통계 기반 분산서비스거부(DDoS) 공격 탐지 모델에 관한 연구

국윤주* · 김용호* · 김점구** · 김귀남*

요 약

분산서비스거부 공격을 탐지하기 위한 많은 개발과 연구가 진행되고 있다. 그 중에서 통계적 기법을 이용한 방법은 정상적인 패킷과 비정상적인 패킷을 판별해 내는데 효율적이다. 본 논문에서는 여러 가지의 통계적 기법을 혼합하여 다양한 공격을 탐지할 수 있는 방법을 제안한다. 효과를 검증하기 위하여 라우터에 DDoS 공격 패킷 필터링을 설정한 경우와 제안 기법을 적용한 리눅스 라우터를 구현하여 실험한 결과, 제안 기법이 다양한 공격을 탐지하는 것 뿐만이 아니라 정상적인 서비스까지도 대부분 유지시키는 것을 확인하였다.

A Study on DDoS(Distributed Denial of Service) Attack Detection Model Based on Statistical

Yoon Ju Kook* · Yong Ho Kim* · Jeom Goo Kim** · Kiu Nam Kim*

ABSTRACT

Distributed denial of service attack detection for more development and research is underway. The method of using statistical techniques, the normal packets and abnormal packets to identify efficient. In this paper several statistical techniques, using a mix of various offers a way to detect the attack. To verify the effectiveness of the proposed technique, it set packet filtering on router and the proposed DDoS attacks detection method on a Linux router. In result, the proposed technique was detect various attacks and provide normal service mostly.

Key words : DDoS, Statistical, Router Packet Filtering

접수일 : 2009년 5월 18일; 채택일 : 2009년 6월 19일

* 경기대학교 정보보호학과
** 남서울대학교 컴퓨터학과

1. 서 론

분산서비스거부(이하 DDoS) 공격은 인터넷 상에서 발생하는 공격 유형 중에서 가장 심각하고 그 발생 횟수도 잦다. 최근 공격의 주요 목적은 웹 사이트나 서버에 네트워크 장애를 발생시켜 해당 업체에 정치적 또는 금전적인 요구를 하며 주로 실시간 서비스를 제공하는 업체들을 주요 목표로 삼는다[3].

DDoS 공격을 탐지하기 위한 연구로는 [7]에서 사용한 SNMP-MIB를 이용한 탐지 방법, [2]에서의 데이터 마이닝 기법을 이용한 방법, [9]의 통계적 기반의 방법 등이 있다. 그러나 이러한 방법들은 특정 프로토콜이나 특정 공격을 탐지하므로 비정상적인 트래픽을 분류해 처리하는 부분에 대해 처리가 미흡하거나 실제 공격이 발생할 경우에는 실시간으로 유입되는 패킷들에 대한 처리 능력이 다소 떨어지는 문제점이 있다.

본 논문에서는 이러한 단점들을 보완하고자 확장된 통계적 기반의 탐지 방법을 이용하여 다양한 공격을 탐지 할 수 있는 방법을 제안한다. 이는 내부 네트워크망과 인접한 에지 라우터에 적용하여 내부망을 보호하며 라우터로 인입(Incoming)되는 모든 패킷들을 대상으로 한다. 통계적 기법을 이용한 이유는 DDoS의 공격 형태가 매우 다양하여 정상적인 패킷과 구별하기가 어렵고, 관리자가 쉽게 탐지할 수 없는 상황에서 비정상 패킷들을 탐지할 수 있기 때문이다. 통계적인 방법은 가장 효율적이며 [5] 여러 기관에서 DDoS 공격을 탐지하기 위한 방법으로 가장 많이 사용된다[1, 9].

제안하는 통계 기반의 탐지 기법에서는 평상시와 공격시의 트래픽을 수집 및 분석한 결과로 산출된 임계값을 탐지의 판단 기준으로 활용하였다. 이에 대한 성능 평가는 SYN Flooding, UDP Flooding, ICMP Flooding 및 HTTP connection 공격을 이용한 실험으로 오탐지율의 신뢰도를 확인하였다.

