한국산학기술학회논문지
Vol. 9, No. 4, pp. 1012-1017, 2008

무선 Access Point 위치 탐지시스템의 설계 및 구현

구용기[1], 홍진근[1*], 한군희[1], 김기홍[2]

Design and Implementation of Location Detection System of Wireless Access Point

Yong-Ki Ku[1], Jin-Keun Hong[1*], Kun-Hui Han[1] and Ki-Hong Kim[2]

요 약 최근 무선통신 기술의 발달과 편리성으로 무선 랜의 활용 증가하고 있다. 이와 더불어 무선 랜의 보안 위협과 취약성에 대하여 이슈화 되고 있다. 따라서 IEEE에서는 802.11 표준안을 제정하고 무선 랜의 보안 취약점을 보완하기 위해 802.11i등 새로운 표준들을 제정하고 있지만, 아직까지 해결되지 않은 보안 위협들이 존재한다. 본 논문에서는 액세스 포인트의 비콘 프레임을 이용하여 건물 내 액세스 포인트의 보안 상태 와 비인가 액세스 포인트를 탐지하는 시스템과 RSSI, 삼각측량법 및 칼만필터 알고리즘을 사용한 위치탐지 알고리즘을 제안하고, 기존 탐지 알고리즘과 제안 알고리즘의 결과 비교로 성능을 평가하였다.

Abstract Recently, the use of wireless lan is increased by the development of wireless communication and convenience. Moreover, it makes an issue of security threat and vulnerability of wireless lan. Therefore, the IEEE established new standard such as 802.11i in 802.11 to supplement security vulnerability of wireless lan. But the security threat that does not solve, still remains. In this paper, we proposed that the location detection algorithm, that is used Kalman-Filter, Lateration and RSSI, and the mechanism that detects security status of AP and unauthorized AP by using beacon-frame of AP in building. Finally, we confirmed performance of proposed algorithm is good in comparison of established algorithm.

Key Words : Access Point, Wireless, Location Detection, Signal, Kalman-filter, locating algorithm, Wireless Lan

1. 서론

무선 랜은 무선 주파수(Radio Frequency)기술을 이용하여 유선망 없이도 데이터를 주고받을 수 있는 기능을 제공한다. 즉, 유선망의 구속됨이 없이 이더넷, 토큰링과 같은 기술의 이점과 기능을 제공한다. 무선 통신 기술의 발달과 편리성으로 인하여 기존의 유선 랜에서 무선 랜으로 변화하는 추세이다. 1990년대 초 IEEE는 여러 무선 랜 기술을 통합하여 802.11 표준을 확립하였고 데이터 전송속도, 보안, 로밍, QoS 등에 관한 기능을 개선한 새로운 802.11 계열의 표준안을 제정하고 있다.

무선 랜은 기존 유선 랜과 달리 무선 전파(RF)를 이용함으로 구축시간, 운영 경비 등의 절감 등 많은 장점을 지니지만 보안에 취약한 단점을 지니고 있다. 이러한 단점들을 보완하기 위해 IEEE에서는 802.11i 표준안을 제공하였지만 아직까지 해결되지 않은 보안 위협들이 존재한다. 무선 랜의 중요한 보안 위협은 다음과 같다. 첫째, 인가되지 않은 엑세스 포인트(합법적 사용자의 하이재킹), 둘째, 보안을 적용하지 않은 엑세스 포인트로 인하여 기업 내에 치명적 손실을 초래할 수 있다. 본 논문에서는 무선 랜 장비인 액세스 포인트와 비콘 프레임(Beaconf Frame)을 이용하여 기업 내 액세스 포인트들의 위치와 보안상태, 비인가 액세스 포인트를 탐지하여 관리할 수 있는 시스템과 알고리즘을 제안하고자 한다[1-3]. 위치탐지와 관련하여 G. P. Yost 등은 TOA 추정을 위한 개선 알고리즘을 제안한 바 있고, N. J Thomas 등은 TOA에 칼만 필터를 기반으로 하는 강인한 위치 추정 알고리즘을 제안한 바 있다. 그러나 센서를 활용한 위치 추정은

[1]백석대학교 정보통신학부
[2]ETRI 부설연구소
*교신저자: 홍진근(jkhong@bu.ac.kr)
접수일 08년 7월 6일 수정일 08년 8월 01일 게재확정일 08년 8월 11일

높은 비용이 요구되고 시스템 설계 시에 복잡도와 기술력을 요구한다. 본 논문에서 제안하는 방식은 무선 랜의 AP 기반에서 위치 탐지 알고리즘을 설계 및 구현하였다. 이 방식은 비용 측면이나 확장성 측면에서 장점을 가지고 있다. 본 논문의 구성은 2장에서 위치탐지 기술을 분석하고, 3장에서 구현된 시스템에 대해 소개하며 4장에서 실험 및 결과를 고찰한 후 5장에서 결론을 맺었다.

