중소기업융합학회 논문지 제4권 제3호 pp. 1-6, 2014 ISSN 2234-4438

트래픽 분석을 통한 DDoS 공격에 대한 대응책 연구

홍성혁[1*]
[1]백석대학교 정보통신학부

DDoS attack traffic through the analysis of responses to research

Sunghyuck Hong[1*]
[1]Division of Information and Communication, Baekseok University

요 약 DDoS (Distributed Denial Service, 분산 서비스) 공격이 인터넷에서 대하여 끊임없는 위협이 발생되고 있으며, 이에 대한 대응책들이 제시 되었다. 그러나 다양한 공격과 복잡한 공격으로 어떠한 대응법이 효과적인지도 상당히 문제점이 되었다. 공격자들은 이러한 대응에 대해 하기 위하여 꾸준한 공격도구를 변경하고 있으며, 이에 대한 대응책으로써 전문가들 역시 새로운 공격에 대해 끊임없이 연구를 하고 있다. 따라서 본 논문은 DDoS의 최근의 대표적인사례인 7.7DDoS와 3.3DDoS에 대해 살펴보고 기존 DDoS 공격유형인 PPS 증가 공격, 대용량 트래픽 전송, 웹 서비스 지연과 라우터와 방화벽 설정으로 대응방안을 소개하고, 응용프로그램과 인증제도에 의한 DDoS 대응책 연구를 기술하여, 앞으로의 DDoS 공격에 효과적으로 방안할 수 있도는 방법을 제시하였다.

키워드 : DDoS 공격, 분산처리공격, 네트워킹 공격

Abstract DDoS (Distributed Denial Service, Distributed Service) attacks are being generated for a constant threat on the Internet, countermeasures for this have been proposed. However, the problem has become an increasingly effective instruction in any Measures are a variety of attacks and sophisticated attacks. Attackers can change a steady attack tools to respond to these, the experts as a countermeasure to this constantly research for a fresh attack. This paper is to introduce countermeasures to DDoS recent representative examples of 7.7DDoS and look for 3.3DDoS existing types of DDoS attacks increased PPS attacks, high traffic sent, web service delay and router and firewall settings, applications and to describe the DDoS countermeasures research by certification, is so that you can plan effectively for the future DDoS attacks proposed method.

Key Words : DDoS attack, Distributed Attack, Networking attack

1. 서론

DoS(Denial of Service, 서비스 거부) 공격은 한 공격자가 악의적인 목적으로 시스템의 리소스를 독점 및 모두사용, 또는 파괴하여 다른 사용자들이 원활한 서비스를 이용하지 못하게 하는 것이다. 이러한 한 공격자의 주소를 확인하고 차단하여 더 이상 공격을 하지 못하게 하는 단점을 보안하기 나온 것이 DDoS(Ditributed Denial Service, 분산 서비스)공격 기법이다.

DDoS 공격은 공격자가 원격에서 PC를 조종할 수 있는 악성코드를 만들어 일반PC를 감염 시킨 후, 명령을 내리는 방식으로 Automaiton Program을 통해 한 번에 여러 PC에게 대상 시스템에 공격 명령을 하여 원활한 서비스를 이용하지 못하게 하는 것이다[1, 2].

Received 2014-08-01 Revised 2014-08-20 Accepted 2014-08-30
*교신저자 : Sunghyuck Hong (shong@bu.ac.kr)

2009년 7월 7일 오후 7시경부터 7월 9일 까지 약 3 일간 청와대를 포함하여 국내 주요 사이트 23곳을 대상으로 한 DDoS 공격이 일어났다. 공격 목적은 분명하지 않지만 공격이 끝나면 좀비PC의 하드디스크를 파괴 후 공격 종료로 감염된 좀비PC수는 115,044대 이다. 7.7 DDoS의 공격 기법은 HTTP Get Foolding, CC(Cashe-Control) 공격형태의 Web Server 의 자원을 고갈시키기 위한 공격 중심으로 UDP Flooding, ICMP, Ping Flooding 네트워크 대역폭 고갈 공격이 함께 이루워 졌다. 공격 특징은 보안에 취약한 웹 서버 공격 및 Spam Mail을 통해 전파하였고 C&C(Comand & Control)서버 없이 자체 공격 리스트와 Timer에 의해 정해진 시간에 공격 후 자가 파괴 기능을 하였다.[Fig. 1] 그림은 취약한 웹사이트에 악성코드를 은닉 하거나, Spam-Relay기법을 통해 악성코드를 배포하여 피해자 PC에 악성코드를 감염 후, 공격 URL List와 Timer에 의해 공격 하였다[1].