2. DDoS 공격 탐지 기법

2.1 SNMP-MIB를 이용한 탐지

SNMP에서의 MIB 정보를 이용한 침입탐지 방법론[6-8]은 트래픽 폭주 공격 탐지에서 MIB 데이터 수집을 위한 시스템 및 네트워크 리소스의 사용이 적고, 계층과 프로토콜을 기준으로 표준화된 네트워크 성능데이터를 제공받을 수 있기 때문에 패킷기반 탐지방법에 비해 보다 빠르고 효과적인 탐지와 분류가 가능하다[7].

2.2 데이터 마이닝을 이용한 탐지

[2]에서는 Netflow 트래픽과 의사결정트리, 신경망 모형의 데이터마이닝 기법을 이용한 DDoS 공격 탐지 방법을 제안하였는데, 특히 DDoS 공격 탐지 성능을 개선시키기 위해서 혼합된 데이터마이닝 기법을 사용하였다. 제안 기법은 정확한 탐지가 장점이지만 관리자의 많은 수작업과 현재 네트워크의 특성이 반영되지 않으며, 새로운 유형의 공격이 발생하였을 때에는 탐지가 불가능하다. 이러한 이유로 실제 정상 트래픽 탐지에서는 비효율적이며 실시간 탐지가 불가능하다는 단점을 보이고 있다.

2.3 통계적 방법을 이용한 탐지

통계적 방법은 침입 탐지 시스템을 설계하거나 DDoS 공격을 탐지하는데 있어 자주 활용되는 알고리즘 중의 하나이며, 종류도 무척 다양하여 엔트로피 통계, 카이 제곱(Chi-square) 통계, 트래픽 볼륨 통계, 평균과 표준편차를 이용한 방법들이 사용되고 있다. 이중 엔트로피 연산법은 어떠한 네트워크 속성 값에 대한 임의성을 계산한 뒤, 그 값의 평균의 변화량을 탐지하는 방법이고, 카이 제곱 검증법은 속성 값에 대한 분산도를 측정하는 방법으

로 그 값에 따라 비정상적인 속성 값을 탐지할 수 있다.

이 기법들에서는 특정 공격만을 고려하여 공격을 탐지하거나 실시간 탐지의 어려움 및 새로운 공격 유형에 대해서는 유연성이 부족하여 실제 공격 상황에 적용하기에는 한계점을 갖는다. 따라서 본 논문에서는 실제 네트워크 상황을 반영하고, 실시간으로 탐지가 가능하며, 다양한 공격 유형에 대해서도 탐지가 가능한 기법을 제안한다.

<표 1>은 각 탐지기법들을 비교한 것이다.

〈표 1〉 각 탐지기법들의 비교

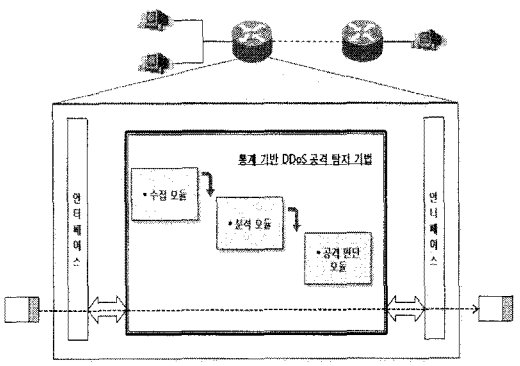
탐지 기법	장 점	단 점
SNMP-MIB	◦ 비교적 정확한 탐지	◦ 객체 정보간의 연산 및 관리 문제로 실시간 탐지의 어려움 ◦ 새로운 공격에 대한 탐지 부족
데이터 마이닝	◦ 오탐율이 낮음 ◦ 비교적 정확한 탐지	◦ 대용량의 학습 데이터가 필요 ◦ 새로운 공격에 대한 탐지 부족 ◦ 실시간 탐지의 어려움
통계적 기법	◦ 정상과 비정상 트래픽 구별용이	◦ 특정 요소에 대한 탐지가 대부분 (예 : 발신지 주소, 포트 번호) ◦ 적절한 임계값 설정의 어려움

3. 통계 기반의 DDoS 공격 탐지 기법

제안하는 기법은 내부 네트워크와 외부 네트워크에서 라우터로 들어오는 패킷을 수집하고 분류하는 수집 모듈, 탐지에 사용될 각종 요소를 추출 및 연산하여 임계값을 산출하는 분석 모듈 그리고 임계값을 이용하여 공격 여부를 판단하여 처리하는 공격 판단 모듈로 구성되어 있다.

