# 무선 Access Point 위치, 보안상태 탐지 시스템 구현

구용기*, 홍진근*, 한군희*
*백석대학교 정보통신학부
e-mail:cutedual@bu.ac.kr

# Implement of Location Detection System of Wireless Access Point

Yong-Ki Ku*, Jin-Keun Hong*, Kun-Hui Han*
*Division of Information Communication, Baekseok University

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.

## 1. 서론

최근 무선 통신 기술의 발달과 편리성으로 인하여 기존의 유선 랜에서 무선 랜으로 변화하는 추세이다. 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. 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 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 고찰하고 5장에서 결론을 맺었다.

## 2. 위치탐지 기술 분석

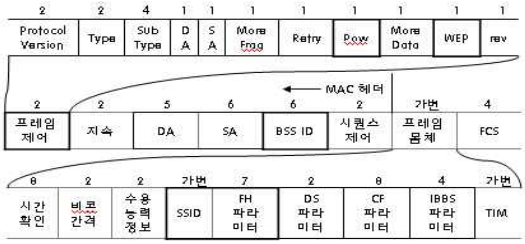
대표적인 위치탐지 시스템으로 GPS(Global Positioning System)가 있지만 실내에서는 사용될 수 없는 단점을 지니기 때문에 실내에서는 초음파, 적외선, 레이저 센서 등이 사용된다. 센서를 이용한 위치탐지 기술은 일반적으로 ToA, TDoA, AoA, 삼각측량방법이 사용된다. ToA(Time of Arrival)는 신호가 도착하는 시간을 이용하여 위치를 측정하는 알고리즘이다[4-6]. TDoA(Time Difference of Arrival)는 이동매체와 2개 이상의 센서가 송/수신 하는 신호의 도착 시간의 차이를 측정하여 거리를 산출하는 알고리즘이다[6]. AoA (Angle of Arrival)는 센서에서 이동 매체가 보내오는 신호의 방위각을 이용하여 각을 측정하고 3개의 센서로부터 산출된 방위각의 연장선의 교점으로 이동 매체의 위치를 측정하는 알고리즘이다[6]. RSSI (Received Signal Strength Indicator)는 신호 손실도를 이용한 거리 측정 방법과 신호세기들의 RSSI 표본 수집을 이용

한 통계적 위치 추측 방법으로 나뉜다. 삼각측량법은 거리 측정을 이용한 Lateration 방법 및 각도 측정에 기초한 Angulation 방법으로 구분된다. 본 논문에서는 RSSI와 칼만 필터를 이용한 환경 데이터베이스를 적용하며, 삼각측량법 중 Lateration 방법을 사용한다.

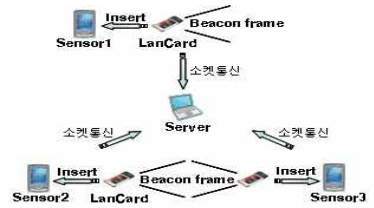
## 3. 제안 시스템 프레임워크

### 3.1. 시스템 구성

건물 내부에 액세스 포인트의 위치와 보안 상태 탐지를 위한 시스템은 비콘 프레임 정보를 수집하여 각 액세스 포인트의 위치 및 상태를 파악한다.




<그림 1> 비콘 프레임 구조



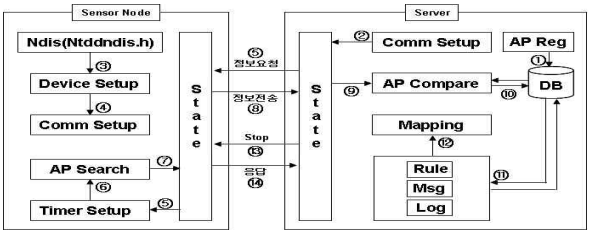

<그림 2> 시스템(물리적) 구성도

<그림 2>에서 보는 바와 같이 제안 시스템에서는 크게 3개의 센서노드와 하나의 서버로 구성된다. 센서노드는 연결된 무선 랜카드부터 주변 액세스 포인트의 비콘 프레임을 수집하고 해당 정보를 소켓통신을 통해 서버로 전송한다. 서버는 3개의 센서노드로부터 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.

### 3.2. 시스템 실험 환경

실험환경은 윈도우 XP환경에서, 마이크로소프트 SQL2005, 무선 랜 IEEE802.11 b/g 카드를 활용하여 비쥬얼 C++ 2005 환경에서 시뮬레이션을 실시하였다. XP 환경의 시스템에서 무선 랜카드로 들어오는 액세스 포인트의 비콘 프레임의 각각의 필드 값을 얻기 위해 Ndis(Network Driver Inter- face Specification)를 사용하며, Ndis는 DDK(Driver Develop- ment Kit)로 제작하는 법과 VC 2005에서 제공하는 ntddndis를 이용하는 방법 가운데 ntddndis 방법을 이용하였다.