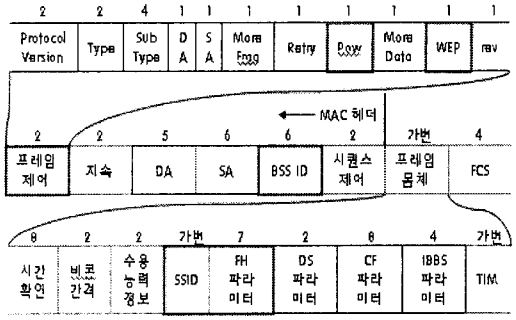
2. 위치탐지 기술 분석

대표적인 위치탐지 시스템으로 실내에서는 초음파, 적외선, 레이저 센서 등으로 분류 할 수 있다.

ToA(Time of Arrival)는 신호가 도착하는 시간을 이용하여 위치를 측정하는 알고리즘이다. 센서에서 이동 매체 사이의 거리는 신호의 종류에 따른 환경상수를 곱하여 산출할 수 있다. 산출된 거리로부터 반경 원을 그려 3원의 교점이 이동 매체의 위치가 된다[4~6]. TDoA(Time Differe- nce of Arrival)는 이동매체와 두 개 이상의 센서가 송/수신 하는 신호의 도착 시간의 차이를 측정하여 거리를 산출하는 알고리즘이다. 이동매체의 위치를 구하기 위하여 타원곡선 공식을 적용한다[6]. 해당 방식은 이동매체와 센서 간 특별한 동기화가 필요하지 않아 알고리즘 구현이 용이한 반면 신호 도달 시간을 구할 때 있어 신호 도착 시간 지연차 와 신호의 다중경로에서 최적경로 신호탐지 문제를 최소화해야 한다[6]. AoA(Angle of Arrival)는 센서에서 이동 매체가 보내오는 신호의 방위각을 이용하여 각을 측정하고 세 개의 센서로부터 산출된 방위각의 연장선의 교점으로 이동 매체의 위치를 측정하는 알고리즘이다. AoA는 이동 매체가 센서 가까이 존재하거나, 신호가 산란되는 환경에는 적용하기 부적절하다[6]. RSSI(Received Signal Strength Indicator)는 신호 손실도를 이용한 거리 측정 방법과 실내 환경에서 신호 세기들의 RSSI 표본 수집을 이용한 통계적 위치 추측 방법으로 나뉜다. 해당 방식은 실내 환경이 복잡하거나, 센서와 이동매체 사이에 많은 장애물이 존재한다면, 거리 측정 오차가 매우 클 수 있다. 삼각측량법은 거리 측정을 이용한 Lateration 방법 및 각도 측정에 기초한 Angulation 방법으로 구분된다. Lateration 방법은 3군데의 센서노드부터의 이동 매체의 거리를 측정하여 3 개의 원의 교차점으로부터 2차원에서의 이동 매체의 위치를 찾아내는 알고리즘이다. 이 알고리즘의 성능 척도는 미리 알고 있는 3개의 센서로부터 이동 매체의 거리를 측정하는 방법에 따라 결정된다. 본 논문에서는 RSSI와 칼만 필터를 이용한 환경 데이터베이스를 적용하며, 삼각측량법 중 Lateration 방법을 사용한다.

