한국산학기술학회논문지
Vol. 9, No. 4, pp. 952-957, 2008

PDA기반 무선 AP의 위치 탐색 시스템 구현

박주평[1], 홍진근[1*], 한군희[1], 김기홍[2]

Implementation of Location Tracking System of Wireless Access Point based PDA

Ju-Pyung Park[1], Jin-Keun Hong[1*], Kun-Hee Han[1] and Ki-Hong Kim[2]

요 약 최근 무선 통신 기술의 발달은 장비를 간편화 하고 편리화 시키게 되었다. 또한 다양한 서비스를 창출 할 수 있는 기반이 마련하였다. 하지만 무선 랜의 다양한 서비스와 접속성의 확대는 보안의 취약점을 야기 시켰다. 본 논문에서는 IEEE802.11 무선 랜 서비스를 통하여 PDA 상에서 AP의 정보를 받아 무선 랜 보안 서비스의 특성과 취약성을 살펴보고 PDA 기반 위치 추적 시스템을 구현을 하였다.

Abstract In this paper, explain about collect that Access Point signal and Implementation of Location Tracking System of Wireless Access Point based PDA. Collect Access point signal in PDA then Signal transmits by computer so Computer is analyze collected signal and is seen on picture. we show the Present problem of wireless LAN and position feeler algorithm through this writing paper.

Key Words : PDA wardriving, Access Point

1. 서론

기술의 발달과 인간의 편리함에 대한 욕구가 충족되어 장비는 간소화 되었으며 하나의 장비는 다양한 서비스를 창출 하였다[1]. 또한 주변의 많은 장비들을 제어하기 위해 네트워크가 발달 되었다. 하지만 다양한 장비들의 네트워크 구성에 있어 유선은 많은 제약 사항이 뒤따른다. 해결책으로 제시된 무선 랜은 유선의 제약 사항을 보안하고 많은 서비스를 지원 할 수 있는 기반을 마련하였다. 기존연구에 따르면 무선 랜의 접근성 및 편리성 확대는 보안위협에 대한 큰 취약점을 가진다[2-3]. 무선랜 접속 시 무선으로 클라이언트(사무실 노트북)에 직접 접근 가능하므로 기존 방화벽, IDS, IPS 심지어 메일 필터와 웹 필터 같은 콘텐츠 보안 솔루션들까지 모든 보안 솔루션을 우회할 수 있다.

또한 침입 경로를 남기지 않는다. 유선으로 내부에 침입하게 되면 시스템에 모든 로그를 지운다고 하더라도 라우터, 스위치 등 지나가는 경로마다 어디를 통해서 침입했는지를 남기게 되는데, 무선을 이용하면 시스템에 직접 접근하므로 이를 최소화하거나 남기지 않을 수 있다. 다음으로 무선 랜에 접속하여 해킹한다면 공격자는 자신의 물리적 위치를 숨길 수 있다. 공격자가 해킹 도중 역추적을 당하더라도 최종 위치는 공격자가 접속해 있는 AP의 위치까지만 알 수 있다. 따라서 공격자가 워 드라이빙(War-driving: 드라이빙을 하면서 무선 랜 접속을 시도함)을 통해 AP를 옮겨 다니며 해킹을 하게 되면 역추적은 현실적으로 어렵다고 할 수 있다. 마지막으로 취약한 많은 무선 랜 기반들을 들 수 있다. 네스팟, 애니웨이와 같은 무선 랜을 이용한 공중망

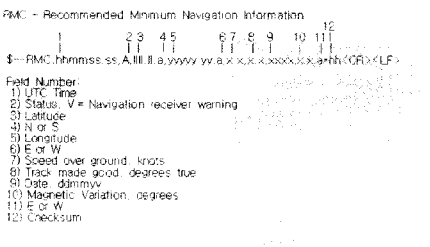
서비스부터 유무선 공유기에 이르기까지 수많은 무선 랜 기반들이 존재하고 이들 대부분이 보안에 취약하다. 2006년 4월에 실시한 무선랜 보안 실태 조사 결과에 따르면 조사 대상 4천여 클라이언트와 500여 AP 중 안전한 64%가 전혀 보안이 되어 있지 않는 오픈 시스템이 있었고, 34%는 크래킹(Cracking)이 가능한 WEP를 사용하고 있다. 그리고 단 2% 만이 안전한 802.1x나 WPA를 쓰고 있는 것으로 나타났다[4]. 본 논문에서는 무선 랜의 취약성을 파악하고자 간편하게 PDA 상에서 AP 정보를 파악