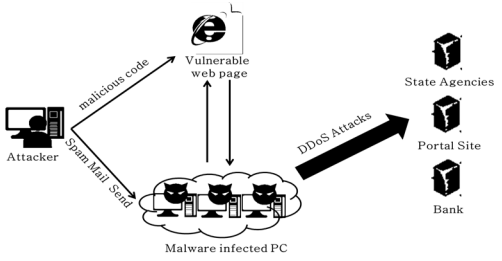

Fig. 1. 7.7 DDos Attack Scenario

2011년 3월 3일부터 4일 청와대를 비롯하여 국내 주요 사이트 40곳을 대상으로 DDoS 공격이 일어났다. 모든 윈도 운영체제가 손상 및 MBR(Master Boot Record)이 파괴되었고 공격용 악성코드는 호스트파일 변조를 통해 백신업데이트를 방해하거나 홈페이지 접근을 방해로 감연된 좀비 PC 수는 77,207대 이다. 3.3 DDoS 공격기번은 HTTP Get Flooding, CC(Cashe-Control) 공격형태의 Web Server의 자원을 고갈시키기 위한 공격중심으로 UDP Flooding, ICMP Ping Flooding 네트워크 대역폭 고갈 공격이 함께 이루워졌다. 공격 특징은 쉐어박스. 파일시티, 보보파일 등 P2P 사이트 등을 통하여 악성코드를 배포하였고 C&C(Command & control) 서버가 명령을 내리는 형식으로 진행 되었다.[Flg. 2] 그림은 국내 주요 P2P 사이트를 통해 악성코드를 웹 하드 설치 모듈 등을 이용하여 배포하고 악성코드 실행시 생성되는 Data파일 내에 기록된 URL로 DDos 공격을 수행하였다[2].

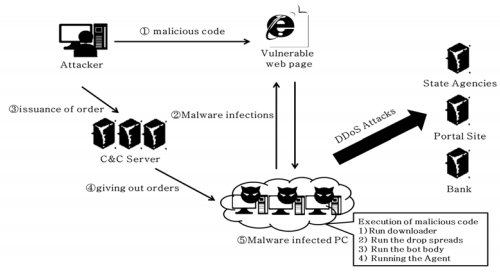

Fig. 2. 3.3 DDos Attack Scenario

7.7 DDoS와 3.3DDos 공격의 유사점은 Table 1와 같다.

Table 1. 7.7 DDos and 3.3 DDoS similarities

That distribute malware	P2P Site
The PC used in the attack	Primarily an individual user's PC
Forms of attack	Pre-planned attack
Target	Typical portal, public agencies, financial institutions, etc.
Purpose Attack	Obscurity
Exit attacks	To destroy the hard disk shut down attacks

본 논문에서는 라우터 및 스위치 설정, 보안장비 IPS 방화벽 설정으로 DDoS 공격을 효율적으로 대응전략 할 수 있는 시스템을 제안한다.

본 논문의은 다음과 같이 구성하였다. 2장은 DDoS 공격에 사용한 PPS증가 공격(PPS Consuming), 대용량 트래픽 전송(Bandwidth Consuming), 웹 서비스 지연(Http Flooding)의 기존의 공격유형과 대응 방법에 대해서 기술한다. 3장은 DDoS공격에 대한 대응전략에 관한 제안을 한다. 4장은 대응전략 연구를 제안한다. 5장은 결론으로 정리한다.

2. DDoS 공격유형

2.1 PPS 증가 공격(PPS Consuming)

본 연구는 TCP프로토콜을 통한 네트워크와 보안 장비에 부하를 발생되게 하여 동일 네트워크의 시스템을 마비시킨다. 공격 유형으로는 IP Spoofed SYN Flooding 공격기법, TCP Connection Flooding 공격기법. TCP Out-Of-State Packet Flooding 공격기법의 원리 및 대응 기초에 대하여 알아본다.

2.1.1 IP Spoofed SYN Flooding 공격

TCP의 3-way handshaking의 연결형 서비스의 대한 취약점을 이용한 공격형태로써 공격자는 IP를 지속적으로 변조하여 TCP 플래그 중, 접속을 요청하는 SYN 플래그만 설정해서 전송하고 SYN/ACK 응답이 오면 ACK를 보내지 않아 서버 측은 Half Open 상태가 되고 연결 요청을 메모리 공간인 백로그 큐(Backlog Queue)에 쌓고 변조된 요청을 계속적으로 보냄으로서 백로그 큐의 포화를 일으켜 서비스 거부상태를 일으키게 된다[3, 4].

