논문 2009-2-13

CDN 기술을 이용한 DDoS 공격에 대한 대안 방법

A Solution Method for DDoS Attack using CDN Technology

노대희*, 유대영*, 안병구**

Dae-Hee Noh, Dae-Young You, Beong-Ku An

요 약 DDoS 공격은 IP주소에 대한 특별한 인증 없이 무제한적으로 대규모의 데이터 패킷을 전송할 수 있다는 인터넷의 취약점을 이용하는 공격이다. 본 논문에서는 DDoS 공격에 대한 연구와 대안으로 CDN 기술을 이용한 대처 방법을 제안한다. 성능평가는 시뮬레이션을 통해서 기존의 대응 방안과 문제점을 알아보고 개선된 대응 방안과 비교 한다.

Abstract The attacks of DDoS use the weakness of Internetworks which can send unlimited great data packets without identification of IP address. In this paper, we propose a solution method for DDoS attacks using CDN technology. The performance evaluation of the proposed solution method is performed via simulation.

Key Words : DDoS Attacks, DSN, CDN

Ⅰ. 서 론

다수의 인터넷 사용자는 TCP/IP 프로토콜[1][2]을 이용하여 발송자의 IP 주소를 가지고 목적지의 IP 주소로 임의의 데이터 패킷을 전송하여 인터넷 서비스를 이용한다. DDoS [3][4][5] 공격은 IP주소에 대한 특별한 인증 없이 무제한적으로 대규모의 데이터 패킷을 전송할 수 있다는 인터넷의 취약점을 이용하는 공격이다. DDoS 공격은 그림 1과 같은 구성을 가진 수백 혹은 수천 개의 좀비 시스템들을 이용해서 공격의 목적이 되는 시스템을 공격하는 형태를 가진다. 감염된 좀비 시스템들은 자신의 시스템에 어떤 일이 일어나고 있는지 인지하지 못 한 채 원격 공격 명령이 떨어지면 그 순간 일제히 타겟 시스템을 공격하게 된다. DDoS 공격[3][4][5]은 엄청난 볼륨의 패킷들을 발송하거나 불완전한 형태의 요청 패킷을 발송하여 공격 대상이 되는 네트워크 장비나 서버가 정상적인 서비스 요청을 받아들일 수 없는 상태, 혹은 자신의 능력으로 처리할 수 있는 용량을 초과하여 처리 불능의 상태에 빠지게 만드는 것이다.

본 논문의 Ⅱ장에서는 관련 연구를, Ⅲ장에서는 그에 따른 제안된 DDOS 공격에 대한 효과적인 환경 구성에 대해 제안하고, Ⅳ장에서는 제안된 대처 방법의 성능을 시뮬레이션을 통해 성능을 측정하고, Ⅴ장에서 결론을 맺도록 한다.