(그림 1)은 본 논문에서 제안하는 DDoS 공격탐지기법의 전체 구성도이다.

탐지 방법은 트래픽을 수집 및 분류하여 발신지



(그림 1) DDoS 공격탐지기법 전체 구조도

와 목적지 주소 비교 및 트래픽 비율 분석, 각 요소별 평균과 표준편차를 이용하여 비정상 패킷을 판별하였고, 적절한 임계값을 산출하기 위해서 일정 주기별로 평상시의 정상 패킷에 대한 학습 시간을 두었으며, 수시로 변하는 네트워크의 상황을 반영하고자 일정 주기로 트래픽을 수집하기 위한 수집 모듈을 백그라운드로 실행되게끔 설계 하였다. 이는 실시간으로 패킷을 수집하여 분석한 후 탐지까지 하는 것은 시스템에 과부하를 초래하기 때문이다.

3.1 수집 모듈

이 모듈에서는 <표 2>에 미리 정의한 기준에 근거하여 공격과 관련된 프로토콜만을 수집한다. 제안 기법을 처음 적용할 때는 정상 트래픽을 수집하는 24시간 동안은 탐지가 이루어지지 않는다. 왜냐하면 최초 24시간 동안 수집된 트래픽을 대상으로 분석하여 최초의 임계값을 산출해 내야 하기 때문이다. 그러나 24시간이 지난 이후부터는 실시간으로 탐지 알고리즘이 적용되며, 이때부터 수집되는 패킷은 탐지 알고리즘을 거쳐 정상으로 판단된 패킷만을 수집대상으로 한다. 패킷 수집 도구는 tcpdump를 이용하였고, 수집되는 패킷의 목록은 <표 2>와 같다.

〈표 2〉 수집 패킷 목록

목 록
srcIP, dstIP, (srcIP, dstIP), srcPort, dstPort, UDP dstPort, ICMP_Type, TCP flag별, TCP, UDP, ICMP, HTTP

3.2 분석 모듈

이 모듈에서는 분류된 항목을 기반으로 통계적 분석을 통하여 각 요소별로 임계값을 산출한다. DDoS 공격 판별시 다양한 공격유형을 탐지하고 비정상 패킷 판별율을 높이기 위해 발신지와 목적지 주소 비교 분석, 프로토콜별 트래픽량 분석, 평균과 표준편차를 이용한 혼합된 형태의 탐지 방법을 이용하였다.

3.2.1 발신지 주소와 목적지 주소의 비교

일정 시간 동안 발신지 주소와 목적지 주소가 동일한 패킷들이 급격하게 임계치 이상으로 발생하면 이후부터는 해당 패킷에 대해서 폐기시키는 정책이 필요하다. 그러므로 발신지 주소와 목적지 주소의 비교에서는 <표 2>의 분류 항목 중 (srcIP, dstIP), 즉 srcIP와 dstIP 내용이 똑같은 패킷에 대한 통계 수치를 산출한다.

〈표 3〉 (srcIP, dstIP)가 동일한 패킷 통계수식

번호	수식
1	$SD_{normal} = \frac{1}{N}\sum_{i=1}^{N} PKT_{count}(T_{k=1,\cdots,n})$ 평상시의 일정 시간 T에서 발신지 주소와 목적지 주소가 동일한 패킷들만의 개수를 계산하여 N번 반복 후 평균 계산
2	$SD_{attack} = \frac{1}{N}\sum_{i=1}^{N} PKT_{count}(T_{k=1,\cdots,n})$ 공격 시의 일정 시간 T에서 발신지 주소와 목적지 주소가 동일한 패킷들만의 개수를 계산하여 N번 반복 후 평균 계산

<표 3>은 통계를 산출하기 위한 수식과 설명을 정리한 것이다. 수식 1에서 패킷은 1시간 간격으로 24회를 반복하였고, 수식 2의 값은 별도의 공격 실험 즉, 0.2초 단위로 20회 사용하여 나온 결과이다.

