PDA 기반 무선 AP의 위치추적 시스템 구현

박주평*, 홍진근*, 한군희*

*백석대학교 정보통신학부
e-mail:maleewh@naver.com

Implementation of Location Tracking System of Wireless Access Point based PDA

Joo-Pyoung Park*, Jin-Keun Hong*, Kun-Hee Han*
*Division of Information Communication, Baekseok University

요 약

최근 무선 통신 기술의 발달은 장비를 간편화 하고 편리화 시키게 되었다. 또한 다양한 서비스를 창출할 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.

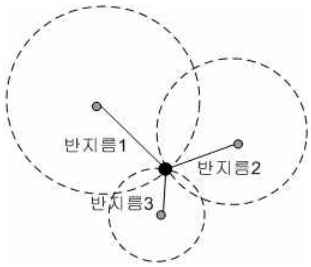
1. 서론

기술의 발달은 장비를 간편화 하고 편리화 시키고 있다. 많은 장비들을 사용자가 편리하게 사용하고 관리하기 위해 장비간의 네트워크는 필수가 되었다. 하지만 다양한 장비들의 서비스 제공을 위한 네트워크 구성에 있어 유선은 공간적 제약 사항이 뒤따른다. 이는 다양한 장비의 네트워크 구성에 있어 많은 불편 사항을 발생 시킨다. 해결책으로 제시된 무선 랜은 유선의 제약 사항을 보안하고 많은 서비스를 지원할 수 있는 기반을 마련하였다. 하지만 무선 랜의 접근성 및 편리성 확대는 보안위협에 대한 큰 허점을 드러내 보인다. 해커들은 불법 무선 랜을 통하여 방화벽을 우회 할 수 있고 침입 경로를 감출 수 있다. 또한 워 드라이빙을 통하여 물리적 위치 또한 감추기 쉽다. 이런 보안 위협을 제공하는 것은 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 대부분은 보안에 취약하다. 06년 4월에 실시한 무선 랜 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. 본 논문에서는 무선 랜의 취약성을 파악하고자 간편하게 PDA 상에서 AP 정보와 보안 상태를 점검 하고 AP 위치를 추적하여 map에 도식하고자 한다. 본 논문의 구성은 다음과 같이 구성된다. 2장에서는 위치탐지 기술 및 특징을 기술하며, 3장에서는 위치 탐지 시스템의 기술적 사항을 소개하였다. 그리고 4장에서 결론으로 맺었다.

2. 위치탐지 기술 및 특징

본 논문에서 제안된 알고리즘에서는 측정자의 위치와 AP 와의 거리를 통하여 AP의 위치를 추론 하였다. 본 프로그램에서는 GPS의 RMC 데이터를 통해 측정자 위치를 파악하고 <그림 1>에서와 같이 3

개의 측정자 위치에서의 신호 값 [반지름1,반지름2, 반지름3]정보를 통해 AP 위치를 2차원 평면에서 추정 하였다.



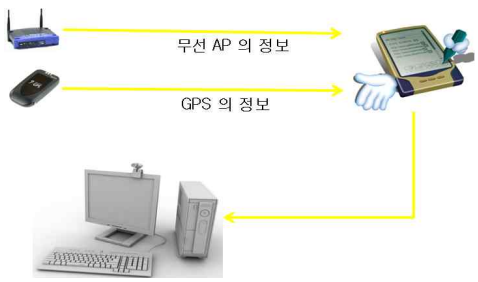
<그림 2> 신호 측정에 의한 2 차원 위치 검출

PDA는 GPS 모듈과 시리얼 통신을 통하여 GPS 정보를 획득하고 NDIS를 통하여 네트워크 카드로부터 무선 랜 신호감쇠 정보를 획득 한다. PDA는 두 정보를 혼합하여 정보 테이블을 만들고 정보 테이블은 소켓통신을 통하여 공간 제약 없이 Computer 로 보내질 수 있다. Computer 는 AP정보 테이블을 통해 AP위치 추적 및 정보를 사용자에게 보기 쉽도록 표현해 준다.

3. 위치 탐지 시스템

3.1 전체적 시스템 구성

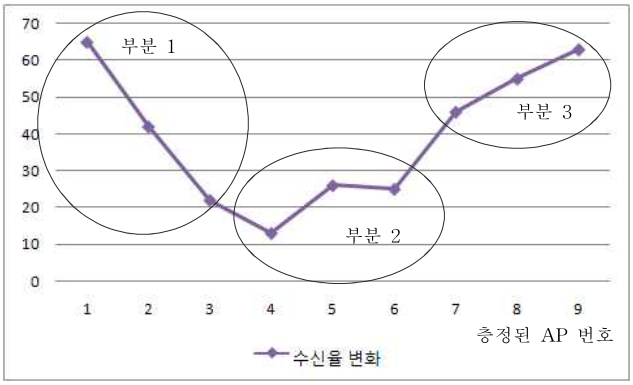
PDA상에서 AP에 대한 전반적인 정보 수집이 이루어진다. 사용자는 PDA를 이용하여 비교적 작은 범위의 지역을 순찰하면서 AP의 상태 파악 및 불법 AP를 탐지할 수 있다. PDA를 통하여 탐지된 전반적인 정보 데이터는 Computer로 옮겨져 맵에 도식화 하고 사용자에게 정보를 보기 편하도록 편리성을 제공해준다. <그림 4> 는 본 프로그램의 구성을 나타낸다.



