JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 3 : 602~608 Mar. 2014

무선랜 침입탐지를 위한 경량 시스템 설계 및 구현

김한길[1] · 김수진[2] · 이환규[2] · 정회경[3*]

Light-weight System Design & Implementation for Wireless Intrusion Detection System

Han-Kil Kim[1] · Su-Jin Kim[2] · Hwan-Kyu Lee[2] · Hoe-kyung Jung[3*]

[1]Department of Sound Production, Korea College of Media Arts, Sejong 339-713, Korea
[2]Co. Ltd Ubi Tech, Daejeon 305-340, Korea
[3*]Department of Computer Engineering, Paichai University, Daejeon 302-735, Korea

요 약

스마트폰 사용이 일반화되고 스마트워크, BYOD(Bring Your Own Device) 트렌드가 확산되면서 국내 무선랜 사용이 가속화되고 이로 인해 보안위협도 크게 증가하고 있다. 시스코시스템즈, 아루바네트웍스 등 무선랜 업체들은 WIPS(침입탐지), MDM(모바일단말관리), DLP 등 다양한 제품들을 출시해오고 있지만 비용이나 관리적인 측면에서 소규모 기업에서는 도입하기가 쉽지 않다.

본 논문에서는 고가의 H/W 장비를 도입하지 않고 무선랜 환경에서 패킷분석, AP, Station관리, 보안취약점을 분석할 수 있는 무선랜 침입탐지 시스템을 제안하고자 한다.

ABSTRACT

Smartphones have become commonplace to use smart, BYOD (Bring Your Own Device) spread the trend of domestic WLAN use is intensifying as a result, the security threat will be greatly increased. Even though WLAN vendors such as Cisco Systems Inc,. Aruba networks released WIPS, MDM, DLP etc, however, these solutions can not be easily introduced for small business due to high cost or administrative reasons.

In this paper, without the introduction of expensive H/W equipment, in WLAN environments, packet analysis, AP, Station management, security vulnerabilities can be analyzed by the proposed intrusion detection system.

키워드 : WIDS, WIPS, 침입탐지, 침입차단

Key word : WIDS, WIPS, Intrusion Detection, Intrusion Protection

접수일자 : 2013. 12. 05 심사완료일자 : 2013. 12. 16 게재확정일자 : 2013. 12. 30

*** Corresponding Author** Hoe-Kyung Jung(E-mail:hkjung@pcu.ac.kr, Tel:+82-42-520-5640)
Department of Computer Engineering, Paichai University, Daejeon 302-735, Korea

Open Access **http://dx.doi.org/10.6109/jkiice.2014.18.3.602** print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

유선인터넷 중심에서 벗어나 스마트폰 등 무선단말기를 이용한 인터넷 접속이 사용이 일반화되고 정부의 모바일 전자정부 추진으로 스마트워크, BYOD (Bring Your Own Device) 트렌드가 확산되면서 국내 무선랜 사용이 가속화되고 빠르게 변화하는 사이버 환경 속에서 보안 위협 또한 계속 새롭게 진화하고 있다[1]. 유선상에서 공격 대상이 서버에 저장된 데이터였다면 무선 상에서는 모바일 기기에 담겨 있는 개인정보가 공격 대상이 되고 있다. 모바일 기기의 경우 전화번호나 개인 사진 이미지 등 사용자에게 민감한 자료가 다수 존재하기 때문에 향후 공격이 본격적으로 발생한다면 심각한 개인 정보 유출 사고들이 발생할 수 있다[2].

무선랜은 WEP/WPA/WPA2 암호화 크랙, 무선랜 인프라의 취약점에 근거한 가용성(Availability)을 침해하는 스푸핑(Spoofing), 공개와 공유 키 인증 방식을 무력화하는 무선랜 인증 해제 DoS공격, 숨겨진 SSID와 맥 필터링을 사용한 침투, PEAP/EAP-TTLS공격, 사회공학(Social Engineering)에 기반하여 사용자의 판단착오를 유도하는 Evil Twins, 세션하이제킹(Session Hijacking)공격, 취약한 클라이언트를 대상으로 하는 허니팟과 오결합 공격, 카페 라떼 등 다양한 공격기법들이 공개되어 있고, 여러 개의 기본 공격을 결합해서 좀 더 어려운 침투 시나리오를 만들어 내고 있다[3].