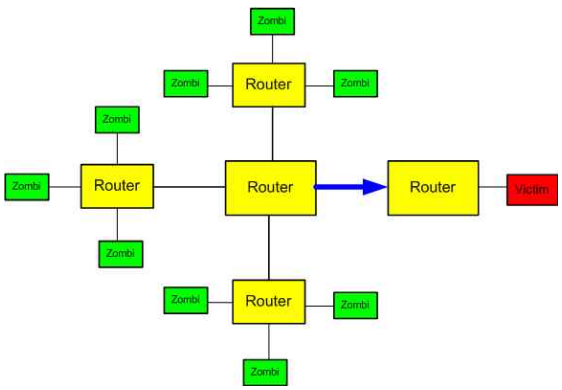

그림 1. 좀비컴퓨터를 이용한 DDOS 공격
Fig. 1 DDoS attacks by zombi computer

*준회원, 홍익대학교 컴퓨터정보통신공학과
**종신회원, 홍익대학교 컴퓨터정보통신공학과
접수일자 2009.3.15, 수정완료 2009.4.5

II. 관련연구

Domain Name System(DNS) [1][2]는 인터넷에서 호스트의 이름과 그 숫자 주소의 연결을 제공하는 디렉토리 참조 서비스이다. DNS는 다음처럼 4개의 구성요소로 이루어진다. (i)**영역 이름 공간:** DNS는 인터넷상의 자원을 식별하기 위하여 트리 구조의 이름 공간을 이용한다. (ii)**DNS 데이터베이스:** 개념적으로 이름공간 트리 구조의 각 노드와 잎노드는 자원레코드에 포함된 정보의 집합을 가르킨다. (iii)**이름서버:** 이것은 영역 이름 트리 구조의 일부와 그에 관련된 정보를 갖고있는 서버 프로그램이다. (iv)**주소 해결자:** 클라이언트의 요청에 응하여 이름 서버로부터 정보를 추출하는 프로그램이다. **Content Delivery Networks**(CDN) [6][7][8]이란 인터넷에서 동영상이나 음악 스트리밍, 파일 다운로드 등 대용량 파일로 인한 트래픽이 증가할 때, 네트워크 주요 지점에 설치한 전용 서버에 해당 콘텐츠를 미리 저장하여 이용자 가까운 곳의 서버로 유지시켜주는 서비스를 말한다. CDN 서비스의 주요 기술은 다음과 같다.

- **GLB(Global Load Balancing):** 인터넷의 여러 곳에 분산 배치된 서버들 중에서 이용자에게 최상의 서비스를 제공할 수 있는 서버를 선정해 서비스를 연결하는 기술로, 최상 위치의 서버에 장애가 일어났을 경우에도 차상위 서비스를 할 수 있는 서버로 우회 연결하여 장애를 해소시키게 된다. 자체 장애에 대비해 서로 다른 네트워크상에 이중으로 배치하게 된다.
- **동기화(Synchronization) 기술:** 콘텐츠 변경 시 ISP별로 분산된 서버에 이를 즉각적으로 반영하여 사용자들이 한꺼번에 동일한 내용의 콘텐츠를 전송 받을 수 있도록 하는 기술로 분산된 서버의 어느 하나에도 파일의 유실이나 오류가 없도록 한다.
- **Grid Delivery:** 단기간 급증하는 트래픽 처리를 위해 콘텐츠 업계가 활용할 수 있는 방법은 첫째, 단기간에 다량의 서버와 네트워크를 투입하는 방법, 둘째, P2P [8]기술을 활용해 트래픽을 분산시키는 방법, 셋째, 일정 트래픽까지는 서버를 활용하되 그 이상에 대해서는 P2P 기술을 활용하는 혼합적 방법이 있다.

현 DDoS공격의 대응 방법들은 소규모의 대응 방법에는 그 효과가 있지만 봇을 통한 대량의 분산 서비스 거부 공격이나 분산 반사 서비스 거부 공격에는 성능이나 네트워크의 대역폭의 문제로 인해서 충분히 그 역할을 다하지 못하고 ISP나 IDC에서는 타 사용자들의 서비스까지 문제를 일으키기 전에 피해 시스템 서비스를 블랙홀링이나 라우터 필터링 기법으로 차단을 하게 된다. 그러면 결국은 해당 피해 시스템 서버는 정상적인 서비스를 하지 못하고 결국 공격자가 원하는 서비스 거부 공격이 이루어지게 되고 공격을 중단하게 하기 위해서 공격자가 요구하는 금품을 제공하게 되는 악순환이 일고 있다.

III. DDoS 공격에 대한 대응 방안

3.1 제안된 시스템

(1) S-DNS를 이용한 캐시서버 접속

아래 그림 2는 본 논문에서 제안하는 S-DNS 의 동작 방식을 도식화한 것이다.

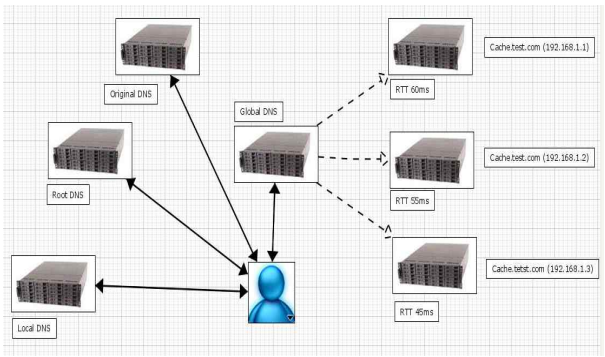

그림 2. S-DNS의 동작 방식
Fig. 2 Operation of S-DNS

제안된 S-DNS 시스템의 동작 순서는 다음과 같다.