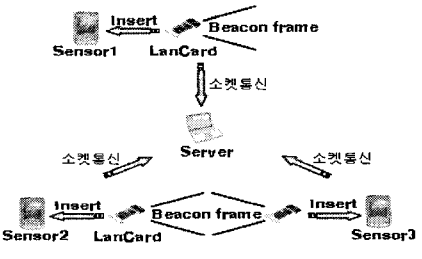
3. 제안 시스템 프레임워크

3.1 시스템 구성



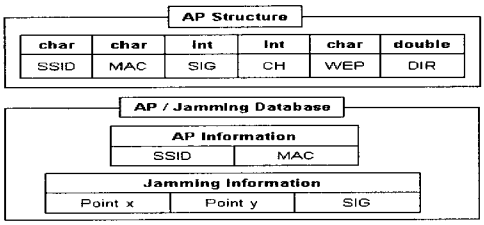
[그림 1] 비콘 프레임 구조

건물 내부에 액세스 포인트의 위치와 보안 상태 탐지를 위한 시스템은 비콘 프레임 정보를 수집하여 각 액세스 포인트의 위치 및 상태를 파악한다. [그림 1]에서 보는 바와 같이 엑세스 포인트가 주기적으로 브로드 캐스팅하는 비콘 프레임의 구조이다. 해당 프레임의 구조를 살펴보면 크게 MAC헤더, 프레임몸체, FCS로 나뉜다. 이 중 엑세스 포인트의 위치와 보안 상태를 파악하기 위해 사용되는 필드는 다음과 같다. BSSID(Basic Service Set ID- entifier)는 무선 LAN 표준인 802.11에서 기본서비스 영역(BSS)을 식별, 48bit 식별자이다. 액세스 포인트의 MAC 주소라 불리기도 한다. SSID (Service Set Identifier)는 무선 랜에서 서비스 제공자가 여러 다른 무선 셀(BSS)들을 구분하는데 사용하는 무선 단말(AP)간의 접속용 ID(식별자)이다. FH(Frequency Hopping)는 주어진 대여폭을 많은 수의 호핑채널(Hopping Channel)로 나눈다. 이는 다중 채널간의 잡음을 줄이기 위해 사용된다. 이를 통해 엑세스 포인트의 채널을 알 수 있다. WEP 해당 필드는 해당 엑세스 포인트의 암호적용 상태를 나타낸다. POW 필드는 엑세스 포인트의 전력에 관련된 정보를 담고 있다.



[그림 2] 시스템(물리적) 구성도

[그림 2]에서 보는 바와 같이 제안 시스템에서는 크게 3개의 PDA와 하나의 서버로 구성된다. 센서노드는 연결된 무선 랜카드부터 주변 액세스 포인트의 비콘 프레임을 수집하고 해당 정보를 소켓통신을 통해 서버로 전송한다. 서버는 3개의 PDA로부터 받은 정보들을 구분하여 데이터베이스와 구조체에 저장하고, 인가된 액세스 포인트인지 비인가 액세스 포인트인지를 구분한다. 비인가 액세스 포인트라면 보안 정책에 따라 로그를 남기고 관리자에게 메시지를 보내며, 인가된 액세스 포인트는 위치, 암호화상태를 파악하여 보안 정책에 맞게 로그를 남기고 메시지를 보낸다.



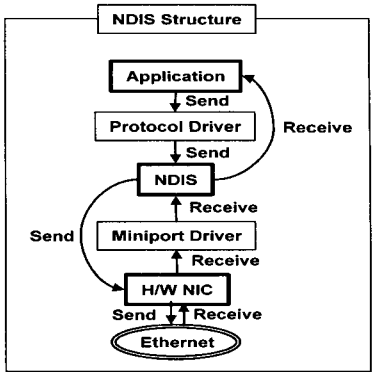
[그림 3] 구조체와 데이터베이스 구조

[그림 3]에서는 서버에서 전송받은 정보들을 관리하기 위해 사용되는 구조체와 데이터베이스 자료 구조를 나타내고 있다. 엑세스 포인트 데이터베이스는 관리자로부터 엑세스 포인트를 등록하기 위해 사용되며 등록되어진 엑세스 포인트 목록과 PDA로부터 전송받은 정보를 비교하여 비인가 엑세스 포인트인지 아닌지를 판단하게 된다. 엑세스 포인트 구조체는 전송받은 엑세스 포인트들의 위치를 맵핑하고 보안 상태를 표현하기 위하여 사용된다. Jamming Information Database는 신호세기를 기준으로 거리를 산출 할 때 위치별 환경요인을 적용하여 거리오차를 보정해주기 위해 사용되어 진다.

3.2 시스템 실험 환경

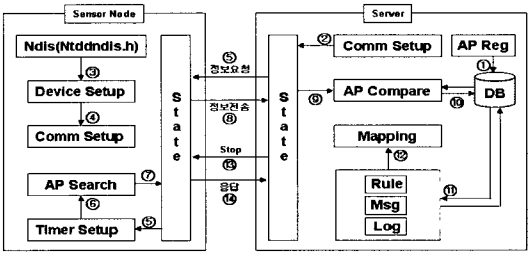
실험환경은 윈도우 XP환경에서, 마이크로소프트 SQL2005, 무선 랜 IEEE802.11 b/g 카드를 활용하여 비쥬얼 C++ 2005 환경에서 시뮬레이션을 실시하였다. XP환경의 시스템에서 무선 랜카드로 들어오는 액세스 포인트의 비콘 프레임의 각각의 필드 값을 얻기 위해 커널부분에 접근해야한다.