이러한 IP Spoofed SYN Flooding 공격기법의 대응방안으로는 3가지를 설명하겠다. 첫 번째로 백로그 큐 확장 기능으로 백로그 큐를 확장하여 임시적으로 연결요청을 수용한다. 두 번째로 SYN cookie의 기능을 이용한것으로3-Way handshaking 과정을 다소 변경하여 TCP 헤더의 특정 부분을 뽑아내 암호화알고리즘 방식으로 하여 적절한 연결 요청에 대해서만 연결을 맺기 위한 리소스를 소비한다.세번째로 SYN Proxy을 이용하여 클라이언트의 SYN을 보안장비에서 응답하고, 클라이언트가 ACK를 보내 정상적인 세션을 맺을 때, 보안 장비가 사용자 SYN Proxy Table에 등록하여 통신을 허락하는 방식이 있다[3, 4].

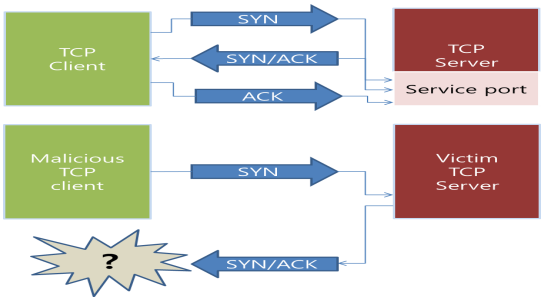

Fig. 3. IP Spoofed SYN Flooding Scenario

2.1.2 TCP Connection Flooding 공격

IP를 변조하지 않고 실제 IP를 사용하여 많은양의 TCP SYN 패킷을 공격대상에 전송하여 공격 받는 서버는 다수의 ESTABLSHED 세션 상태가 발생하게 하여 서버 부하를 일으키는 공격 기법이다.

이러한 TCP Conection Flooding 공격의 대응방안으로는 DDoS방어 장비에서 탐지된 공격 IP 확인 후 방화벽에서 차단하여 SYN 패킷이 전송되는 것을 차단하는 것이다[3, 4].

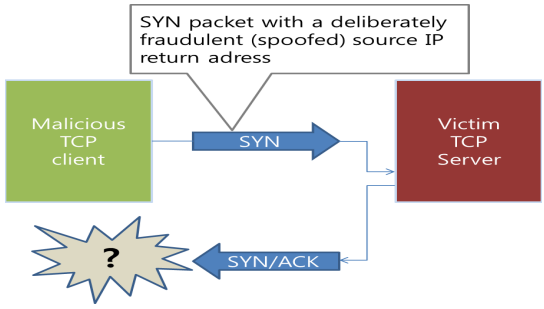

Fig. 4. TCP Connection Flooding Scenario

2.1.3 TCP Out-of-State Packet Flooding 공격

수많은 ACK/SYN + ACK/FIN/RST 등의 패킷을 공격하는 대상의 서버로 전송방식으로 방화벽이나 L4 등에서 같이 세션을 관리하는 장비에서 차단하지만 일부분의 네트워크 장비 또는 서버의 CPU 사용량이 올라가는 작동 발생 가능성이 있다.[4, 5]

이러한 TCP Out-of-State Packet Flooding 공격기법의 대응방안으로는 세가지가 있다. 첫 번째로 IP가 변조되었을 경우 IP Spoofed SYN Flooding 공격 대응 방안과 일치한다. 두 번째로 IP가 변조되지 않았을 경우는 TCP Connection Flooding 공격 대응 방안과 동일하다. 세 번째로 취약한 서버 또는 네트워크 장비에 대한 패치 및 교체 진행하는 방식이 있다[4, 5].

2.2 대용량 트래픽 전송(Bandwidth Consuming)

UDP/ICMP Flooding은 1000~1500byte 규모의 큰 패킷을 공격하는 대상 서버로 전송하여 네트워크 회선 대역폭을 고갈시켜 공격 대상서버와 같은 네트워크에 있는 모든 서버의 접속 장애를 유발시킨다.[4, 6]

대응방안으로는 3가지를 설명하겠다. 첫 번째로 임시방편으로 공격하는 대상의 서버에 대해 NULL 라우팅을 적용한다. 두 번째로 공격하는 대상의 서버에 대해 NULL 라우팅을 적용하여 점진적인 공격에 대한 트래픽 감소에 대하여 ISP(Internet Service Provider)/IDC(Internet data center)와 협조하여 차단한다. 세 번째로 동일 네트워크에서 운영 중인 다른 서버/서비스를 보호한다[4, 6].