- **Step 1:** 사용자가 웹 서비스를 이용하기 위해서 접속하고자 하는 웹 서버의 도메인 주소를 로컬 DNS에 질의
- **Step 2:** 로컬 DNS는 자신에게는 해당 웹 서버의 정보가 없으므로 Root DNS로 질의하라고 응답
- **Step 3:** 사용자의 시스템은 다시 Root DNS로 질의하고 도메인에 따라 다르겠지만 한 두 번의 Root DNS 질의를 거침

- **Step 4:** 웹서버의 DNS정보를 가지고 있는 Original DNS의 IP응답
- **Step 5:** 다시 사용자는 Original DNS서버에 질의를 하고, Original서버는 자신에게 정의된 CNAME 설정으로 포워딩된 S-DNS로 다시 질의하라고 응답
- **Step 6:** 다시 사용자는 S-DNS에게 질의
- **Step 7:** S-DNS는 Cache 서버들에게 질의를 하게 되고 RTT를 비교하여 가장 RTT값이 적은 IP를 가진 Cache서버의 IP를 반환
- **Step 8:** S-DNS는 가장 가까운 Cache서버의 IP를 전달
- **Step 9:** 사용자는 Cache 서버에 접속하여 웹서비스를 이용하게 됨

(2) CDN 서비스를 이용한 동기화

본 논문에서 제안하는 원본서버와 캐시서버의 구성은 그림 3과 같으며, 동작 과정은 다음과 같다.

- **Step 1:** 앞서 소개한 CDN 서비스 주요기술 중 동기화 서비스로 캐시서버 와 원본 서버의 관계를 설정한다.
- **Step 2:** 원본서버와 캐시서버 사이에 방화벽을 구성하여 등록된 캐시서버 IP외에 모든 접근을 차단한다. 이는 차후에 공격자가 원본 서버의 IP주소를 알아내어 원본서버에 대한 DDoS 공격을 방지하기 위함이다.
- **Step 3:** CDN 서비스의 로드밸런싱 기능은 앞서 설명한 S-DNS에서 담당하게 된다. 아래 그림5는 제안된 대응방안이 적용된 전체 시스템이다.

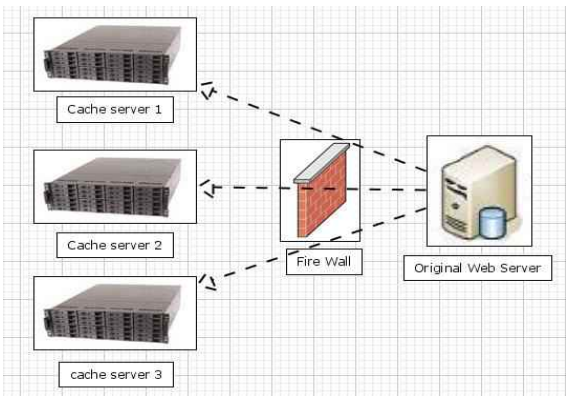

그림 3. 동기화 CDN 서비스 구성
Fig. 3 Structure of synchronous CDN service

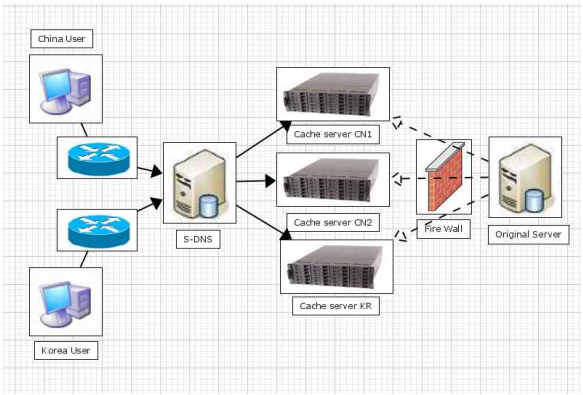

그림 4. S-DNS와 CDN 구성된 전체시스템
Fig. 4 System structure by using S-DNS and CDN

IV. 성능 평가

4.1 성능 평가 환경

기존의 시뮬레이션 도구인 NS-2나 OPNET의 경우, 프로토콜이나 패킷의 종류에 대한 분석에 치우쳐져 있다. 물론, 네트워크 분석에서 패킷과 프로토콜의 분석은 매우 중요한 부분을 차지한다고 할 수 있지만, 기존의 시뮬레이션 도구로는 DDoS 공격에 예측할 수 있는 환경적인 요인들에 대한 분석에 한계가 있다고 본다. 그래서, DDoS에 특화된 간단한 시뮬레이션 도구를 자바언어 로 구성하여 기존의 환경과 변화된 환경사이의 성능을 측정하였다. 개방환경은 Java SDK update6, 라이브러리는 JHotdraw 7.0, 개발도구로는 Eclipse SDK를 사용 하였다.

