인증 네트워크 상의 비 인가된 모바일 AP 탐지 및 차단 기법★

임재완* · 장종덕** · 윤창표* · 유황빈*

요 약

현재 무선 이동 통신 기술은 빠른 속도로 발전되고 있으며 새로운 기술의 출현과 함께 빠르게 진화되고 있다. 이러한 발전을 기반으로 스마트폰의 이용자는 빠르게 늘어나고 있고 스마트 폰의 대중화에 따라 무선 네트워크의 사용은 쉽고 편리해졌다. 그러나 보안적인 관점에서 무선은 유선 네트워크에 비해 취약한 상태이며 본 논문에서 스마트폰을 활용한 모바일 AP 기술의 보안 취약점을 지적하였다. 즉, 사내 보안 기능을 갖춘 기업 망을 우회하여 기업 내의 정보를 외부로 유출하는 등의 기술로 악용 될 수 있다는 것이다. 이에 본 논문에서는 인증 네트워크 내에서 스마트 폰을 이용한 비인가 AP(Access Point)의 탐지 및 차단하는 기법에 대해 제안한다. 비 인가된 모바일 AP의 탐지는 리눅스 환경에서 개발한 탐지 프로그램을 사용하였으며 무선 센서를 통해 비 인가된 모바일 AP의 무선 패킷을 분석하였다. 또한 무선 센서를 통해 탐지된 비인가 모바일 AP는 무선 패킷에 정보를 분석하여 본 논문에서 제안하는 차단 기법을 통해 차단하였다.

Mobile Malicious AP Detection and Cut-off Mechanism based in Authentication Network

Jae-wan Lim* · Jong-deok Jang** · Chang-pyo Yoon* · Hwang-bin Ryu*

ABSTRACT

Owing to the development of wireless infrastructure and mobile communication technology, There is growing interest in smart phone using it. The resulting popularity of smart phone has increased the Mobile Malicious AP-related security threat and the access to the wireless AP(Access Point) using Wi-Fi. mobile AP mechanism is the use of a mobile device with Internet access such as 3G cellular service to serve as an Internet gateway or access point for other devices. Within the enterprise, the use of mobile AP mechanism made corporate information management difficult owing to use wireless system that is impossible to wire packet monitoring. In this thesis, we propose mobile AP mechanism-based mobile malicious AP detection and prevention mechanism in radius authentication server network. Detection approach detects mobile AP mechanism-based mobile malicious AP by sniffing the beacon frame and analyzing the difference between an authorized AP and a mobile AP mechanism-based mobile malicious AP detection.

Key words : Mobile Malicious AP, Authentication Network, Detection

접수일(2012년 2월 29일), 수정일(1차: 2012년 3월 15일), 게재확정일(2012년 3월 19일)

★ 본 논문은 2011년도 광운대학교 연구년에 의하여 연구되었음.

* 광운대학교 컴퓨터과학과

** 광운대학교 임베디드소프트웨어학과

1. 서 론

무선 네트워크는 빠른 기술 진화를 바탕으로 급속하게 유선 네트워크를 대체하고 있다. 무선 기술은 유선에 비해 많은 편의성을 제공하지만 유선 네트워크에 비해 보안이 취약하다는 문제가 있다. 그 중 스마트폰을 활용하여 모바일 AP로 활용하는 것은 기업 내부 네트워크에서 심각한 보안 문제를 발생시키는데 비인가 모바일 AP를 악의적인 목적으로 사용 할 경우에 이를 차단하기가 어렵다. 무선 AP에 대한 접근은 스마트폰의 이용자가 많아짐에 따라서 비인가 사용자의 접근이 용이해지고 있다. 이에 기업 네트워크의 관리자는 비인가 사용자의 접근 차단을 대비해야 하며 비인가 모바일 AP를 이용한 기업 내부 정보 유출에 대해서도 사전에 차단 할 수 있는 조치가 필요하다. 본 논문에서 보안 취약점을 발생시키는 비인가 모바일 AP는 일반적으로 기업 내부 네트워크에서 불법적인 접근을 통한 정보 유출을 목적으로 한다[1, 2, 3].