3.2.2 트래픽 비율 분석

[4]에서 제안한 트래픽 비율 분석법(Traffic Rate Analysis)은 TCP의 모든 플래그를 포함해서 TCP, UDP, ICMP 프로토콜의 비율도 함께 고려하므로 SYN Flooding 공격뿐만 아니라 다양한 DDoS 공격에 대한 탐지에도 이용할 수 있다.

TCP 플래그 비율 $R_t[F]$는 t시간 동안 특정한 TCP 플래그를 가진 패킷 개수를 전체 TCP 패킷 총수로 나누어 구한 비율이다. $R_t[TCP]$는 전체 IP 패킷에서 TCP 패킷의 발생비율을 t시간 마다 측정한 결과값을 의미한다.

〈표 4〉 평상시와 공격시의 트래픽 비율변화

유 형		평상시	공격시(Flooding)			
			SYN	UDP	ICMP	HTTP
TCP	S	956 (5%)	85020 (100%)	16132 (100%)	0	0
	F	584 (3%)	0	0	0	0
	A	14800 (80%)	0	0	0	0
	P&A	2096 (12%)	0	0	0	0
	U	0	0	0	0	0
	All 0	0	0	0	0	60949 (100%)
	All 1	0	0	0	0	0
TCP		13504 (70%)	85020 (100%)	16131 (25%)	0	0
UDP		3108 (16%)	0	48481 (75%)	0	0
ICMP		24(1%)	0	0	88015 (100%)	0
HTTP		2276 (12%)	0	1 (0%)	0	60949 (100%)

<표 4>의 내용을 보면 공격전과 공격후의 트래픽 비율의 차이가 현저하게 나타남을 확인 할 수 있다. 그러므로 특정 트래픽이 평상시 트래픽 비율보다 일정 시간 이상 지속되면 공격 징후라고 판단할 수 있다.

3.2.3 각 요소별 평균과 표준 편차 산출

비정상적인 행위 패킷들을 탐지하는데 이용할 수 있는 방법으로 <표 1>에서 정의한 목록을 기준으로 각 요소별 평균과 표준편차를 산출하였다. 수집된 패킷은 산술 평균과 표준 편차를 구하기 위한 적당한 표본으로 만들기 위해서 총 패킷 수를 100으로 나누었다. 이 표본(sample)을 S라고 했을 때 매 S개마다 프로토콜별, 플래그별, 포트 별 산술 평균 및 표준 편차를 구한다.

그리고 산술평균과 표준 편차의 평균을 이용하여 각 요소에 대해 임계값 *TH(f)*를 구한다.

이렇게 통계적 기법을 이용하여 산출된 평균, 표준편차, 임계값은 백그라운드 작업 실행으로 매 24시간 간격의 새로운 트래픽에 대하여 산출되므로 매번 네트워크의 상황에 따라 그 값들이 달라진다.

3.3 판단 모듈

이 절에서는 임계값을 이용하여 실시간으로 패킷들에 대한 공격 여부를 판단하고 처리한다.

ICMP Flooding 공격을 탐지하는 알고리즘은 발신지 IP 주소와 목적지 IP 주소를 동일하게 가지고 있는 패킷들이 임계값 내에 있거나, ICMP 트래픽 비율이 임계값 이상이면 일단 공격 징후로 간주한다. 그러므로 이 때 일정시간동안 ICMP의 type 필드값이 0인 패킷 개수에 대한 표준 편차가 임계값보다 크면 ICMP Flooding 공격으로 판단한다. 그 외의 조건에 대해서는 정상 패킷으로 판단한다.