다양해진 공격툴들과 방법들이 공개되어 있어 쉽게 무선 구간의 데이터를 유출하거나 내부 네트워크에 침투가 가능하고 무선랜 취약점이나 모바일 단말의 취약점을 이용한 공격 또한 더욱더 지능화되고 빨라져서 국내외의 피해 가능성이 더욱 높아지고 있다. 이런 위협들에 대응하기 위해 무선랜 업체들은 WIPS(침입탐지), MDM(모바일단말관리) 등 다양한 제품들을 출시해오고 있지만 비용이나 관리적인 측면에서 일반인이나 소규모 기업에서는 도입하기가 쉽지 않다[4].

본 논문에서는 고가의 H/W 장비를 도입하지 않고 무선랜 환경에서 패킷분석, AP, Station관리, 공격기능을 테스트하고 보안취약점을 분석할 수 있는 무선랜 침입탐지 시스템을 제안하고자 한다.

Ⅱ. 선행 연구

무선랜 보안이 특히 취약한 이유 중 하나는 허가나 신고가 필요없는 ISM대역을 사용하고 있어 전파가 도달 가능한 거리에 있는 경우 어디에서든지 스니핑(sniffing)과 침투 공격이 가능하다는 점이다. 일차적으로 개방되어 있는 무선랜에 권한없이 접속하거나 해킹하여 접속함으로써 불법적으로 개인정보를 취득하는 경우도 있을 수 있으며, 타인의 IP를 도용하여 명예훼손, 저작권 침해, 바이러스 및 음란물을 유포하는 등 이차적 문제의 발생 가능성이 높다[5]. 또한 건물 밖 외부에서 건물 내부의 무선 AP에 손쉽게 접근할 수 있어 유선관문 구간의 보안장비인 FireWall, IDS 등이 무용지물이 되는 비인가자/비인가단말의 내부 네트워크 우회 접속 취약점이다. 이를 해결하기 위한 무선랜 보안 대책으로 접근 제어와 강화된 인증/암호화 방안들이 제안되고 있다.

표 1. 무선랜 보안 취약성/대응방안
Table. 1 WLAN Security Vulnerability/Responses

보안 취약점 형태	발생 사유	대응 방안	대응 가능 취약점
타인/타회사 무선랜에 제약없이 접속가능	사용자 인증 미설정	개인 - 공유키 인증기업 - IEEE802.1x 인증	미인가자 내부망 접속
무선랜에 접속하지 않고 무선구간 데이터 도청이 가능	데이터 암호화 미적용	개인 - WPA2-PSK/AES 기업 - WPA2-Enpterprise	Air Sniffing WEP/WPA Cracking MITM, 세션하이재킹

무선랜 접속인증기술은 SSID, MAC주소인증, WEP 공유키 인증, IEEE 802.1x 프로토콜 등이 있고, USIM 카드가 장착된 단말기의 경우 이동통신망을 이용한 인증 등 무선랜 표준 외의 방법으로 사용자 인증을 할 수도 있다. 무선전송 데이터 암호화 기술에는 WEP, WPA/WPA2가 있다. 이에 반해 인증과 암호 기능은 없지만 무선신호 감지 및 접속차단 통제는 물론 무선랜공격을 탐지하고 관제할 수 있는 단위 보안 솔루션 WIPS, 기업용 관리 장비로 Wireless Controller가 있다. 상용 WIPS 제품들에서 아래와 같은 위협들을 탐지하기 위한 모듈을 구현하고 있다.

(1) Rogue AP

Rogue AP들은 사용자 편의성을 위해 무선보안기능을 설정하지 않고 임의적으로 설치 및 사용된다. Rogue AP의 설치는 건물내부에 한정되어 있는 것이 아니라서, 외부로부터의 해킹에 무방비로 노출되는 역할을 한다.

(2) 보안정책위반(Mis-Configured) AP

무선랜AP는 기본적인 보안기능 및 구성방법을 제공하고 있으나 암호화미적용, WEP과 같은 낮은 수준의 보안설정 또는 보안정책에 위반되는 보안설정의 경우 전체 네트워크에 문제를 초래할 수 있게 된다.