스마트 폰을 모바일 AP로 사용 가능하게 하는 모바일 AP 기술은 스마트폰을 AP나 모뎀으로 활용하여 단말기에 연결한 후 3G 이동 통신망으로 인터넷을 연결하게 하는 기술이다. 모바일 AP는 3G 통신망을 이용하여 정보를 유출하므로 일반적인 유무선 패킷 모니터링을 통한 탐지가 어렵다. 또한 기업이 보유한 기존 보안 시스템으로는 차단을 하기가 쉽지 않다. 따라서 모바일 AP를 통한 비 인가된 모바일 AP를 탐지하고 차단할 수 있는 대처 방안이 요구된다.[4]

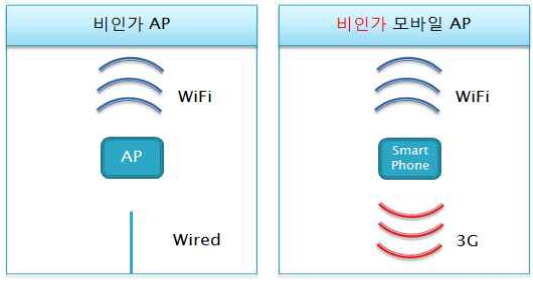
본 논문에서는 기업 망 내의 AP에 직접적인 사용자 인증방식을 모니터링하여 인가된 정상적 AP와 비 인가된 모바일 AP를 식별한다. 또한 무선 센서를 통해 비컨 프레임 스니핑(Beacon Frame Sniffing)을 분석하여 모바일 AP 기술을 활용한 비인가 모바일 AP를 탐지하고 차단하는 기법에 대해 제안한다.

2. 비인가 AP와 무선 랜 표준

본 장에서는 비인가 AP 탐지를 진행한 기존 연구들에 대해서 알아보고 비인가 AP와 모바일 AP 기술 그리고 무선 랜 보안에 대해서 알아본다.

2.1 비인가 AP

악의적 목적을 가진 비인가 AP는 기업 보안 정책에 위배되는 AP를 말한다. 비인가 AP의 정보 유출 유형은 크게 두 가지로 분류할 수 있다. 첫 번째는 일반적인 AP보다 강한 무선 신호를 이용하여 개인 단말기로 접속을 유도하고 개인 정보를 가로챈 이후에 인가된 단말기로 위장하는 공격 형태이다. 두 번째는 내부 네트워크의 접근이 가능한 공격자가 비인가 AP를 설치하여 기업 내부 네트워크에 접근 가능한 백도어(back door)를 생성하는 공격 형태이다. 비인가 AP의 차단을 위해서는 스위치 장비에 802.1x 인증을 적용한 AP 인증 방식이 있다. 차단 방법에는 여러 가지가 존재하지만 가장 확실한 차단을 위해서는 관리자가 무선 패킷 분석기를 이용한 물리적인 차단이 필요하다[3].



(그림 1) 비인가 모바일 AP의 차이점

2.2 모바일 AP 기술

모바일 AP 기술은 스마트폰을 모뎀이나 AP로 활용하여 3G 이동 통신망을 통해 인터넷을 사용 가능하게 하는 기술이다. 모바일 AP 기술은 본래 3G 이동 통신망 사용 이전부터 존재하였지만 빨라진 통신망의 지원과 과거에 비해 저렴해진 비용으로 무선 데이터 통신이 가능한 현재에 더 부각되고 있다. 또한 모바일 AP 기술은 3G 이동 통신망을 이용하고 와이브로(Wibro)와 와이파이(Wi-Fi)에 비해 속도가 느리지만 스마트폰이 수신되는 모든 지역에서 인터넷을 사용할 수 있게 해주는 매우 유용한 기술이다. 단말기와 휴대전화를 연결하는 방식은 USB(Universal Serial Bus), 블루투스(Bluetooth), 와이파이 방식을 이용할 수 있는데 본 논문에서는 와이파이 방식을 사용한다.

모바일 AP 기술은 매우 유용한 기술이지만 악용하

여 기업 내에서 비인가 모바일 AP로 사용한다면 보안에 문제가 되는데 3G 이동 통신망을 이용하기에 보통의 기업 보안 장비로는 탐지가 어려우므로 기업 정보 유출의 통로가 될 수 있다[4].

