있다. 또한 본 논문에서는 확장된 블룸 필터 기반 목적지 주소 모니터링 기법의 정확성을 향상시키기 위하여 다층 구조를 제안하였다. 층수와 추가

테이블 수를 변경시키면서 시뮬레이션을 수행한 결과 층수와 추가 테이블 수의 적절한 조합으로 공격 탐지 정확성을 향상시킬 수 있음을 알 수 있었다.

참 고 문 헌

〔1〕 S. Abdelsayed , D. Glimsholt , C. Leckie , S. Ryan, "An Efficient Filter for Denial-of-Service Bandwidth Attacks," *Proc. of* GLOBECOM '03, Vol. 3, pp. 1353-1357, Dec. 2003.

〔2〕 김영선, "*BcN의 기술적 이슈와 전망*," 한국정보통신기술협회, 2005년 8월 4일.

〔3〕 M. Thomer and P. Massimiliano , "MULTOPS: A Data-structure for Bandwidth Attack Detection," *Proc. of the 10th USENIX Security Symposium*, vol. 10, pp. 23-38, August 2001.

〔4〕 Y. K. Chan, H. W. Chan et al., "IDR: An Intrusion Detection Router for Defending against Distributed Denial-of-Service (DDoS) Attacks," *Proc. of the 7th International Symposium on Parallel Architectures, Algorithms and Networks,* pp. 581-586, May 2004.

〔5〕 F. L. Schnaxkenberg. D. Balupari. R. Kindred, "Statistical Approaches to DDoS Attack Detection and Response," *Proc. of DARPA Information Survivability Conference and Exposition*, vol. 1, pp. 303-314, April 2003.

〔6〕 G. Zhang and M. Parashar, "Cooperative Defense against Network Attacks," *Proc. of WOSIS' 05, ICEIS 2005, INSTICC Press,* pp. 113-122, May 2005.

유 경 민 (Kyoung-Min Yoo) 정회원

1992년 8월 전북대학교 컴퓨터공학과 졸업
1997년 2월 전북대학교 컴퓨터공학과 석사 졸업
2005년 3월~현재 전북대학교 컴퓨터공학과 박사과정

<관심분야> BcN, 네트워크 보안, 인공면역체계 기반 망 제어

심 상 헌 (Sang-Heon Sim) 정회원

2004년 2월 전북대학교 컴퓨터공학과 졸업
2007년 8월 전북대학교 컴퓨터공학과 석사 졸업
현재 전북대학교 영상정보신기술연구센터 연구원

<관심분야> BcN, 네트워크 보안

한 경 은 (Kyeong-Eun Han) 정회원

한국통신학회 논문지 제31권 제7B호 참조
현재 전북대학교 영상정보신기술연구센터 연구원

소 원 호 (Won-Ho So) 정회원

한국통신학회 논문지 제29권 제9B호 참조
현재 순천대학교 컴퓨터교육과 조교수

김 영 선 (Young-Sun Kim) 종신회원

한국통신학회 논문지 제31권 제8B호 참조
현재 한국전자통신연구원 광대역통합망연구단 네트워크연구그룹장

김 영 천 (Young-Chon Kim) 종신회원

한국통신학회 논문지 제19권 제2호 참조
현재 전북대학교 전자정보공학부 교수