2.3 웹 서비스 지연(HTTP Flooding)

IP를 변조하지 않고, 정상적인 3way handshaking 후 상품조회 및 로그인과 같은 동일한 URL 반복 요청하여

일부 웹 서버의 CPU 및 Connection 자원의 고갈을 유발하는 것이다[4, 7].

대응방안으로는 DDoS 방어 장비에서 탐지된 공격 IP 확인 후 방어벽 차단 하고 서버 설정을 KeppAlive를 off로 변경, MaxClient를 최대 수치로 조정한다[4, 7].

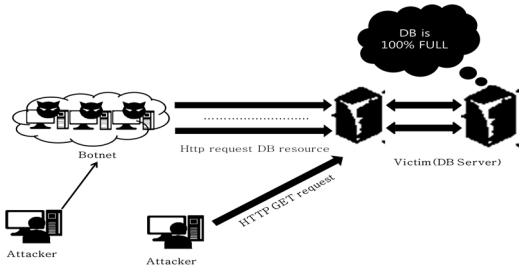

Fig. 5. HTTP Flooding scenario

Table 2. DDoS attack types and effects

Protocol	Attack Type	Impact of the attack
TCP	SYN Flood	Session and server queue exhaustion attacks
	Out-of-State TCP Flag Flood	
	Connection Flood	
	HTTP Flood	
UDP/ICMP	UDP Flood	Bandwidth exhaustion
	ICMP Flood	
	IGMP Flood	CPU / Session exhausted
Etc.	Anomaly attack	

3. DDoS 대응전략

3.1 라우터 및 스위치 설정

라우터 혹은 스위치에서 제공하는 애플리케이션 제어 언어인 ACL을 이용하여 DDoS 공격 트래픽일 가능성이 큰 패킷을 차단한다.

3.1.1 IP주소 Spoofing 공격 트래픽차단 ACL설정

URPF(Unicast Reverse Path Forwarding)의 FIB (Forwarding Information Base)tables를 이용해서 Table에는 없는 Source IP 주소가 유입 시 차단하고 ACL을 사용해서도 사설 네트워크 대역이나 Broadcast 주소를 차단함으로써 IP주소 Spoofing을 방지한다. 다음 Table 3은 RFC 1918에 정의된 모든 IP 주소 영역 차단이다[4, 8].

Table 3. RFC 1918

Access-list 101 deny ip 10.0.0.0 0.255.255.255. any
Access-list 101 deny ip 172.16.0.0 0.15.255.255. any
Access-list 101 deny ip 192.168.0.0 0.0.255.255. any

3.1.2 UDP,ICMP Flooding 트래픽차단 ACL 설정

UDP 패킷의 크기가 2M 이상이면 Drop 한다[4. 7].

- Access-list 106 remark CAR-ICMP ACL
- Access-list 106 u에 any any
- 해당 Interface 선택
- Rate-limit input access-group 104 2000000 25000 25000 confrom-action
- ransmit exceed-action drop

ICMP 패킷의 크기가 256K 이상이면 Drop한다[4 8].

- Access-list 106 remark CAR-ICMP ACL
- Access-list 106 permit icmp any any echo
- Access-list 106 permit icmp any any echo-reply
- 해당 Interface 선택
- Rate-limit input access-group 106 2560000 8000 8000 confrom-action
- Transmit exceed-action drop

3.1.3 CAR(Committed Access Rate) 설정

단위 시간 동안 일정량 보다 많은 패킷들이 라우터에 들어 올 경우, 일정량 이상의 패킷은 초과시키지 않도록 설정한다[4, 9, 14, 15].

3.1.4 라우터에서 TCP SYN Attack 방지 설정

Cisco 라우터는 DDos 공격 중 SYN Flooding 공격 또는 half-open 공격에 대한 방어 방법으로 TCP Intercept 기능을 제공한다. SYN Flooding 공격 시 합법적인 호스트와 공격 호스트를 구분하는 기술로서 클라이언트의 접속 요청 SYN을 가로채어 라우터 운영체제인 IOS가 프락시로서 응답을 하며 이에 사응하는 응답 ACK로 호스트의 정당성을 확인할 수 있다[4, 10].