(그림 2) 모바일 AP 기술의 종류

2.3 무선 랜 표준

802.11i는 기존의 무선 랜 보안 기술을 보완하기 위한 암호 알고리즘, 사용자 인증방식, 키 교환 방식을 정의한 무선 보안 표준이다. 단말기와 AP간의 무선 링크계층 암호화를 위하여 WEP(Wired Equivalent Privacy) 방식을 사용한다. 그러나 일부 공격에 대한 취약점이 존재하여 개량된 TKIP(Temporal Key Intergrity Protocol)방식, CCMP(Counter mode with CBC-MAC Protocol)방식, EAP(Extensible Authentication Protocol) 암호 방식, EAP 인증 절차나 사전 공유키(Pre Shared Key)와 같은 상호 인증 절차가 제안되었고, IEEE 802.11i 표준에서 이것을 규정한다[5].

2.4 비인가 AP 탐지 및 대응 연구

비인가 AP 탐지에 대한 기존 연구는 크게 무선, 유선, 유무선 접근방식으로 분류된다. 먼저 무선 방식은 무선 패킷 분석 툴을 이용한 센서를 가지고 건물을 이동하며 탐지하는 방법이다. 센서를 통한 무선 패킷에 대한 탐지가 가능하지만 관리자가 직접 모니터링을 하여 이동하며 진행하는 방식으로 탐지까지 소요시간이 많이 걸리고 제한된 탐지 범위와 별도의 장비가 필요한 단점을 가지고 있다.

유선 방식은 유선 트래픽을 이용하므로 직접적인 탐지 작업이 필요 없고 기존의 탐지 도구를 활용할 수 있다. 분석 방법에 따라서 다양한 방법이 존재하지만 결정적으로 유선 상의 트래픽을 대상으로 하기 때문에 무선을 이용하는 비인가 모바일 AP에 적용 시킬 수 없다.

마지막으로 유무선 접근방식은 무선과 유선을 함께 병행하는데 탐지를 위해서 무선 센서를 이용하고 탐지된 비인가 AP 차단을 위해서 유선 방식인 중앙 관리 센터를 이용한다. 유무선 방식의 사용은 무선과 유선 접근 방식의 장단점을 모두 가지지만 일반 비인가 AP가 탐지 대상이므로 모바일 AP 기술 기반의 비인가 모바일 AP는 탐지 할 수 없다[6].

3. 비인가 모바일 AP 탐지 및 차단

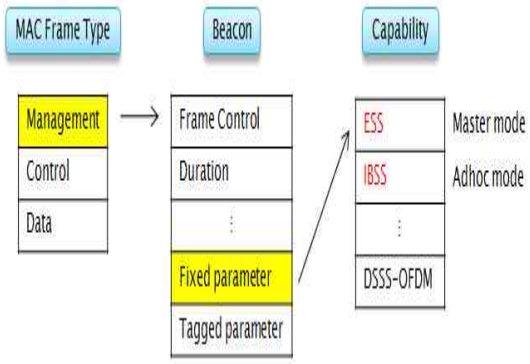
본 논문에서 제안하는 무선 접근방식을 이용한 탐지를 위해서 비인가 모바일 AP에 대한 기술적인 분석이 요구된다.

3.1 비인가 모바일 AP 분석

본 논문의 제안 기법은 무선 패킷 분석 툴을 이용하여 비인가 모바일 AP에 관련 무선 패킷을 스니핑하여 분석한다. 이를 위해 대부분의 스마트폰에 사용되는 OS에서 와이파이 연결로 모바일 AP를 설정하고 패킷을 분석하였다. 와이파이로 연결한 모바일 AP 기술 설정 방법은 OS의 root권한을 얻는 과정이 필요한데 이는 스마트 폰의 무선 랜 모드를 마스터(Master) 모드나 애드혹(Ad-hoc) 모드로 변경하여 무선 패킷을 분석하기 위해서이다.

3.2 탐지 방법

비인가 모바일 AP탐지 방법은 스마트 폰 각 OS에서 설정된 세팅에 따라 애드혹 모드와 마스터 모드로 구분된다. 애드혹 모드는 AP 설치 없이 단말기 간에 일대일 통신이 이뤄지는 방식인데 기업 내에서는 애드혹 사용이 비인가 모바일 AP로 간주된다. 애드혹 모드의 탐지는 무선 네트워크에 브로드 캐스트 되는 비컨 프레임 정보를 이용한 분석을 통해서 가능하다.