### 3.3. 제안 시스템 모듈별 기능 및 알고리즘




<그림3> 시스템 흐름도

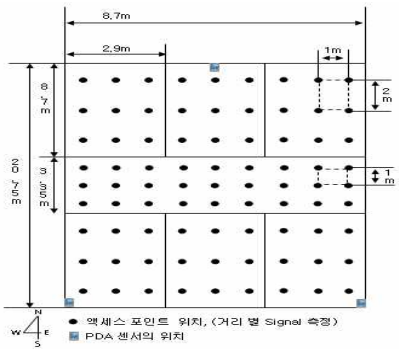
수신 신호세기를 이용하여 이동매체로부터 기준점까지의 거리를 구하기 위해서 Friis 공식 즉, 자유공간에서의 경로 손실을 이용.

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

위의 식을 d(거리)에 대하여 정리하면,

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

와 같이 정리된다. 여기서 L은 수신신호세기를 나타내며, $\lambda$는 전파파장을 의미한다. 무선 랜에서 전파파장은 0.56m로 정의된다. 삼각측량법의 중에서 Lateration을 사용한다[3]. 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, 칼만필터를 적용하여 산출 값을 데이터베이스에 저장한다[8-9]. <그림 4>에서는 각 좌표에서의 신호세기 측정법에 대하여 설명한다.




<그림 4> 각 거리별 신호세기 측정법

건물 내부를 3m거리로 범위를 자르고, 센서노드를 기준으로 8방향으로 액세스 포인트의 신호세기를 여러 번 측정하고 칼만필터 알고리즘을 적용하여 측정 시 무

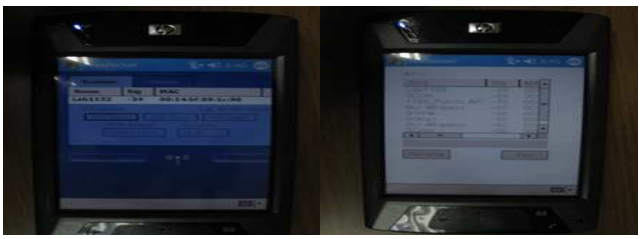
선 신호 Jumping 현상을 막아 오차범위를 줄이고 산출된 값을 데이터베이스에 저장한다[8-9]. 어디에 있는지 모르는 액세스 포인트의 신호세기 센서노드로 수집되었고, 그 세기가 67dB라 가정하자. Friis공식에 의하여

$$d = \frac{0.56}{4 \times 3.1415926535} 10^{\frac{67}{20}} [dB] \quad (3)$$
$$= 0.0453591587 \times 10^{3.35} [dB]$$
$$= 0.0453591587 \times 2238.7211385683$$
$$= 101.54650759403m$$

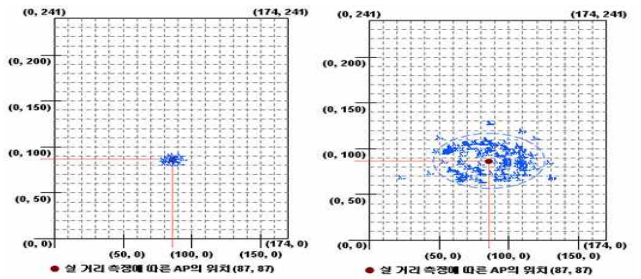
거리는 약101.5465m가 나온다. 측정 센서를 중심으로 거리만큼 원을 그린다. 이와 같이 각 2개의 센서도 측정된 신호세기에 따라 원을 그리면 3개의 원의 교점을 구할 수 있다. 그러나 데이터베이스에서 67dB를 포함하는 영역을 구해 적용하면 겹쳐진 사각형 영역들이 나온다. 겹쳐진 사각형 영역과 3개의 원의 교점과 겹친 곳이 액세스 포인트의 위치로 결정하여 보다 정확한 위치를 계산할 수 있다.

## 4. 실험 결과 및 고찰


<그림 5-A> 서버 실행 화면



<그림 5-B> (좌)RSSI DB측정 화면 (우)센서 실행 화면




<그림 6> (좌)제안 알고리즘 (우)RSSI 알고리즘

<그림 6>에서는 RSSI와 ToA에서는 주변 환경에 따른 신호 Jumping 현상으로 위치탐지 오차 범위가 약 2~3m정도 이며, 신호 Jumping 현상으로 인하여 3개의 원의 교점을 구하지 못하는 탐지에러가 빈번히 발생한다. 따라서 제안 알고리즘은 그러한 신호 Jumping 현상을 방지하고 탐지에러를 최소화 하기위해 칼만필터 알고리즘과 환경신호 데이터베이스를 이용하여 위치탐지의 최대 오차를 약 30cm로 줄이는 것을 확인 할 수 있었다.

## 5. 결 론

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 방지 할 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 32권 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.