3.2 보안장비 설정

3.2.1 방화벽

서비스 연결에 필요한 포트를 제외한 모든 Inbound 트래픽 차단하고 DMZ 운영 시, 네트워크 대역이 아닌 서버별 허용 트래픽을 설정하고 모니터링 위해 서버별 통계자료를 확보 할 수 있는 형태로 설정한다. 장비 부하 및 서비스 품질을 고려하여 로그 정책을 설정하고 스푸핑된 IP로 부터의 트래픽 유입을 차단하기위해 방화벽에 '192.168.x.x , 10.10.x.x , 172.16.x.x.'로 부터의 트래픽 차단 정책 적용 필요하고 대역폭 공격을 차단하기 위해 불필요한 UDP, ICMP 패킷 차단 정책 적용이 필요하다[4, 11, 12, 13].

4. DDoS 대응전략 연구

4.1 응용프로그램을 이용한 트래픽 방어

DDoS 검출 응용프로그램은 트래픽들을 수집한 후 프로토콜을 분석한다. 대교적인 TCP Flooding 공격과 같은 경우에는 정상적인 TCP 패킷은 반응하지 않고 공격 트래픽만 반응하게 된다. 이것은 정상적인 TCP패킷은 연결설정을 목적으로 하나 비정상적인 패킷은 완전한 쓰리웨이 핸드쉐이킹을 하지 않고 계속적으로 패킷을 보내므로 트래픽을 발생시키게 된다. 이러한 TCP 플로딩의 경우 일정량의 유입패킷이 일치하게 된다. 따라서 [Fig. 6]과 같은 구조상에서 5초 이상의 동일양의 패킷이 계속 유지된다면 이것은 공격으로 탐지된다. 마찬가지로 UDP 플로딩 경우는 TCP플로딩과 같은 방법으로 공격을 탐지한다. 마지막으로 ICMP 공격 탐지는 공격 트래픽의 경우 패킷의 크기가 256K이상이면 적용 시켜서 탐지하여 드롭시킨다. 이러한 기능을 알약, V3와 같은 실시간 검색기법을 이용하여 수시로 변하는 트래픽의 양을 분석하고 공격 패킷인지 확인한다.

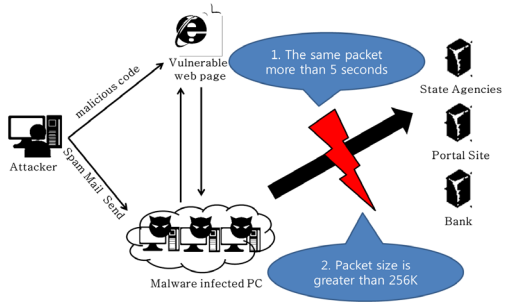

Fig. 6. Using a traffic defense applications

4.2 일정이상의 사용자 서비스 인증제도

DoS 와 DDoS의 경우 방식의 차이는 있지만 서비스 거부 공격이므로 한 사이트 혹은 서버에서 이용자의 서비스 범위는 최대에서 일정량의 여유공간을 남겨두고 일정이상의 사용자가 접속 시 평소와 다른 창이 열려 다른 방식으로 사이트에 인증서 로그인으로 바로 로그인 화면으로 넘어가서 계속되는 서비스 거부 공격을 접속할 수 있게 하여 과도하게 한 서버에 집중되는DoS와 DDoS에서 벗어 날수 있다.

4.3 빅데이터를 이용한 트래픽 분석

현재 데이터의 주로 미래 예측, 상황 분석, 분위기 측정, 이상 감지 등을 통해 품질 개선, 공정 개선, 신상품 개발, 고객 행동 패턴 분석, 부정 행위 판별 등에 활용되고 있다. 이러한 관점을 DDoS에 관한 패킷을 심층적으로 분석하여 DDoS공격을 방지할수 있다.