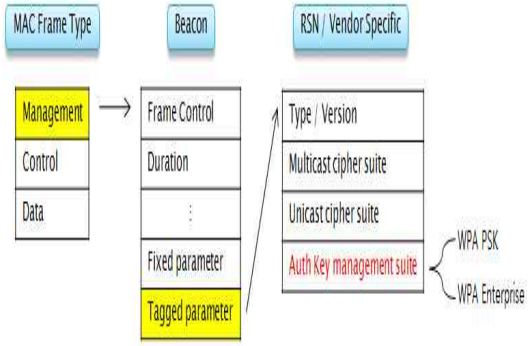


(그림 3) Ad-hoc mode

(그림 3)과 같이 비컨 프레임은 자신의 정보를 담아서 주기적으로 브로드캐스트 하는 프레임으로서 Frame Control. Duration, Address, Sequence Control, Frame Body, FCS(Frame Check Sequence)로 구성된다. 그 중 Frame Body는 Fixed Parameter와 Tagged Parameter로 이루어지며, Fixed Parameter는 Time Stamp, Beacon Interval, Capability와 같은 고정된 정보를 담고 있다. 그 중 Capability 속성에는 ESS(Extended Service Set)와 IBSS(Independent Basic Service Set) 플래그가 존재하는데 이 정보를 이용하여 해당 AP가 애드혹 모드로 동작 중인지 혹은 마스터 모드로 동작 중인지를 확인 할 수 있다[6].

마스터 모드는 일반적인 AP가 동작하는 방식이며, 인프라스트럭처 모드(infrastructure mode)라고도 하는데 마스트 모드로 동작하는 모바일 AP 기술 기반의 비인가 모바일 AP와 일반적인 AP의 구분하기는 어렵다. 따라서 본 논문에서는 AP와 단말기 간의 사용자 인증 방식의 차이점을 이용하여 마스터 모드로 동작하는 비인가 모바일 AP를 탐지한다. 마스터 모드에서 비인가 모바일 AP 탐지 방법은 애드혹 모드의 탐지 방법과 마찬가지로 비컨프레임을 스니핑 하는 방법을 사용한다. (그림 4)과 같이 Frame Body는 Fixed Parameter와 Tagged Parameter이며, Tagged Parameter는 SSID(Service Set Identifier) Parameter Set, Supported Rates, DS Parameter Set, Extended Supported Rates 등의 정보를 담고 있다.

그 중 RSN(Robust Security Network) Information과 Vendor Specific에는 해당 무선 AP가 지원하는 암호화 방식과 사용자 인증방식에 대한 정보가 담겨 있다. 특히, Auth Key Management Suite에는 현재 동작하고 있는 AP의 사용자 인증방식이 WPA-PSK (Wi-Fi Protected Access-Pre Shared Key)인지 WPA-Enterprise 인지를 확인 할 수 있는 정보가 들어있다[6]. 탐지 대상이 되는 AP의 사용자 인증방식을 확인하여 WPA-Enterprise 방식의 인증을 따르지 않고 사전 공유키 방식의 WPA-PSK 방식을 따른다면 비인가 모바일 AP로 판단하고 해당 AP를 탐지한다.



(그림 4) Master mode

3.3 차단 방법

탐지된 비인가 모바일 AP 차단을 위해서 탐지 방법과 동일하게 무선 패킷 정보를 활용한다. 그러나 무선 패킷을 분석한 결과는 비인가 모바일 AP와 일반적인 AP를 구별할 수 있는 특별한 차이점이 발견되지 않았다. 때문에 패킷 정보를 이용하여 구분하는 방법을 적용하기가 어려웠지만 기업 내부 네트워크에서 인가되지 않은 일반적인 AP도 비인가 AP로 간주되므로 차단 대상에 포함 시켜야 한다고 판단된다. 기본적으로 단말기와 일반적인 AP가 연결되는 과정은 탐색, 인증, 결합 과정으로 구분 지을 수 있다. 이 과정을 이용한 무선 센서를 통해 직접적인 방법으로 비인가 모바일 AP를 차단한다. 비컨 프레임 또는 프로브 메시지(probe message)를 이용해 주변 AP를 찾는 탐색 과정을 거치고 암호화 방식을 선택하는 과정을 통해 인증 과정이 진행되며 마지막으로 단말기와 AP 간 식별 가능한 연결 설정을 거쳐 결합 과정이 완료된 단말기가 네트워크 통신에 참여할 수 있다. 차단 방법은 이 과정에서 해킹 기법 중 DOS(denial of service)공격을 무선 센서

를 통해 사용하여 단말기의 연결을 차단하고 해당 비인가 모바일 AP에 인증을 요구하는 과정을 반복하여 과부하를 유발시켜 연결 불가능한 상태로 만든다. 이 차단 방법은 지속적으로 반복하게 되면 공격 대상이 되는 비인가 모바일 AP는 제 기능을 사용하지 못할 뿐만 아니라 하드웨어적인 작동 불능 상태로도 발전할 수 있다.