(3) 비인가AP 접속(Client Mis-Association)

인가된 클라이언트가 외부의 비인가 AP에 접속하여 내부의 보안통제범위를 벗어난 경우이다. 만약 비인가AP 접속이 허용되는 경우라면 외부로의 자료유출이 가능하여 막대한 금전적 손실을 초래할 가능성이 높다.

(4) Ad Hoc 연결(Ad-Hoc Connection)

무선 단말들끼리 AP의 개입없이 구성되는 네트워크로, Peer-to-peer 연결과 같다. 무선사용자가 단말기를 통한 연결을 이용하여 악의적인 침입자가 사용자의 취약점을 검색하거나 공격가능하며, 바이러스감염과 같은 해킹이 가능하다.

(5) AP의 MAC 변조(AP MAC Spoofing)

무선랜 AP로부터 주기적으로 전송되는 Beacon에는 AP의 MAC 주소(AP고유ID)와 SSID (네트워크 ID정보)가 포함되어 있다. 클라이언트들은 주변의 다양한 AP에서 전송하는 각기 다른 Beacon의 정보를 수집할 수 있는 소프트웨어기반 Tool들을 사용하여 SSID와 MAC의 변경이 가능하다. 인가된 AP의 MAC주소를 도용한 불법AP는 Packet Dropping, Corruption, Modification을 통해 DoS공격이 가능하다.

(6) 불법복제AP (Honey Pot AP)

악의적인 목적을 가진 침입자가 SSID와 MAC을 복제하여 설치한다. 무선단말은 전파강도가 강한 AP에 우선 접속하기 때문에, 사용자는 불법복제된 AP에 접속하게 되고, 자신의ID, Password와 같은 정보를 전송하게 된다.

(7) DoS Attack

DoS는 공격자의 위치에 따라 내부/외부로 구분이 가능하며, 정상적인 서비스를 방해할 목적으로 대량의 데이터를 보내 대상 네트워크에서 서비스를 제공하는 AP들에 접속된 사용자들의 접속을 차단하는 공격이다. 종류에는SYN Flooding, UDP Flooding, ICMP Flooding 등이 있다[4].

Ⅲ. 제안 시스템 설계 및 구현

3.1. 제안 시스템 설계 구성사항

본 시스템은 무선랜 패킷수집 및 저장 모듈, 패킷 분석 모듈, AP/단말 상태 정보 처리 모듈, 패킷 상세분석 모듈, 연결정보 모듈, 채널 상세 분석 모듈, 공격 에뮬레이션 모듈로 구성되어 있다. 7가지의 모듈들은 따로 서버를 구현하지 않고 WIPS S/W가 설치된 데스크탑이나 노트북에서 위의 7가지의 모듈들을 통합 실행한다. 7가지의 모듈들의 설명은 아래와 같다.

(1) 패킷 수집 및 저장 모듈

패킷 수집부는 현재 2가지 방법으로 구현하였는데 먼저 OpenWRT기반 라우터에 오픈소스인 kismet을 설치하고 이를 활용하여 패킷을 수집하는 방법과 무차별 모드를 지원하는 무선랜카드를 이용하여 수집하는 방법을 사용하였다. 패킷 수집부는 향후에도 다양한 방식으로 패킷을 수집할 수 있기 때문에 유동성을 두어 구현하였다.

(2) 패킷 분석 모듈

패킷 분석 모듈은 패킷분석시 공통으로 처리하는 작업들을 라이브러리화 하였다. 이 모듈을 기반으로 AP/단말 상태 정보 처리 모듈, 패킷 상세분석 모듈, 채널 상세 분석 모듈, 공격 에뮬레이션 모듈을 구성하게 된다.

(3) AP/단말 상태 정보 처리 모듈

수집된 패킷들을 실시간으로 분석하여 존재하는 AP와 단말들을 분류하고 상세정보를 출력한다. 보안설정 상태, 인가/비인가 AP/단말을 분류할 수 있다. AP/단말 상태 정보 처리 모듈에서 분석할 결과를 리스트로 출력한다. 공격에뮬레이션은 이 리스트에서 victim을 선택한 후 공격을 시도하게 된다.

(4) 패킷 상세분석 모듈

이 모듈은 wireshark의 분석기능과 유사한 것으로 실시간분석은 물론 추후 저장된 데이터를 이용하여 포렌식 분석이 가능하도록 다양한 기능을 구현하였다.