4.2 성능평가 파라미터

앞서 살펴본 것 같이 DDoS 공격의 형태는 다양하기 때문에 성능측정을 할 때에는 실제와 같은 환경을 구성하고 측정하기는 어렵다. 기존의 연구에서 DDoS 공격을 분석하기 위한 주요한 성능평가 파라미터 로는 패킷 비율, 프로토콜비율, 공격포트넘버, Flag신호 비율 등을 들 수 있다. 본 논문에서 우리는 대표적으로 네트워크에 영향을 미치는 변수를 우선순위로 고려하여 성능측정을 하였다. 본 성능측정에서 사용할 파라미터들은 다음과 같다.

- **패킷의 평균량(Packet avg):** 패킷량은 DDoS공격 여부를 판단할 수 있는 중요한 요소이다.
- **처리율(throughput):** 네트워크요소에서 처리율은 라우터/서버/회선을 생각할 수 있다. DDoS공

격은 라우터 와 서버를 공격대상으로 하기 때문에 변수로 두고 측정하였다.

처리율(Packet/ms) = (패킷처리시간/단위시간)

- **RTT(RoundTrip Time):** RTT는 상대적인 요소로서 시간에 따라 변화한다. RTT는 사용자 와 서버간의 회전 시간으로 RTT값이 작다면 물리적으로 가까운 위치에 있다거나, 네트워크가 유휴상태에 있다는 것을 의미한다.
- **DDoS 공격패턴:** DDoS 공격패턴은 지속시간 과 패킷증가비로 정의하였다.

4.3 성능 측정 요소

그림 5는 시뮬레이션 인터페이스 구성을 보여주고 있다. 성능측정에 앞서 자바로 구성한 시뮬레이터의 인터페이스에 대한 설명을 하면 아래와 같다.

- 컴퓨터 : 클라이언트를 의미하며 , IP대역폭, 패킷 평균량 ,DDoS공격패턴의 입력값을 받는다.
- 라우터 : 클라이언트와 서버 사이의 라우터를 의미하며, 처리량의 입력값을 받는다.
- 캐시서버 : 오리지널 서버에 CDN서비스를 구성할 캐시서버로 IP주소 ,RTT값, 처리율의 입력값을 받는다.
- 서버 : DNS서버와 오리지널서버를 의미하며, IP주소, 등록된 캐쉬서버를 입력값으로 받는다.
- 회선 : 각 구성요소들의 관계를 설정해주는 회선
- 구성환경 : 각 구성요소들이 배치되는 화면
- 파라미터 입력창 : 각 구성요소들의 파라미터를 입력할 수 있는 입력창.

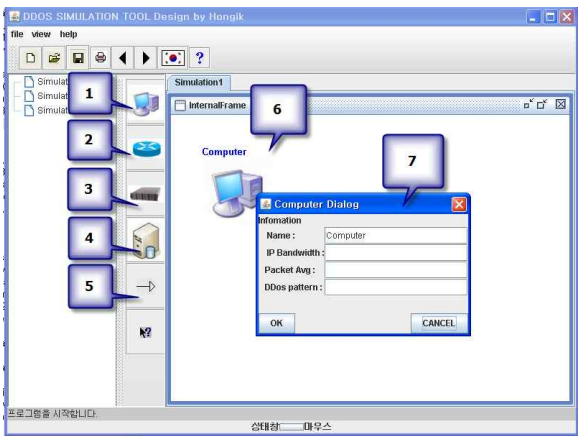

그림 5. 시뮬레이션 인터페이스 구성
Fig. 5 Structure of simulation interface

본 성능측정에 구성요소는 표 1과 같다.

표 1. 성능측정의 구성요소
Table 1. System environments for performance evaluation

시스템 명칭	설 명
Cache Server CN	중국 IDC에 설치된 서버
Cache Server CN2	중국 IDC에 설치된 서버
Cache Server KR	한국 IDC에 설치된 서버
Original Web Server	Cache 서버와 CDN 관계
S-DNS	제안된 DNS
Fire wall	IP 패킷 접근 차단

아래 그림 6은 두 지역의 사용자가 라우터를 통하여 CDN서비스가 적용된 3대의 캐시서버에 접속하는 환경을 구성한 것이다. 사용자1은 한국 내에 IP주소로 접속한 경우이고, 사용자2의 경우는 중국IDC를 거쳐 접속했다고 가정하였다. 파라미터값으로는 25Gbytes 의 평균 패킷량으로 가정하고, t=2000sec에 들어온다고 하였을 때, 측정값은 아래 그림9와 같다.