5. 결론

DDoS 공격은 인터넷의 항상 안전함과 굳게 믿을 수 있는 신뢰성에 심각한 위협을 가하고 있다. 공격은 점점 더 조직화, 정교화 되고 있으며, 이러한 공격기법들에 대응하기 위하여 많은 대응분석기법도 제안되었다. 최근에 일어난 DDoS 공격이 불특정한 대상으로 하고 있으나, 공격의 대상은 언제든지 전체 네트워크로 바뀔 수 있으며, 이런 경우, 전체 네트워크에 대한 총괄적인 대응체제가 사전에 준비되어 있지 않다면, 전체 인터넷의 마비뿐만 아니라 글로벌 사회의 마비를 유발하게 되어, 천문학적인 피해가 발생할 것이다. 이와 같은 DDoS 공격상황을 극복하기 위해서는 서버에서 들어오는 전체 네트워크를 지속적으로 감시하여, 신속한 공격의 탐지 및 차단을 수행하는 것뿐만 아니라, DDoS 공격 발생 이전부터 공격을 시도하기 위한 행위들을 탐지하여 이를 사전에 차단함으로써, 공격 자체가 불가능하도록 해야 한다. 이를 위해 본 논문에서는 기존에 나와 있던 DDoS 공격들을 소개하고 라우터와 방화벽을 통해서 모든 DDoS가 차단되지는 못하지만 기존의 있던 DDoS와 대응전략 연구로 인하여 향후에 있을 DDoS 공격을 효과적으로 차단하기 위해 제안하였다.

참 고 문 헌

[1] Sunghyuck Hong, “Analysis of DDoS attack and countermeasure: Survey”, Journal of Digital Convergence, vol. 12, no. 1, pp.423-429, Jan, 2014

[2] Xiang,, Yang; Li, Zhongwen, "An Analytical Model for DDoS Attacks and Defense," Computing in the Global Information Technology, 2006. ICCGI '06. International Multi-Conference on, vol., no., pp.66, Aug. 2006

[3] Yu Chen; Kai Hwang, "Collaborative Change Detection of DDoS Attacks on Community and ISP Networks," Collaborative Technologies and Systems, 2006. CTS 2006. International Symposium on, vol., no., pp.401-410, 14-17 May 2006

[4] Kang-San Jang, 2013 University Circle Information Security Information Security Training Education (incident response plan), KISA, pp.55-116

[5] Wang Hao-yu; Zhu Xu; Cao Hui-zhi; Ji Chao-jun; Ji Xiao-juan, "The Security and Promotion Method of Transport Layer of TCP/IP Agreement," Information Technology and Computer Science (ITCS), 2010 Second International Conference on, vol., no., pp.513,517, 24-25 July 2010

[6] Gallego-Nicasio Crespo, B., "User Interface Harmonization for IT Security Management: User-Centered Design in the PoSecCo Project," Availability, Reliability and Security (ARES), 2013 Eighth International Conference on, vol., no., pp.829,835, 2-6 Sept. 2013

[7] Hwi-Seok Jeong, Detection and Protection of Distributes Denial of Service Attacks through the Traffic Analysis, 2003.

[8] Chul-Ho Lee·Kyung-Hee Choi·Jeong-Gi Hyeon·Sang-Uk Noh, Detection of Distributes Denial of Service Attacks through the analysis of traffic, June, 2003

[9] Jin-Seok Yanh, A DDoS Attack Test, Analysis and Mitigation Method in Real Networks, 1226-9182, 2013

[10] Rash Michael, Linux Security Systems Guide sets, Acorn, pp.105-172, January, 2010

[11] Sunghyuck Hong, Sunho Lim, "Analysis of attack models via Unified Modeling Language in Wireless Sensor Networks: A survey study," WCNIS, vol., no., pp.692-696, 25-27 June 2010

[12] Zargar, S.T.; Joshi, J.; Tipper, D., "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," Communications Surveys & Tutorials, IEEE , vol.15, no.4, pp.2046-2069, 2013

[13] Rawal, B.; Ramcharan, H.; Tsetse, A., "Emergence of DDoS resistant augmented Split architecture," HONET-CNS, 2013 10th International Conference on , vol., no., pp.37,43, 11-13 Dec. 2013

[14] Robichaud, Y.; Changcheng Huang; Jinmei Yang; Peng, H., "Access delay performance of resilient packet ring under bursty periodic class B traffic load," Communications, 2004 IEEE International Conference on, vol.2, no., pp.1217,1221 Vol.2, 20-24 June 2004

[15] Carr, A., "Development and trials for W-CDMA infrastructure," UMTS - The R&D Challenges (Ref. No. 1998/496), IEE Colloquium on, vol., no., pp.7/1,7/7, 23 Nov 1998

저 자 소 개

홍 성 혁(Hong, Sunghyuck) [종신회원]

- 1995년 2월 : 명지대학교 컴퓨터공학과(공학사)
- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교, 정보통신학부 교수

<관심분야> : 네트워크 보안, 센서네트워크