[1]백석대학교 정보통신학부
[2]ETRI 부설연구소
*교신저자: 홍진근(jkhong@bu.ac.kr)
접수일 008년 7월 7일 수정일 08년 8월 05일 게재확정일 08년 8월 11일

할 수 있도록 하고 보안 상태를 점검 하고자 한다. 또한 PDA에서 수집한 내용을 참고로 컴퓨터 맵 상에 AP 위치를 도식하고 보안 파악 및 현 실태 조사를 하고자 시스템을 설계 및 구현하였다. 본 논문의 구성은 다음과 같이 구성된다. II장에서는 위치탐지 기술 및 특징을 기술하며, III장에서는 위치 탐지 시스템의 기술적 사항을 소개하였다. 그리고 IV장에서 결론으로 맺었다.

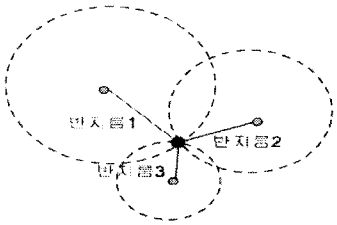
2. 위치탐지 기술 및 특징

본 논문에서 제안된 알고리즘에서는 AP 위치를 추측할 때 측정자의 위치와 AP 와의 거리를 통하여 AP의 위치를 추론 하였다[5]. AP의 위치를 추적하기 위해서는 우선 측정자의 정확한 위치 정보가 필요하다. 이는 GPS 수신기를 통하여 좌표를 PDA로 가져옴으로서 측정자의 위치를 파악할 수 있다. GPS 정보에는 다양한 정보를 포함하고 있다. 하지만 본 프로그램 에서는 RMC 데이터를 통해 위치 정보를 얻고자 한다. <그림1>에서 본 프로그램에서 사용된 GPS의 RMC 데이터 구조를 나타내고 있다.



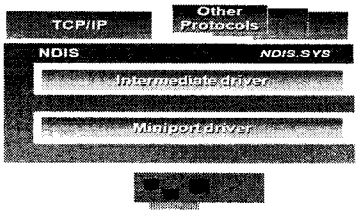
[그림 1] RMC 데이터 구조

자신의 위치를 측정 후 AP 위치를 추론하기 위해서 위치탐지 방법 RSSI 방식을 채택 하였다. 대표적 위치 탐지 방법으로 ToA, TDoA, AoA, RSSI 방식이 있지만 모든 AP 에 호환되며 부과적인 센서 없이 간편하게 AP 위치를 탐지하는 방식으로 RSSI 방식이 가장 부합 된다고 생각한다. RSSI(Received Signal Strength Indicator)는 신호를 수신하는 측에서 신호의 세기를 통계적인 방법에 근거하여 확률분포와 대조하여 위치를 측정하는 방법이다. RSSI 방식을 이용하기 위해서는 우선적으로 미리 정의된 다양한 지점에서의 신호 세기들을 RSSI 표본 수집을 통해 측정하여야 한다. 이러한 과정을 수행하고 나면 타깃의 송신 신호를 수신할 때 발생하는 신호의 감쇠 정도를 측정한 뒤 미리 수집되었던 RSSI 표본과 매핑 하여 타깃의 위치를 측정한다. 하지만 이 방식은 타깃과 센서 사이에 많은 장애물이 존재하거나 복잡한 환경일 경우 거리 측정 오차가 매우 클 수 있다는 단점이 있다. <그림 1>에서는 RSSI 방식을 참고하여 3 개의 기준점에서의 신호 측정[반지름1,반지름2,반지름3]에 의해 AP 위치 측정 방식을 보여주고 있다.



[그림 2] 신호 측정에 의한 2 차원 위치 검출

상기 RSSI 방식을 사용함에 있어 PDA 는 AP가 보내는 신호의 감쇠 정도를 파악하여 측정 위치로부터 거리를 구한다. 또한 측정 AP의 정보를 획득하여 상이한 AP 간의 구분을 짓는다. AP 정보를 획득 방식은 PDA에서 랜카드를 제어하여 랜카드로부터 AP정보테이블을 획득한다. 네트워크카드를 제어하기 위해 NDIS 드라이버를 사용하였다. NDIS란 driver 계층의 중간적인 위치에서 <그림 3>에서와 같이 아래에 있는 miniport driver와 위에 있는 protocols driver 와 통신을 가능케 하는 매개체 이다. PDA 프로그램에서는 NDIS를 통해 네트워크 카드로부터 무선 랜 정보를 획득 후 GPS 정보와 혼합하여 AP의 전반적 정보를 파악할 수 있는 데이터를 만든다.