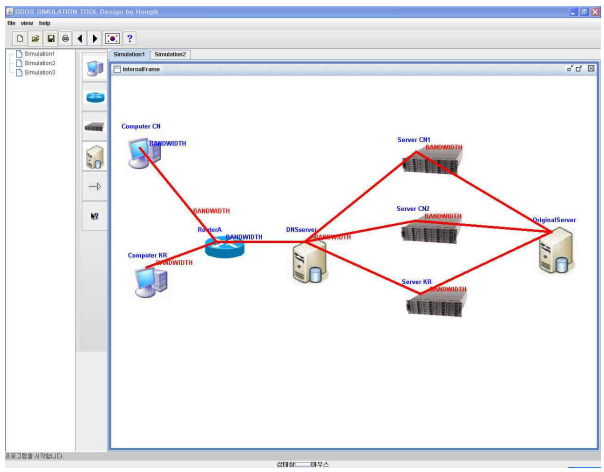

그림 6. 성능평가를 위한 시스템 구성도
Fig. 6 System structure for performance evaluation

그림 7의 결과 값에서 보여 지듯이, 중국측에서 DDoS 공격이 들어오더라도 한국 내 IP 대역폭에 존재하는 캐시서버는 DDoS공격에 영향을 받지 않는 것을 측정할 수 있다. 중국측 캐시서버 1, 2는 RTT의 변화에 따라 들어오는 패킷 량 을 분담하는 것을 확인할 수 있다.

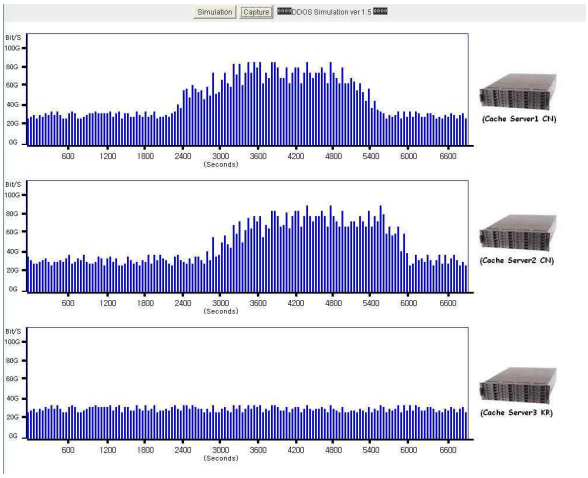

그림 7. DDoS 공격패턴 1
Fig. 7 DDoS attack pattern 1

그림 8은 중국에서 대규모의 트래픽공격 (평균패킷량 = 100G) 이 왔다고 가장했을 때의 결과 값 이다.

결과적으로 중국 쪽 캐시서버는 (처리율<패킷평균량) 이 되어 캐시서버가 서비스거부(Denial of Service) 상태가 되지만, 한국 내에 캐시서버에는 영향을 주지 않으므로, 한국 사용자는 정상적으로 서비스를 이용할 수 있게 된다.