표 2. 패킷 분석 모듈 API
Table. 2 Packet Analysis Module API

함수 이름	설명
getAddress	SourceAddress, DestinationAddress, TransmitterAddress, ReceiverAddress, BssIDAddress를 찾음.
getCapabilities Info	AP의 정보를 분석하여, Ad-Hoc, 보안 유무를 확인.
getCurrent Channel	AP의 사용 채널을 알 수 있음
getEAPOL	EAPOL프로토콜을 알 수 있음
getFrame Subtyppe	프레임의 Subtype을 알 수 있음
getRadio_ Datarate	Radiotap프레임의 데이터 전송 속도를 알 수 있음
getRadio_Dbm_ antsignal	RSSI(신호세기)를 알 수 있음
getRadio_ Frequency	radiotap프레임의 주파수를 알 수 있음
getSecurity	WPA, WP2보안 방식과 TKIP, CCMP등 암호화 방식을 알 수 있음
getSSID	SSID를 알 수 있음
getSupported Rates	지원 네트워크 속도를 알 수 있음
getWlan_fc_ds	FrameControl의 DS값을 알 수 있음
Is80211nType	802.11n 지원 유무를 알 수 있음
IsFCS	패킷의 에러 유무를 알 수 있음

- 패킷필터 입력부

다양한 방식으로 필터를 입력하여 패킷을 분류하고 총패킷수와 데이터량의 통계를 위해 다음 정보를 표시한다. 필터입력창(입력된 필터값에 따라 패킷을 검색), BSSID(검색된 AP의 MAC Address값으로 검색), 관심AP(관심AP로 등록된 AP의 MAC Address값으로 검색), 관심단말 : 관심단말로 등록된 단말의 MAC Address값으로 검색), Channel(채널 별로 검색), 802.11 Frame(Frame의 Type(Management, Control, Data) 및 Sub-Type별로 검색), Sub-type별 패킷량 표시).

- 패킷리스트 출력부

필터링된 패킷들을 출력하고 다음의 패킷 정보를 상세히 표시한다. No.(패킷 인덱스), Time(수신된 패킷 시간), Source(송신 단말 MAC Address), Destination(수신 단말 MAC Address), Length(패킷 길이), Type(802.11의 Sub-type), Info(SSID, 채널 출력).

- 패킷상세정보/헥사정보 표시부

패킷의 헥사 정보를 표시하고 헥사 정보에 해당하는 text정보들을 맵핑하여 표시한다.

(5) 연결정보 모듈

관심AP/단말을 설정하여 인가/비인가 AP/단말정보를 관리하고 보안정책에 위배되는 경우를 직관적으로 파악할 수 있다. 또한 AP/단말사이의 연결선 상태로 트래픽양을 파악할 수 있도록 구현하였고 포인트별 상세정보를 확인할 수 있다.

(6) 채널 상세 분석 모듈

수집된 패킷의 채널별 AP/Station수, 신호세기, 패킷수, 데이터량을 분석하고 그래프로 추이를 표시한다.

(7) 공격 에뮬레이션 모듈

AP, 단말 정보 리스트에서 victim을 선택하여 수행하고 해당 공격에 따라 적절한 정보가 공격화면에 자동입력되도록 구성하여 Rogue AP/Fake AP, WEP/WPA키 Crack, 다양한 DoS공격(Deauthentication Association/ Deassocitaion / EAPOL/RTS/CTS Flooding)을 시도하여 무선랜 환경변화를 관찰할 수 있다.

표 3. 시스템 개발 환경
Table. 3 System Development Environment

항목	설명
운영체제	Windows 7 Professional
개발 환경	- CPU : Intel Pentium Ⅲ 800Mhz 이상 - Memory : 최소 128MB 이상 - HDD : 100MB이상 여유공간 확보 - 무선랜카드
개발언어	C#

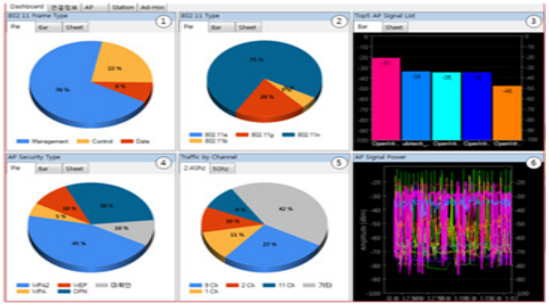

그림 1. Dashboard 화면
Fig. 1 Dashboard Screen

3.2. 시스템 구현 및 성능 평가

(1) 구현 화면

패킷수집을 시작하면 802.11 Frame Type, 802.11 Type, Top5 AP Signal, 채널 별 패킷 비율, AP RSSI 신호세기의 통계 및 그래프 정보를 실시간으로 모니터링 할 수 있도록 표시한다.