하지만 Windows계열 OS는 Ndis(Network Driver Interface Specification)를 사용해야 한다. Ndis는 DDK(Driver Development Kit)로 제작하는 법과 VC 2005의 ntddndis를 이용하는 방법 가운데 ntddndis 방법을 이용하였다[그림 4].



[그림 4] Ndis 구조 및 역할

3.3 모듈 별 기능 및 알고리즘

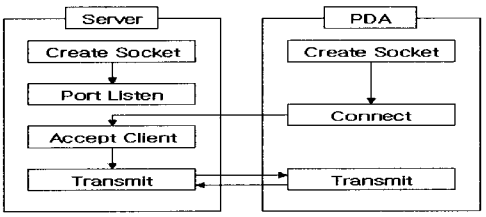


[그림 5] 시스템 흐름도

3.3.1 AP Registration Module [Server]

시스템 관리자는 등록할 엑세스 포인트의 SSID 와 MAC 주소를 입력하여 인가된 엑세스 포인트를 등록하며 더불어 등록된 목록을 수정, 삭제, View기능을 담당한다. 입력된 정보는 데이터베이스에 저장된다[그림 3].

3.3.2 Comm Setup Module [Server]



[그림 6] 소켓 통신 구조도

서버와 PDA 간의 비동기소켓 통신 설정을 담당한다. [그림 6]과 같이 서버에서 먼저 소켓 생성과 동시에 포트를 열고 PDA로부터 요청이 올 때 까지 Listen 상태로 대기한다. PDA의 접속 요청이 들어오면 Accept 하고 서로 통신을 시작 한다.

3.3.3 Comm Setup Module [PDA]

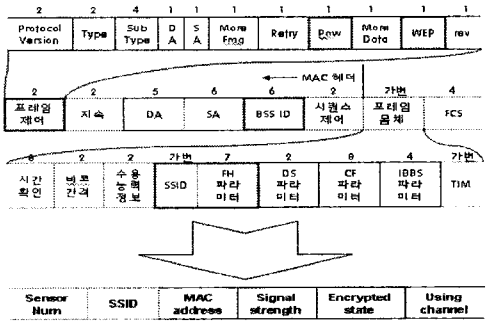
서버와 마찬가지로 PDA의 소켓을 생성하고 서버의 아이피, 포트로 연결 요청을 전송한다. 이때 서버는 Listen 상태에서 PDA의 연결 요청을 수락한다. 시스템 관리자에 의하여 서버에서 PDA들에게 주변 엑세스 포인트를 수집한 정보를 전송해 달라고 요청 메시지를 보낸다[그림 5].

3.3.4 AP Search Module [PDA]

자신의 주변에 돌아다니는 비콘 프레임를 받아서 필요한 정보들만을 재조합하여 서버로 전송하게 된다.

3.3.5 AP Compare Module [Server]

제안 시스템에서 가장 중요한 모듈 중 하나로서, 3군데의 PDA로부터 전송받은 정보와 데이터베이스<그림 3>에 저장된 엑세스 포인트와 비교하여 결과를 보안 정책에 대응하여 관리자에게 메시지를 보내고 로그를 남긴다. 보안정책은 경고(엑세스 포인트의 위치 변경), 위험(엑세스 포인트의 허용 위치 이탈), 긴급(비인가 엑세스 포인트 탐지, Pow off, 도난)로 구성된다.



[그림 7] 엑세스 포인트 정보 재조합 과정

3.3.6 Mapping Module [Server]

AP Compare 모듈과 더불어 중요한 모듈 중 하나로 각 엑세스 포인트의 위치를 계산하는 기능과 엑세스 포인트 위치 계산과 오차를 보정하는 기능을 담당한다. 엑세스 포인트의 위치를 찾는데 사용되는 알고리즘은 RSSI를 이용한 삼각측량법을 사용하고 전파환경 DB를 이용하여 거리 오차보정을 한다.