TCP 프로토콜 관련한 공격은 가장 많이 발생하는 공격이므로 알고리즘이 가장 복잡하다. 먼저 발신지 IP 주소와 목적지 IP 주소를 동일하게 가지고 있는 패킷들이 임계값 내에 있거나, TCP 트래픽 비율이 임계값 이상이면 일단 공격 징후로 간주한다. 그러므로 일정시간동안 SYN 트래픽의 비율이 임계값 보다 크면서 TCP_syn 패킷 개수에 대한 표준 편차가 임계값보다 크면 SYN Flooding 공격으로 판단한다. ACK, FIN, URG PSH+ACK, All 0, All 1 플래그 등을 이용한 공격 탐지 방법도 이와 같다.

UDP Flooding 공격을 탐지하는 알고리즘에서 UDP 프로토콜은 P2P나 멀티미디어 데이터 송수신 시 사용되는 프로토콜이므로 네트워크 트래픽의 상황을 고려하여야 한다. 그러므로 발신지 IP 주소와 목적지 IP 주소를 동일하게 가지고 있는 패킷들이 임계값 내에 있고, UDP 트래픽 비율이 임계값 이상이면 일단 공격 징후로 간주한다. 그러므로 일정시간동안 UDP 프로토콜의 목적지 포트 번호에 대한 표준 편차가 임계값보다 크면 UDP Flooding 공격으로 판단하고 그 이외의 패킷에 대해서는 정상 패킷으로 판단한다.

이상과 같이 각 탐지 알고리즘을 적용했을 때 공격으로 판단이 내려지면 시간, 해당 프로토콜, 공격의 종류 등이 로그로 기록된 후 패킷을 폐기한다. 정상 패킷인 경우에는 라우터의 경로 테이블 정보에 따라 해당 인터페이스로 넘겨주게 된다.

4. 성능 평가

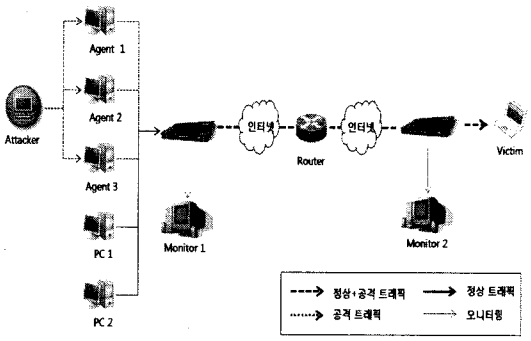
제안한 DDoS 공격 탐지 기법의 검증을 위해 SYN Flooding, UDP Flooding 및 ICMP Flooding, HTTP connection 공격과 기타 네트워크 장비들을 이용하여 공격 탐지 효과를 확인하였다.

4.1 실험 환경

일반적으로 많이 이용되는 라우터에 DDoS 공

격 필터링을 적용한 [실험 1]과 제안 탐지 기법이 적용된 [실험 2]의 2가지로 나누어진다. 두 가지 실험에서 하드웨어는 일반적인 PC의 사양이고, 모니터링을 위한 프로그램은 WireShark 1.0.0이고, 공격 툴은 hping2[10]이다. 이들은 모두 사용법이 쉽고 누구나 무료로 사용할 수 있는 프로그램들로 설정하였다. 그리고 사용된 네트워크 장비는 Cisco 2821, Catalyst 3550이다.

(그림 2)는 [실험 1]의 구성도이며, 라우터는 DDoS 공격에 대응하기 위한 필터링이 적용된 상태이다.

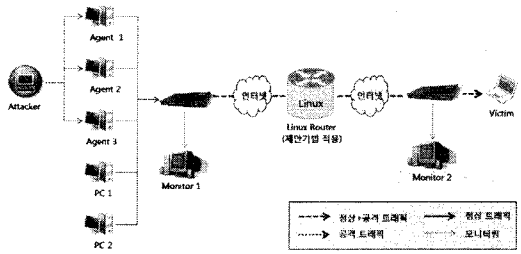


(그림 2) [실험 1]의 환경 구성도

공격자가 Agent1~3을 이용하여 공격을 진행하고, 나머지 PC1~2는 정상적인 패킷들을 송수신한다. Monitor 1에서는 공격 패킷과 정상 패킷들을 모두 수집하며, 라우터는 모든 패킷들을 받아들여 설정된 필터링을 기반으로 차단하거나 Victim으로 흘러 들어가게 라우팅한다. Monitor 2는 필터링이 설정된 라우터가 공격 패킷들을 어느 정도 걸러낼 수 있는지 확인하기 위하여 패킷들을 수집한다.