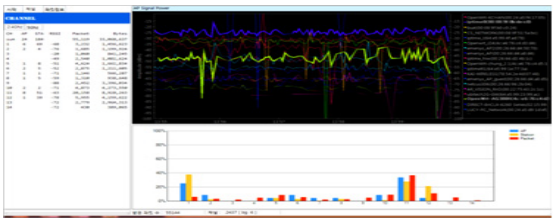

그림 2. AP & 단말 List 화면
Fig. 2 AP & Device List Screen

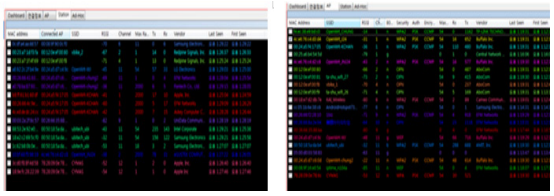

그림 3. 채널정보 화면
Fig. 3 Channel Info Screen

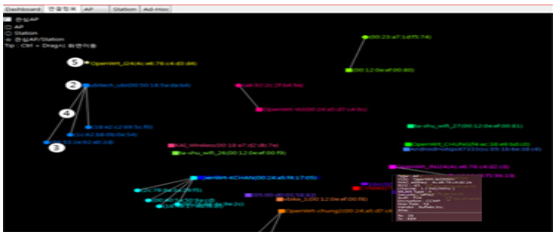

그림 4. 연결정보 화면
Fig. 4 The Connection Information Screen

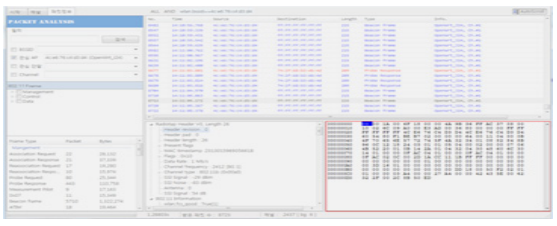

그림 5. 패킷 상세 분석 화면
Fig. 5 The Packet Detailed Analysis Screen

그림 6. 공격 에뮬레이터 화면
Fig. 6 Attack the Emulator Screen

(2) 성능 비교 평가

본 시스템은 고가의 무선 장비가 없어도 WIPS 및 무선제어관리 시스템에서 제공하는 AP/단말 상세정보, 연결정보, 채널분석 정보, 패킷분석 정보, 인가/비인가 AP/단말 관리, 탐지관리, 공격 에뮬레이션 등의 다양한 기능을 수행할 수 있다. 아래 표는 상용 WIPS에서 제공하는 기능과 비교한 것이다.

표 4. 상용 WIPS 성능 비교표
Table. 4 Commercial WIPS Performance Comparisons

비교내용 [6]	제안 시스템	상용WIPS
송/수신지 주소 캡쳐	지원	지원
포트번호 캡쳐	지원	지원
패킷 헤더 분석	지원	지원
계층별 헤더 해석	지원	지원
네트워크 성능테스트	지원	지원
전체망 분포도 모니터링	지원	지원
실시간 모니터링	지원	지원
구간 모니터링	지원	지원
필터링캡쳐	지원	지원
그래프 표시	지원	지원
분석내용 저장	지원	지원
공격에뮬레이션	지원	미지원
채널분석	지원	지원
공격탐지	지원	지원
위치추적	미지원	지원
가격	저가	고가

Ⅳ. 결 론

무선랜의 보안성을 강화시키기 위해 IEEE 802.1x와 같은 사용자 인증 및 접속 제어 기술은 무선 링크 계층 보안 기술이 표준화되고 이를 준용하는 장비가 다수 등