3.3.7 제안 위치탐지 알고리즘

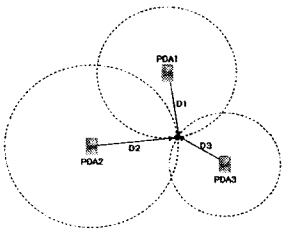
수신 신호세기를 이용하여 이동매체로부터 기준점까지의 거리를 구하기 위해서 Friis 공식 즉, 자유공간에서의 경로 손실을 이용한다. 식(1)과 같다.

$$L = 20\log_{10}(\frac{4\pi d}{\lambda})[dB] \qquad (1)$$

위의 식을 d(거리)에 대하여 정리하면, 식(2)와같이 정리된다.

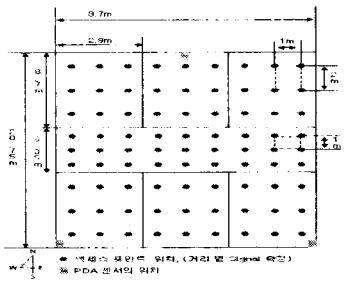
$$d = \frac{\lambda}{4\pi}10^{\frac{L}{20}}[m] \qquad (2)$$

식(2)에서 L은 수신신호세기를 나타내며, λ는 전파파장을 의미한다. 무선 랜에서 전파파장은 0.56m로 정의된다. 삼각측량법의 중에서 Lateration을 사용한다[3].



[그림 8] 삼각측량법(Lateration)

[그림 8]과 같이 기준점으로부터 거리를 반지름으로 3개의 원의 교점을 액세스 포인트의 위치로 판단할 수 있지만, RSSI를 기반으로 하는 만큼 오차가 존재한다. 따라서 미리 정의된 다양한 지점에서의 신호 세기들을 측정, 칼만-필터를 적용하여 산출 값을 데이터베이스에 저장한다[8-9]. [그림 9]에서는 각 좌표에서의 신호세기 측정법 [그림 10]에서는 오차보정 적용에 대하여 설명한다.



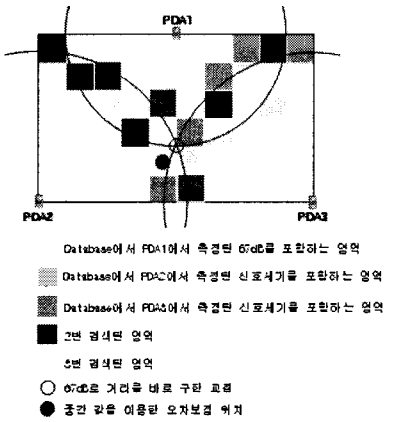
[그림 9] 각 거리별 신호세기 측정법

건물 내부를 각 영역의 9군데에서 PDA를 기준으로 액세스 포인트의 신호세기를 측정하여 칼만-필터 알고리즘을 적용하여 산출된 값을 데이터베이스에 저장한다[8-9]. 예를 들어 위치를 모르는 액세스 포인트의 신호세기가 PDA로 측정되었고, 그 세기가 67dB라 가정하자. Friis공식은 식(3)과 같다.

$$d = \frac{0.56}{4\times 3.1415926535}10^{\frac{67}{20}}[dB] \qquad (3)$$

$= 101.54650759403m$

식(3)에 의해 거리는 약101.5465m가 나온다. 측정 PDA를 중심으로 거리만큼 원을 그린다. 같은 방법으로 나머지 PDA도 신호세기에 따라 원을 그리면 3개의 원의 교점을 구할 수 있다.

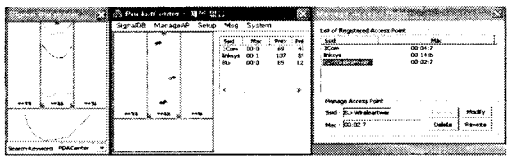


[그림 10] 오차보정 과정

그러나 데이터베이스에서 67dB를 포함하는 영역을 구해 적용하면 겹쳐진 사각형 영역들이 나온다. 겹쳐진 사각형 영역과 3개의 원의 교점과 겹친 곳이 액세스 포인트의 위치로 결정하여 보다 정확한 위치를 계산할 수 있다.