(그림 3)은 [실험 2]의 구성도이며, Linux Router는 제안 탐지 기법을 구현한 리눅스에 랜카드 2장을 장착하여 라우터 기능을 추가한 리눅스 라우터이다.

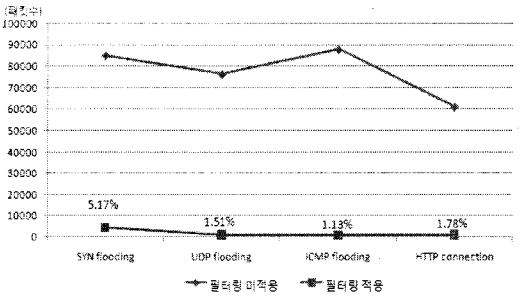
이는 제안 탐지 기법과 DDoS 공격 대응 필터링이 적용된 라우터와의 성능 비교를 위해서다. 그 외에 트래픽의 흐름 방향과 모니터링 방법은 [실험1]과 같다.



(그림 3) [실험 2]의 환경 구성도

4.2 실험 및 분석

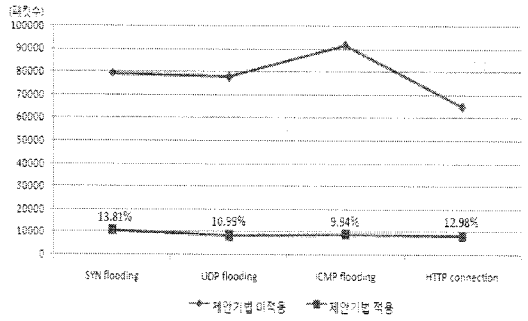
(그림 4)는 [실험 1]의 환경에서 5초 동안 공격을 진행하여 DDoS 공격 필터링이 설정되지 않은 경우와 설정된 경우의 패킷 개수를 측정하여 통과비율을 산출하였다.



(그림 4) 라우터의 필터링 적용여부에 따른 패킷통과비율

(그림 4)에서 차단 효과가 좋은 이유는 필터링 설정에서 패킷 개수나 대역폭이 임계치를 넘는 경우 모두 차단하기 때문이다. 그러나 이것은 정상적인 연결까지도 대부분 차단됨을 실제 확인했으며 오탐율이 다수 발생하였다. 오탐율 확인은 정상 패킷과의 구별을 위해 특정 문자열을 공격 패킷 전송에 사용함으로써 정확한 측정이 가능하다[10].

(그림 5)는 제안 기법을 적용한 경우의 공격 유형별 패킷통과율을 측정한 결과이다.



(그림 5) 제안기법 적용여부에 따른 패킷통과율

[실험 1]보다 패킷통과율이 높은 이유는 정상적인 패킷을 포함하고 있기 때문이다. 즉, DDoS 공격 필터링을 설정한 라우터보다 패킷 차단율이 낮았으나, 이는 정상적인 패킷을 포함하고 있어 낮아 보이는 것이며, 실제 공격 패킷을 차단하는 비율은 제안 기법이 적용된 라우터에서의 비율이 더 높았고, 정상 패킷이 통과하는 비율 또한 높았다. 그러나 제안 기법에서 정상 패킷이 100% 통과되지 못한 이유는 공격 패킷의 순간적인 대역폭 100%의 점유율과 시스템의 과부하로 인하여 시스템이 다운되지는 않지만 순간적으로 비정상을 보이기 때문이라고 생각된다. <표 5>는 [실험 1]과 [실험 2]에서의 정상 패킷 통과율과 공격 패킷 통과율을 보여주고 있다.