[그림 3] Intermediate NDIS Drivers

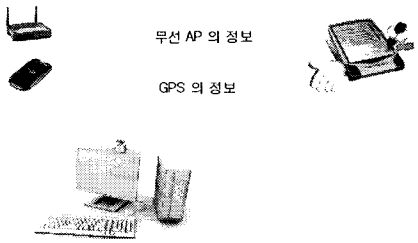
PDA에서 만들어진 정보는 Computer로 보내져 Computer 는 AP의 위치 추적 및 AP 정보를 사용자에게 보기 쉽도록 표현해 준다.

3. 위치 탐지 시스템

3.1 전체적 시스템 구성

PDA상에서 AP에 대한 전반적인 정보 수집이 이루어

진다. 사용자는 PDA를 이용하여 비교적 작은 범위의 지역을 순찰하면서 AP의 상태 파악 및 불법 AP를 탐지할 수 있다. PDA를 통하여 탐지된 전반적인 정보 데이터는 Computer로 옮겨져 맵에 도식화 하고 사용자에게 정보를 보기 편하도록 편리성을 제공해준다. <그림 4>에서 위치 탐지를 위한 시스템 구성도를 제시하였다.



[그림 4] 시스템 구성도

3.2 시험환경

본 실험은 GPS 장비와 PDA, Computer로 구성되어졌다. <표 1>는 본 실험의 PDA 환경을 나타낸다.

[표 1] PDA 실험 환경

OS	windows Movile(TM) 2003 Second Edition 버전 : 4.21.1088(빌드 14235.2.0.0)
Device	제조사 : Acer Incorporated 제품명 : Acer n50 handheld CPU : intel(R) PXA272 (312 MHz) bluetooth 및 WLAN 지원 Royaltek 미니블루 GPS
Language	Visual C++ 2005 (MFC)

<표 2>은 본 실험의 Computer의 환경을 나타낸다.

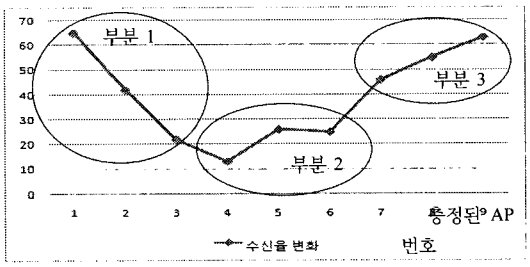
[표 2] Computer 실험 환경

OS	Window XP Service Pack 2
Device	제조사 : 삼보 제품명 : Dreamsys CPU : intel(R) Core(TM)2 1.86GHz RAM :1.97GB
Language	Visual C++ 2005 (MFC)

위치 계산함에 있어 인공물 및 자연적 환경 요소는 고려하지 않았으며 저녁 시간을 이용하여 인위적 오차를 줄이도록 했다.

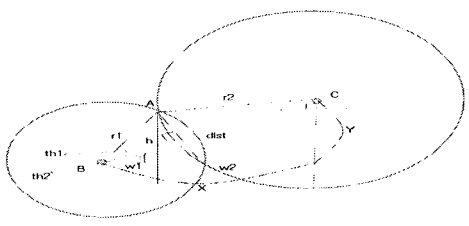
3.3 위치 추적 알고리즘

RSSI방식에 따라 AP의 위치 추정을 위해서는 측정자의 위치 정보와 각 AP 의 신호감쇠에 의한 거리가 필요하다. 본 구현된 시스템에서는 PDA에서 얻어진 축적된 데이터를 MAC 주소별로 구분을 짓는다. <그림 5>은 주기에 따라 신호를 측정한 그림이다. 가로축은 일정 주기로 체크한 AP번호를 나타내므로 시간 흐름과 동시에 이동 거리를 의미한다. 세로축은 측정된 AP의 신호 세기를 나타낸다.