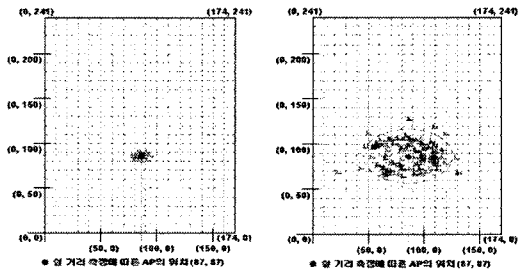
4. 실험 결과 및 고찰

[그림 13]에서는 RSSI와 ToA에서는 주변 환경에 따른 신호 Jumping 현상으로 위치탐지 오차 범위가 약 2~3m 정도 이며, 신호 Jumping 현상으로 인하여 3개의 원의 교점을 구하지 못하는 탐지에러가 빈번히 발생한다. 따라서 제안 알고리즘은 그러한 신호 Jumping 현상을 방지하고 탐지에러를 최소화 하기위해 칼만-필터 알고리즘과 환경 신호 데이터베이스를 이용하여 위치탐지의 최대 오차를 약 30cm로 줄이는 것을 확인 할 수 있었다.



[그림 11] 서버 실행 화면

[그림 12] (좌)RSSI DB측정 화면 (우)PDA 실행 화면



[그림13] (좌)제안 알고리즘 (우)RSSI

5. 결론

본 논문에서는 무선 AP탐지 시스템을 설계 및 구현하였으며, 제안된 위치탐지 알고리즘을 적용하여 실험한 결과 기존 알고리즘과 비교하여 액세스 포인트의 위치 정확도 향상 및 탐지에러를 줄일 수 있었고, 액세스 포인트의 보안 상태와 인가된 사람의 하이재킹을 사전에 방지할 수 있음을 실험을 통해 확인 할 수 있었다. 향후 연구과제로는 데이터베이스 검색시간을 최소화 할 수 있는 정보검색 기법에 대한 연구와 실내 환경의 특성을 보다 손쉽게 반영할 수 있는 기법 및 알고리즘의 연구가 필요하다.

참고문헌

[1] Y.S. Kang, K.H OH and B.H Chang, "Trends of the Evilution of Wireless Lan Security Technologies," 전자통신동향분석 제18관 제4호 2003년 8월.

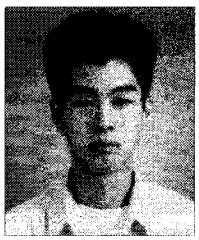
[2] J. Hightower, G. Borriello, "Location systems for ubiquitous computing," IEEE Computer, Vol. 34, No. 8, August 2001, pp. 57-66.

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

[4] G. P. Yost and Panchapakesan,"Improvement in Estimation of Time of Arrival(TOA) from Timing Advance(TA),"IEEE International Conference on Universal Personal Communications,

Vol.2, Oct, 1998. pp. 1367-1372.
[5] N. j. Thomas et al.,"A Robust Location Estimator Architecture with Based Kalman Filtering of TOA Data for Wireless Systems," Spread Spectrum Techniques and Applications, 2000.
[6] 박종태, 이위혁, 조영훈, 나재욱, "유비쿼터스 센서 네트워크에서 위치 측정 기술," 전자공학회지 제 32 권 7호, 2005. 7, pp.849-862.
[7] L. Zhu and Zhu,"A New Model and its Performance for TDOA Estimation," IEEE Vehicular Technology Conference 2001, Vol.4 Oct. 2001, pp.2750-2753.
[8] G. Welch and G. bishop,"An Introduction to the Kalman Filter," UNC-Chapel Hill TR 95-041, 2004.
[9] K. K. C. Yu, et al., "An Adaptive Kalman Filter for Dynamic Harmonic State Estimation and Harmonic Injection Tracking," IEEE Transactions on Comm. Vol. 20, No. 2, 2005, pp. 1577-1584.

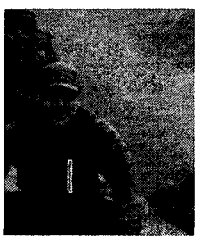
구 용 기(Yong-Ki Ku) [준회원]



• 2008년 8월 : 백석대학교 정보통신학부

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

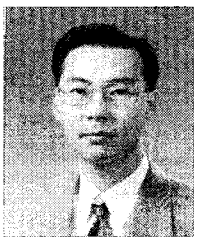
홍 진 근(Jin-Keun Hong) [정회원]



• 2008년 8월 현재 : 백석대학교 정보통신학부 교수

<관심분야>
전술통신, 센서넷, RFID, 무선랜 보안

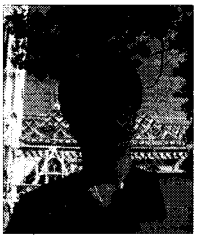
한 군 희(Kun-Hee Han) [종신회원]



• 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