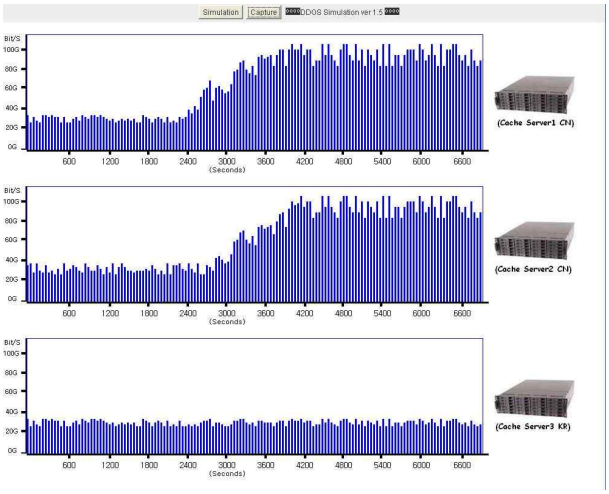

그림 8. DDoS 공격패턴 2
Fig. 8 DDoS attack pattern 2

V. 결 론

본 논문에서는 CDN와 S-DNS 기술을 이용한 글로벌 로드 밸런싱에서 아이디어를 통해서 분산 서비스 거부 공격에 대한 개선된 대응 기술을 제시했다. 특히 Cache 서버를 이용해 중국발 분산 서비스 거부 공격을 대역폭이 작은 국제가 아닌 중국의 국내 트래픽으로 돌리게 하고, 지속적인 공격 시 추가적으로 다른 Cache 서버들을 두어 공격 트래픽을 분산시키면서 수천만원의 보안장비를 이용한 고비용의 기존 대응 방식과는 다르게, 중국 IDC에 서버만 넣어두면 추가적인 비용이 발생하지 않아 효과적인 대응이 가능함을 보였다. 국제 패킷량 의 60% 이상이 중국을 경유한다는 연구결과에서 보듯이 중국 IDC에 캐시서버를 두는 것을 고려해 보아야 할 것이다. 앞으로도 더욱 분산서비스 거부 공격이 기승을 부릴 것으로 예상이 되는데, 본 논문에서 제안한 대응 방법을 좀 더 연구하여 사용한다면 좀 더 효과적인 대응 및 온라인 기업의 사업 안정성이 보장되며 서비스 공격 자체가 줄어들어 깨끗한 네트워크가 될 수 있을 것이다.

참고문헌

[1] Dimitri Bertsekas, Robert Gallager, “Data Networks,” Prentice Hall, Second Edition.

[2] James F. Kurose, Keith W. Ross, “Computer Networking: A Top-Down Approach Featuring the Internet,” Addison Wesley, Second Edition.

[3] Yang Xiang, Wanlei Zho Li, “An Analytical Model for DDoS Attacks and Defense,” Proc. of ICCGI 2006, August 2006.

[4] Jun Xu, Wooyong Lee, “Sustaining Availability of Web Services under Distributed Denial of Service Attack,” IEEE Transaction on Computers, vol.52, no.2, pp.195-208, February 2003.

[5] Wei Lu, Issa Traore, “An Unsupervised Approach for Detecting DDoS Attacks based on Traffic-based Metrics,” Proc. of PACRIM2005, pp.462-465, August 2005.

[6] Kartik Hosanagar, Ramayya Krishnan, Machael Smith, John Chung, “Optimal Pricing of Contebt Delivery Network (CDN) Services,” Proc. of HICSS 2004, January 2004.

[7] Mukaddim Pathan, Rajkumar Butta, “Performance

models for peering Content Delivery Networks," Proc. of ICON2008, December 2008.

[8] Daniel Pakkala, Aki Koivukoski, Tuomas Paaso and Juhani latvakoski, "P2P Middleware for Extending the Reach, Scale and Functionality of Content Delivery Networks," Proc. of ICIW2007, May 2007.

※ Acknolodgement : This work was supported by the Korea Science and Engineering Foundation Grant.
(KOSEF-R01-2007-000-20400-0)

저자 소개

노 대 희(준회원)

• 2009년: 홍익대학교 컴퓨터정보통신공학과 졸업 (BS)
<주관심분야: 정보보안, 네트워크보안, 무선네트워크>

유 대 영(준회원)

• 2009년: 홍익대학교 컴퓨터정보통신공학과 졸업 (BS)
<주관심분야: 정보보안, 네트워크보안, 무선네트워크>

안 병 구(종신회원)

• 1988년:경북대학교전자공학(BS),
• 1996년:(미)Polytechnic Univ. Dept. of Electrical & Computer Eng.(MS),
• 2002년:(미)New Jersey Institute of Technology(NJIT), Dept. of Electrical & Computer Eng. (Ph.D),
• 1990년-1994년: 포항산업과학기술연구(RIST), 선임연구원,
• 1998년-2002년: Lecturer, New Jersey Institute of Technology(NJIT). USA,
• 2003년-현재: 홍익대학교 컴퓨터정보통신공학과 교수,
• 2005-2008: Marquis Who's Who in Science and Engineering was listed,
• 2006-2008: Marquis Who's Who in the World was listed
<관심분야:Wireless Networks, Ad-hoc & Sensor Networks, Multicast Routing, Cross-Layer Technology, Cooperative Communications, QoS, Mobility Management, Location-Based Technology>