장하였다. 하지만 이러한 보안 기술들이 사용되더라도 사용자 단말과 액세스포인트(AP, Access Point, 이하 AP)사이에서 사용자 인증을 받고 키 일치를 하기 전까지의 모든 데이터는 암호화되지 않으며, 사용자 데이터가 아닌 IEEE 802.11 관리 및 제어 프레임들은 키 일치 이후라 하더라도 암호화가 되지 않으므로 이를 이용한 서비스 거부 공격이나 세션 가로채기 공격, 중간자 공격 등 다양한 능동적 공격 시도가 유선에 비하여 매우 쉽고, 공격이 이루어진 위치파악이 어렵다. 또한, 엔터프라이즈 망에서는 내부 사용자가 사용자 인증을 받고 정상적으로 망 접근 권한을 받은 후에 망이 정상적으로 운용되지 않도록 하는 위협의 경우에 대해 탐지 및 예방이 매우 중요하다.

따라서 무선랜 망을 계속 모니터링하면서 위협적인 공격 시도를 탐지 및 수집하고 공격 성향을 분석하여 관리자가 피드백할 수 있는 무선랜 침입탐지 시스템이 요구된다. 그러나 관리 및 비용 문제로 도입이 이루어지기가 쉽지 않다.

본 제안 시스템은 이러한 환경에 적용하여 무선랜을 침입을 통한 개인정보나 데이터의 유출 등 보안측면에서 상용시스템을 도입하기 위해 고가의 비용을 지불하지 않고 소규모 무선랜 네트워크 환경에서 무선구간의 취약성 분석관리 도구로 활용하거나, 또한 무선랜 센서 및 관리 시스템에 연계하여 통합보안관리의 한 수단으로 활용할 수 있을 것이다.

감사의 글

본 논문은 중소기업청에서 지원하는 2013년도 산학연협력기술사업(No. C0095893)에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

REFERENCES

[1] Security Market Erends "Social media and privacy protection security hardening", Ajou Economical, Nov. 2013.

[2] Trifinite group [Internet]. Available: http://trifinite.org/.

[3] Vivek Ramachandran, *BackTrack 5 Wireless Penetration Testing*, 1th ed. Uiwang, KR:Acorn, 2011.

[4] J. S. Park, M. H. Park, and S. H. Jung, "A Whitelist-Based Scheme for Detecting and Preventing Unauthorized AP Access Using Mobile Device," *Journal of the Korea information and communications society*, vol. 38, no. 8, pp. 632-640, Aug. 2013.

[5] Internet Policy Department of Legal Analysis Team, "Study on WLAN security legislation overseas," KISA: KR, Technical Report KISA-WP-2010-0003, 2010.

[6] H. S. Seo, H. W. Kim, and W. Y. Ahn, "Monitoring system for packet analysis on Wi-Fi environment," *Journal of the Korean society for computer information*, vol. 16, no. 12, pp. 227-234, Dec. 2011.

김한길(Han-Kil Kim)

2002년 한밭대학교 전자공학과(공학사)
2011년 한밭대학교 전자공학과(공학석사)
2012년 ~ 현재 배재대학교 컴퓨터공학과 박사과정
2005년 ~ 현재 한국영상대학 음향제작과 교수
※관심분야 : 멀티미디어정보처리, XML, Web Services, USN, Android

김수진(Su-Jin Kim)

1994년 계명대학교 전산학과(공학사)
1996년 계명대학교 전산학과(공학석사)
2012 ~ 현재 (주)유비테크 부설연구소 팀장
※관심분야 : 정보보호(ISMS, PIMS, ISO27001), 보안관제, 취약점분석, 모바일네트워크 보안, 디지털 포렌식

이환규(Hwan-Gyu Yi)

2012년 한밭대학교 컴퓨터공학과(공학사)
2012년 ~ 현재 (주)유비테크 부설연구소 연구원
※관심분야 : Web Service, Smart Home, 무선보안

정회경(Hoe-Kyung Jung)

1985년 광운대학교 컴퓨터공학과(공학사)
1987년 광운대학교 컴퓨터공학과(공학석사)
1993년 광운대학교 컴퓨터공학과(공학박사)
1994년 ~ 현재 배재대학교 컴퓨터공학과 교수
※관심분야 : 멀티미디어 문서정보처리, XML, SVG, Web Services, Semantic Web, MPEG-21, Ubiquitous Computing, USN