<그림 4> 시스템 구성도

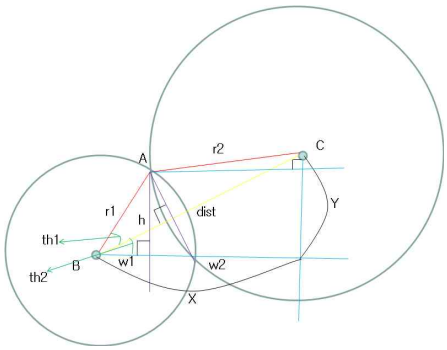
3.2위치 추적 알고리즘

<그림 6>은 주기에 따라 신호측정 데이터 그래프이다.



<그림 6> AP 신호표

본 프로그램에서는 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 방식을 적용하여 실험을 해보았다. 첫 번째 방식은 분류된 AP의 모든 정보 갯수를 3등분 하여 3부분으로 나누고 각 부분에서 신호가 가장 좋은 신호만을 추출 하는 방식이다. 본 방식은 넓은 범위에서 신호가 좋은 데이터를 얻어 표현 하고자 한 방식이다. 두 번째 방식은 분류된 AP 의 모든 데이터 갯수를 3등분 하여 나누어진 각 부분의 중간 위치의 신호를 추출 하는 방식이다. 신호 세기를 고려하지 않고 중간 값을 추출함으로서 물리적 위치의 평균점에서 AP 위치를 측정하고자 하였다. 마지막 방식은 측정 위치와 관계없이 동일 위치가 아니면서 가장 좋은 신호 값 3개를 추출 하는 방식이다. AP위치를 측정함에 있어 간섭이 적은 신호를 추출하여 신호적 오차가 적은 데이터를 얻고자 하였고 데이터의 일관성을 갖고자 하였다. 추출된 3개의 신호 정보는 측정자의 위치로부터 무 방향성으로 AP위치를 표현해 준다. 이는 3개의 신호정보를 취하여 AP 위치를 2차원에 표시할 수 있게 한다. <그림 9>는 신호 값을 원 의 반지름으로 표시하고 해당 원의 교차점을 얻고자 한다.



<그림 9> 위치 교점 탐색 1

위의 두 원의 교차점을 구하기 위하여 (1)과 같은 식을 사용하였다.

$$x = x_1 + r_1 \cos(\tan^{-1}\frac{Y}{X} \pm \cos^{-1}(\frac{r_1^2 - r_2^2 + D^2}{2r_1 D}))$$

$$y = y_1 + r_1 \sin(\tan^{-1}\frac{Y}{X} \pm \cos^{-1}(\frac{r_1^2 - r_2^2 + D^2}{2r_1 D}))$$

(1)

두 원의 교점을 구한 후 나머지 신호 정보를 이용하여 2차원 평면상에서 AP의 위치를 추론한다.

3.3 시스템 구동 및 시뮬레이션 결과

구현된 PDA 프로그램을 통해<그림12> 및 <표 4>에서와 같은 데이터를 얻을 수 있었다. AP의 정보는 실시간으로 PDA에서 표현되어 진다.

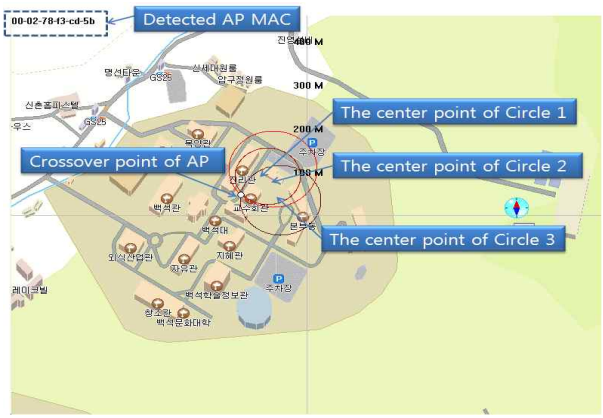
<그림 12>시뮬레이션 결과 화면

얻어진 PDA의 데이터는 컴퓨터에 보내지고 컴퓨터는 PDA를 통해 얻은 정보<표 4>를 통하여 <그림13>과 같이 나타낼 수 있다.

<표 4> 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

3개의 신호 값을 반지름으로 하는 원을 그리고 그 원들의 교점을 구함으로서 <그림13>과 같은 AP위치를 탐지할 수 있다. AP위치 추적을 위해 측정자 위치가 다른 최적의 신호 값 3개를 추출하여 교점을 구하였다. 맵 좌측 상단에 해당 AP의 MAC 주소가 표시된다.



<그림 13> 추적된 AP 도식

시험된 대학가 주변을 탐색한 결과 80% 이상이 보안 설정을 하지 않고 사용 중임이 나타났다. 또한 신호정보를 통하여 위치 정보를 추론할 수 있었다.

4. 결 론

본 논문에서는 PDA를 활용하여 실외에서 무선 AP를 탐지하는 탐지시스템을 구현하였다. 구현을 위해 PDA 환경 인터페이스 설계, PDA와 호스트 PC 간 소켓통신 인터페이스 설계, 호스트 상에서 맵 도식 인터페이스 및 GUI 설계, 구현하였다. 구현된 시스템을 활용하여 모 대학 주변을 탐지한 결과, 지도에 도식된 AP 정보를 통하여 사용자는 AP의 위치를 알 수 있었다. 또한 PDA를 통해서 얻은 AP 정보 테이블을 보면 대부분의 AP는 오픈되어 있어 보안 설정이 미흡한 상태로 나타났다. 본 논문에서 구현된 시스템을 적용하여 무선 랜 위치 및 AP정보를 을 살펴봄으로써 많은 위협으로부터 AP들이 안전하지 못하다는 것을 파악할 수 있었다.

참고문헌

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

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

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

[4] 김태은, "두 원의 교점구하기," http://www.davpia.com/MAEUL/Contents/Detail.aspx?BoardID=18&MAEULNO=8&no=1217