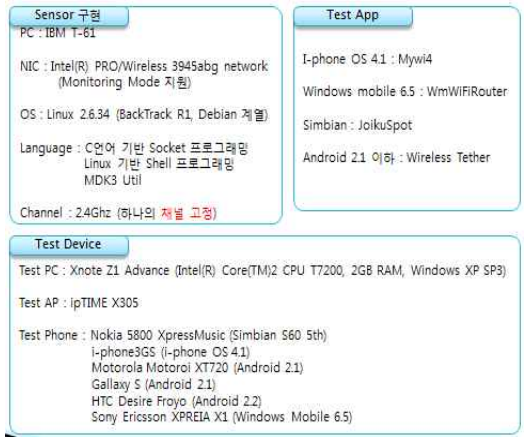
(그림 5) 차단 방법

4. 실 험

본 논문에서 제안한 비인가 모바일 AP 탐지와 차단에 대해서 검증하기 위해 실험 방법과 결과에 대해서 설명한다.

4.1 실험 환경

실험 환경을 구축하기 위해 무선 센서 구현 환경, 비인가 모바일 AP 테스트 프로그램 환경, 비인가 모바일 AP 테스트 장비 환경, 프레임 오류율로 나눠진다. 먼저 무선 센서로 사용하기 위해 IBM T계열 노트북을 사용하였고 운영체제로는 무선 해킹을 위해서 리눅스 계열인 BackTrack R1 버전이 사용되었다. 무선 패킷을 스니핑하기 위해서는 모니터링 모드가 지원되는 랜 카드가 필요한데 실험에서는 Intel 사의 PRO/Wireless 3945abg 모델이 사용되었다. 프로그램의 구현은 C언어로 작성된 소켓 프로그램이 사용되었고 무선 패킷의 스니핑과 DoS 공격에 활용된다. 무선 패킷의 스니핑을 위해서 무선 채널은 편의상 한 개의 채널로 사용되었다. 모바일 AP 기술 설정을 하기 위해 실험에서 사용된 스마트 폰인 삼성 Galaxy S 모델은 관리자 모드를 사용하기 위한 루팅이나 별도의 어플리케이션 지원 없이 와이파이 모바일 AP 기술을 이용한 모바일 AP 설정이 가능하다.



(그림 6) 실험 환경

4.2 실험 방법

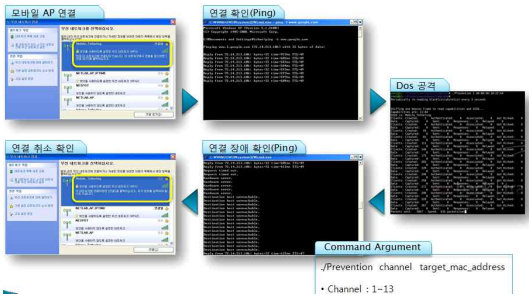
실험방법은 탐지 방법에 대한 실험과 차단 방법에 대한 실험 그리고 차단 방법에서 사용된 DoS 공격 진행 시 무선 네트워크 트래픽에 대해서 영향을 미치는 실험으로 진행된다.

탐지 방법의 실험 과정은 공격 대상이 될 비인가 모바일 AP를 실행시키고 무선 센서의 탐지 프로그램에 인자 값을 입력하여 실행한다. 마지막으로 해당 모바일 AP 탐지 여부를 확인한다. 차단 방법의 실험 과정은 탐지 방법과 동일하게 비인가 모바일 AP를 실행시키고 실험 PC와 모바일 AP를 연결한다. 그 다음 ping 테스트를 하여 연결 상태를 확인한다. 그리고 구현한 차단 프로그램을 이용하여 DoS 공격 실행한다. 마찬가지로 ping 테스트를 하여 비인가 모바일 AP와 실험 PC의 연결 해제 상태를 확인한다. 마지막으로 DoS 공격을 진행 중인 상태에서 실험 PC를 이용하여 비인가 모바일 AP와 연결 가능 여부를 확인한다.