[그림 5] AP 신호표

제안된 시스템에서 신호에 따른 교차점을 찾기 위하여 3개의 수신신호 세기를 추출하여 계산 하였다. 신호 선정 기준에 따라 위치 탐색에 영향을 미치게 되어 다음과 같은 3가지의 신호 선정 방안을 적용하여 실험을 해보았다. 첫 번째 방안은 분류된 AP 의 모든 정보 개수를 3등분하여 3부분으로 나누고 각 부분에서 신호가 가장 좋은 신호만을 추출 하는 방안이다. 이 방안은 넓은 범위에서의 신호가 좋은 측정 데이터를 얻어 표현 하고자 한 방안이다. 두 번째 방안은 분류된 AP 의 모든 정보 개수를 3등분 하여 나누어진 각 부분의 중간 위치의 신호를 추출 하는 방안이다. 이 방안은 신호 세기를 고려하지 않고 중간 값을 추출함으로서 물리적 위치의 평균점에서 AP 위치를 측정한다. 마지막 방안은 측정 위치와 관계없이 동일 위치가 아니면서 가장 좋은 신호 값 3개를 추출 하는 방안이다. AP위치를 측정함에 있어 간섭이 적은 신호를 추출하여 정확한 데이터를 획득하며 측정된 많은 데이터에서 일관성을 갖도록 하였다. 추출된 3개의 신호 정보는 측정자의 위치로부터 무 방향성으로 AP위치를 표현해 준다. 이는 3개의 신호정보를 취하여 AP 위치를 2차원에 표시할 수 있게 한다.



[그림 6] 위치 교점 탐색 1

<그림 6>는 신호 값을 원 의 반지름으로 표시하고 해당 원의 교차점을 통하여 AP 위치를 얻고자 한다.

위의 두 원의 교차점을 구하기 위하여 다음과 같은 식을 사용하였다.

$$(x-x_1)^2+(y-y_1)^2=r_1^2 \quad (1)$$
$$(x-x_2)^2+(y-y_2)^2=r_2^2$$
$$x=x_1+r_1\cos\theta$$
$$y=y_1+r_1\sin\theta$$

x1, y1 이 첫 번째 원의 중심좌표, x2, y2가 두 번째 원의 중심좌표 r1은 첫 번째 원의 반지름이구요, r2는 두 번째 원의 반지름 이다. 실제 구하고자하는 두 원의 교점 좌표는 x, y가 된다.

$$(x_1+r_1\cos\theta-x_2)^2+(y_1+r_1\sin\theta-y_2)^2=r_2^2 \quad (2)$$
$$X=x_2-x_1,\ Y=y_2-y_1$$
$$(r_1\cos\theta-X)^2+(r_1\sin\theta-Y)^2=r_2^2$$
$$r_1^2\cos\theta^2-2r_1X\cos\theta+X^2+r_1^2\sin\theta^2-2r_1Y\sin\theta+Y^2=r_2^2$$
$$r_1^2-r_2^2+X^2+Y^2=2r_1(X\cos\theta+Y\sin\theta)$$
$$=2r_1\sqrt{X^2+Y^2}\cos(\theta-\tan^{-1}\frac{Y}{X})$$

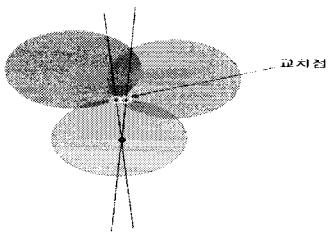
식 (1)을 이용하여 간단하게 정리하면 식(2)에서와 같이 식을 유도할 수 있다.

$$D=\sqrt{X^2+Y^2} \quad (3)$$
$$\phi=\tan^{-1}\frac{Y}{X}$$

식 (3)을 식(2) 에 대입하여 풀면 식(4)에서와 같은 식을 도출 할 수 있다

$$r_1^2-r_2^2+D^2=2r_1D\cos(\theta-\phi) \quad (4)$$
$$\theta=\phi\pm\cos^{-1}(\frac{r_1^2-r_2^2+D^2}{2r_1D})$$
$$x=x_1+r_1\cos(\phi\pm\cos^{-1}(\frac{r_1^2-r_2^2+D^2}{2r_1D}))$$
$$x=x_1+r_1\cos(\tan^{-1}\frac{Y}{X}\pm\cos^{-1}(\frac{r_1^2-r_2^2+D^2}{2r_1D}))$$
$$y=y_1+r_1\sin(\tan^{-1}\frac{Y}{X}\pm\cos^{-1}(\frac{r_1^2-r_2^2+D^2}{2r_1D}))$$

위의 도출된 식을 이용한 알고리즘을 통하여 두 신호로부터 교차점 신호를 구하고 두 개의 신호 정보로 추측된 위치 정보와 나머지 신호정보를 직선의 방정식으로 이용하여 <그림 7>과 같이 교차점을 찾아낸다.