〈표 5〉 [실험 1],[실험 2]의 정상·공격패킷통과율

실험 / 공격 유형	[실험 1](%)		[실험 2](%)	
	정상패킷 통과율	공격패킷 통과율	정상패킷 통과율	공격패킷 통과율
SYN flooding	16.40	12.77	92.37	1.00
UDP flooding	24.42	11.16	94.49	1.20
ICMP flooding	14.71	10.37	96.43	1.03
HTTP connection	34.51	13.78	95.35	1.11

5. 결론 및 향후과제

본 논문에서는 지금까지 제안되었던 여러 가지 DDoS 공격 탐지 기법들 중에서 통계적 기반의 탐지 기법을 확장하여 DDoS 공격의 피해를 줄이고자 하였다. 이는 내부 네트워크를 보호하기 위해 망 경계의 라우터에 위치하여 라우터로 인입되는 모든 패킷들을 검사한다.

제안 기법을 검증하기 위해서 DDoS 공격 필터링이 적용된 라우터와 제안 기법이 적용된 리눅스 라우터를 구현하여 비교하였다. 실험 결과, 일반 라우터의 DDoS 공격 필터링 설정은 수동적이어서 대응하는데 한계가 있지만, 제안 기법이 적용된 라우터는 실험 환경에서 공격이 진행 중에도 정상적인 서비스를 90% 이상 가능하게 하였고, 공격 패킷에 대해서도 98% 정도를 탐지하는 효율성을 보였다. 그러나 stealthy 공격에 대한 탐지 방안을 제시하지 못하였고, 공격 진행 중의 정상적인 서비스를 100% 보호하지 못한 점, 스푸핑(위조) IP 탐지 방안 등이 고려되지 않아 논문의 신뢰성을 확보하기 위해 향후 연구되어야 할 것이다.

참 고 문 헌

[1] 김선영, 패턴 매칭과 통계적 기법을 이용한 공격 탐지 알고리즘, 충북대학교, 2006.

[2] 박정민, 나현정, 황경애, 채기준, "광역망에서의 DDoS 탐지 메커니즘에 관한 연구", 이화여자대학교, 2003.

[3] 성재모, "DDOS 공격 기술 동향", 금융보안연구원, 2009.

[4] 이철호 외 3인, "웹 서버에 대한 DDoS 공격의 네트워크 트래픽 분석", 정보처리학회논문지 제10-C권, 제3호, 2003.

[5] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-Service Attack-Detection Techni-

ques", IEEE, Vol. 10, No. 1, 2006.
[6] J. B. D. Cabrera, L. Lewis, X. Qin, and C. Gutierrez, W. Lee, and R. K. Mehra, "Proactive intrusion detection and SNMP-based security management : new experiments and validation", IFIP/IEEE 8th ISINM, pp. 93-96, 2003.
[7] J. Li and C. Manikopoulos, "Early statistical anomaly intrusion detection of DOS attacks using MIB traffic parameters", IEEE, pp. 53-59, 2003.
[8] L. P. Gaspary, R. N. Sanchez, D. W. Antunes, and E. Meneghetti, "A SNMP-based platform for distributed stateful intrusion detection in enterprise networks", IEEE Journal on Selected Areas in Communications, Vol. 23, No. 10, pp. 1973-1982, 2005.
[9] Laura Feinstein, Dan Schnackenberg, Ravindra Balupari, Darrell Kindred, "Statistical Approaches to DDoS Attack Detection and Response", Proceedings of the DISCEX 2003, 2003.
[10] http://www.radarhack.com, HPING2.

국 윤 주

1999년 광운대학교 정보통신 대학원(이학석사)
2009년 경기대학교 정보보호학과 박사수료

김 용 호

광운대학교 정보통신학과 (공학석사)
경기대학교 정보보호학과 (이학박사)
경찰청 사이버테러대응센터 연구원
현재 경기대산업기술보호특화센터 K-포렌식 연구소장

김 점 구

광운대학교 전자계산학과 (이학사)
광운대학교 전자계산학과 (이학석사)
한남대학교 컴퓨터공학과 (공학박사)
(주)제성프로젝트 연구원
(주)시사컴퓨토피아 인터넷사업본부장
현재 남서울대학교 컴퓨터학과 교수

김 귀 남

미국 캔자스대학교(공학사)
미국 콜로라도주립대학 (공학석사)
미국 콜로라도주립대학 (공학박사)
현재 경기대학교 산업기술보호특화센터 센터장
현재 경기대학교 정보보호학과 교수