4.3 실험 결과

실험 방법에서 설정한 진행과정에 따른 결과는 애드혹 모드와 마스터 모드의 구분 없이 탐지와 차단이 되는 것을 확인 할 수 있었다. 차단 방법으로 제안한 무선 센서에서 발생되는 DoS 공격은 탐지 대상이 되

는 비인가 모바일 AP를 지속적으로 공격하여 정상적인 연결이 이뤄지지 않았다. 또한 차단되는 과정에서 발생되는 무선 트래픽에 미치는 영향을 프레임 오류률과 실험이 반복된 순서로 측정한 결과는 공격 횟수에 비해서 높지 않은 수치를 나타냈다. 이러한 결과는 공격대상이 되는 비인가 모바일 AP를 일대일 방식으로 무선 센서에서 차단하기 때문이라고 판단된다.



(그림 7) 실험 결과

5. 결론 및 향후 연구방향

본 논문을 통해서 비 인가된 모바일 AP를 악용할 경우 손쉽게 기업 정보 유출이 가능하다는 것을 확인할 수 있었다. 이 문제에 대해서 제안한 방법으로 비인가된 모바일 AP도 일반적인 AP와 함께 무선 패킷 정보를 활용한다면 차단이 가능하다. 무선 패킷 정보를 이용하는 것은 탐지와 차단이 가능하고 차단되는 과정에서 해당 네트워크 트래픽에 미치는 영향은 작았다. 그러나 효율적인 차단 방법은 트래픽 영향력을 고려해야 하므로 향후 연구에서는 네트워크 트래픽을 최소화한 차단 방법이 필요하다. 또한 차단 방법에서 DoS 공격 방법이 아닌 위치 정보를 이용한 개선된 차단 기법에 대한 연구가 진행되어야 한다.

참고문헌

[1] Joshua Burke, Brad Hartselle, Brad Kneuven and BradleyMorgan, “Wireless Security Attacks and Defense”, WindowSecurity, 2006.

[2]Raheem Beyah, Shantanu Kangude, George Yu, Brian Strickland, and john Copeland, "Rogue Access Point Detection using Temporal Traffic Characteristics", IEEE Communications Society Globecom, 2004.

[3] Sachin Shetty, Min Song and Liran Ma "Rogue Access Point Detection by Analyzing Network Traffic Characteristics", IEEE Communications Society Globecom, 2007.

[4] Beyah R, Venkataraman A, "Rogue-Access-Point Detection", IEEE Security and Privacy Magazine, 2011.

[5] Namedurali E, Qaddour J, Doss D, "Wireless LAN: Security Problems, Solutions & Challenges", World Wireless Congress, 2004.

[6] Shital V Jagtap and K N Honwadkar, "Rogue Access Point Detection in WLAN by Analyzing Network Traffic and Behavior", International Journal of Computer Applications Volume 1 – No. 22, 2010.

[저 자 소 개]

임 재 완 (Jae-wan Lim)

2003년 호서전산전문학교
정보처리학과 (이학사)
2011년~ 현재 광운대학교
컴퓨터과학과
(공학석사 재학중)

e-mail : ljfurcal@kw.ac.kr

장 종 덕 (Jong-deok Jang)

2009년 단국대학교 컴퓨터과학과
(공학사)
2011년 광운대학교
임베디드컴퓨터소프트웨어학과
(공학석사)

e-mail : xelaga@nate.com

윤 창 표 (Chang-pyo Yoon)

1998년 광운대학교 전자계산학과
(공학사)
2001년 광운대학교 컴퓨터과학과
(공학석사)
2009년~ 현재 광운대학교 컴퓨터과
학과(공학박사 재학중)

e-mail : cpyoon@kw.ac.kr

유 황 빈 (Hwang-bin Ryu)

1975년 인하대학교 전자공학과
(공학사)
1977년 연세대학교 대학원
(공학석사)
1989년 경희대학교 대학원
(공학박사)
1981년 ~ 현재 광운대학교 컴퓨터소
프트웨어학과 교수

e-mail : ryou@kw.ac.kr