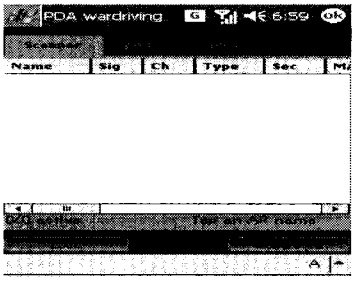


[그림 7] 위치 교점 탐색 2

두 원의 교점과 직선 방정식을 통하여 구한 나머지 원과의 교점을 비교하여 거리가 작은 교점 두 개를 추출하고 두 교점의 중간점을 구함으로서 3개의 신호의 교점을 추론할 수 있다.

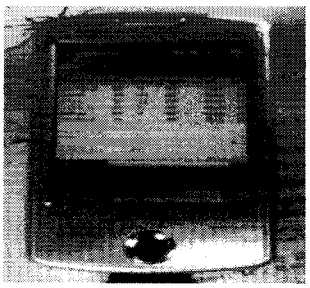
3.4 시스템 구동 및 시뮬레이션 결과 고찰

PDA 프로그램 인터페이스는 <그림 8>에서 제시하였다. 인터페이스는 Scanner, port, options 패널로 구성되고 이 가운데, Scanner 패널을 제시하였다.



[그림 8] PDA 프로그램 인터페이스

Scanner 패널에서는 AP에 대한 모든 정보를 볼 수 있으며, Scanner 패널에 담고 있는 내용은 AP의 SSID, RSSI, Channel, Infastructure, Auth, MAC 정보를 포함하고 있으며 GPS의 위, 경도 정보 AP 신호의 첫 수신 시간이 나타난다. 구현된 PDA 프로그램을 이용하여 테스트 해본 결과 <그림 9> 및 <표 3>에서와 같은 데이터를 얻을 수 있었다. AP의 정보는 실시간으로 PDA에서 표현된다.



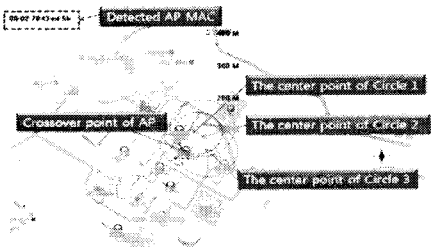
[그림 9] 시뮬레이션 결과 화면

[표 3] AP 정보 데이터 테이블

NESPOT	00-02-78-f3-xx-xx	-88	1	36503699	127111627
BonBu	00-0f-cb-98-xx-xx	-85	1	36503706	127111536
BU-Wireless	00-02-78-f3-xx-xx	-56	1	36503724	127111375
BonBu	00-0f-cb-98-xx-xx	-80	1	36503724	127111375
BU-Wireless	00-02-78-f3-xx-xx	-77	1	36503747	127111375
lab1132	00-14-bf-89-xx-xx	-60	2	36503747	127111364

얻어진 PDA의 데이터는 컴퓨터에 보내지고 컴퓨터는 PDA를 통해 얻은 정보<표 3>를 통하여 <그림 10>과 같이 나타낼 수 있다.

본 논문에서는 PDA를 활용하여 실외에서 무선 AP를 탐지하는 탐지시스템을 구현하였다. 구현을 위해 PDA 환경 인터페이스 설계, PDA와 호스트 PC간 소켓통신 인터페이스 설계, 호스트 상에서 맵 도식 인터페이스 및 GUI 설계, 구현하였다. 구현된 시스템을 활용하여 ○○ 대학 주변을 탐지한 결과, 지도에 도식된 AP 정보를 통하여 사용자는 AP의 위치를 알 수 있게 된다. 물리적 위치를 파악함으로서 보안의 위협의 요소를 파악할 수 있다. PDA를 통해서 얻은 AP 정보 테이블을 보면 대부분의 AP는 오픈되어 있어 보안 설정이 미흡한 상태로 나타났다.



[그림 10] 추적된 AP 도식

시험된 대학 주변을 탐지한 결과 80% 이상이 보안설정을 하지 않고 사용 중이였다. 그밖에 사용자들은 WEP을 설정하고 있으나 WEP 또한 안전하지 못하며, 공격가능한 WEP 크래킹 툴은 웹사이트에서 쉽게 찾아 사용할 수 있다. WEP 크랙 툴은 대부분 RC4 알고리즘의 취약점으로 인해 특정한 조건에서 암호화키를 복구할 수 있게 되어 있으며, 대표적인 프로그램에는 에어스노트(Airsnort)와 WEP 크랙이 있다. 에어스노트나 WEP 크랙을 이용하면 WEP 알고리즘으로 암호화된 데이터 트래픽을 충분히 모아서 WEP 키를 알아낼 수 있다. WEP 키를 알아내면 패킷 스니핑을 통해 데이터의 수집 및 네트워크 침투가 가능해진다. 이는 해당 네트워크상의 치명적 보안의 허점을 드러내는 것이다. 또한 침입자에게 AP의 물리적 위치를 제공함으로써 더 큰 위험에 노출된다.

4. 결론

본 논문에서는 PDA 환경에서 GPS 수신기를 제외한 무선 랜 환경에서 AP의 위치 탐지 시스템을 구현하였으며, 구현된 시스템을 적용하여 무선 랜 보안 환경을 살펴봄으로써 해킹의 위협으로부터 AP가 안전하지 못한 것을 파악할 수 있었다. 현재 무선 랜AP 탐지를 위한 프로그램에는 MiniStumbler, Retina WiFi Scanner, Wifi FoFum, Kismet (PDA style) 등이 있다 이 프로그램들은 쉽게 인터넷 상에서 구할 수 있으며 사용자들에게 AP의 정보를 제공한다. 구현된 시스템은 기존의 구현된 시스템에 비해 가벼운 wardriving 시스템을 설계 및 구현하였으며, 또한 map 과 연동하여 AP의 위치를 추적 할 수 있도록 GUI를 구성하였다. 이로 인해 AP의 정보 관리와 불법 AP 탐지추적을 효율적으로 수행 할 수 있도록 하였다.

참고문헌

[1] 김보미, 심민진, 이종은, 최상호, "정보통신전자공학부 학사과정 세계인류 IT기술16- 유비쿼터스 센서 네트워크의 위치탐지 기술 및 동향," 2007.

[2] ISO/IEC, "Wireless Lan Medium Access Control and Physical Layer Specifications," ISO/IEC 8802-11, ANSI/IEEE Std 802.11, 1999.

[3] Chris Hurley (Roamer), Russ Rogers, Frank Thornton (Thorn), "Learning to war Drive," War Driving, syngress, 2004.

[4] A.T.Rager, "WEPCrack - An 802.11 key breaker," HTTP://wepcrack.sourceforge.net

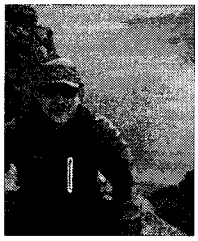
[5] 김태은, "두 원의 교점구하기," http://www. davpia.com/MAEUL/Contents/Detail.aspx?BoardID=1&&MAEULNO=8&no=1217

박 주 평(Ju-Pyung Park) [준회원]

• 2008년 8월 : 백석대학교 정보통신학부

<관심분야>
센서네트워크, 위치탐지, 리눅스 커널, NDIS, RFID, Wireless Lan

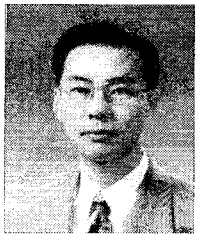
홍 진 근(Jin-Keun Hong) **[정회원]**



- 2008년 8월 현재 : 백석대학교 정보통신학부 교수

<관심분야>
전술통신, 센서넷, RFID, 무선랜 보안

한 군 희(Kun-Hee Han) **[종신회원]**



- 2008년 8월 현재 : 백석대학교 정보통신학부 교수

<관심분야>
RFID, 경영정보컨설팅

김 기 홍(Ki-Hong Kim) **[정회원]**

- 2008년 8월 현재 : 한국전자통신연구원 부설연구소 선임연구원

<관심분야>
정보보호, 음성처리