IEEE 802.11i 에서 수신 신호세기를 이용한 무선 노드 인증 기술

김신구 O, 이현진, 김재현

아주대학교 전자공학과

An Authentication Technique in IEEE 802.11i Using Received Signal Strength

Shin-Gu Kim O, Hyun-Jin Lee, Jae-Hyun Kim

School of Electrical and Computer Engineering, Ajou University

{youdotan, 133hyun, jkim}@ajou.ac.kr,

요 약

브로드캐스팅 방식의 무선 네트워크 서비스는 일정 범위 내에서 누구든지 자유롭게 무선랜 AP에 접속할 수 있기 때문에 이는 보안 사고를 유발할 수 있다. 본 논문에서는 이러한 보안 문제를 극복하기 위하여 AP가 같은 실내에서만 무선 노드의 접속을 허용하는 무선 노드 인증 기술을 제안한다. 제안하는 무선 노드 인증 기술은 IEEE 802.11i 표준에 AP로부터 수신 신호의 세기를 이용하여 접속 허용 여부를 결정하는 절차를 추가하여, 노드의 위치가 실내인지 실외인지를 구분하고, 실외일 경우 접속을 차단하여 보안 문제를 사전에 방지할 수 있다.

1. 서론

무선 네트워크 서비스는 IEEE 802.11 표준을 기반으로 지속적인 발전을 통해 사용범위가 확대되어 빌딩 내 Enterprise Network 환경에서 유선랜의 역할을 대체하고 있다. 그러나 브로드캐스팅 방식의 무선 네트워크 서비스는 일정 범위 내에서 자유롭게 노트북, PDA 등을 통해 무선랜 AP(Access Point)에 접속할 수 있기 때문에 보안 문제가 발생할 수 있다. 흔히 발생할 수 있는 예로, 사무실과 가까운 곳에 위치한 노드는 사무실 내 AP 로의 접속이 가능하기 때문에, 외부인이 같은 AP 에 접속한 사무실 내 노드의 데이터를 빼내올 수 있다. 이와 같이 IEEE 802.11 은 보안상의 문제점이 많다는 것이 알려지게 되어, 강한 보안을 제공하는 IEEE 802.11i 표준이 제안, 채택되었다[2], [5]. 표준 내 WPA(Wi-Fi Protect Access)에는 임시 키 암호화, 메시지 무결성 점검 등의 강력한 인증 기능이 포함되어 있어 무선 네트워크를 위한 기존 보안 프로토콜에서 발생하는 보안 문제를 일부 해결해 준다[1], [9].

그러나 암호화를 통한 인증 기술에서도 보안 문제는 발생할 수 있다. 사무실 내 AP 에 접속이 가능한 기업 내부인이 사무실과 가까운 외부에서 AP 에 접속하여, 사무실 내 데이터를 외부인에게 보여줄 수 있다. 또한 기업 외부인이 AP 접속 암호를 알게 되면, 가까운 외부에서 자유롭게 Enterprise Network 에 접속할 수 있다. 같은 AP 에 접속한 노드 내에 개인 정보, 금융 정보, 기업 기밀자료 등이 있다면, 이는 바로 보안 사고로 이어질 수 있다.

본 논문에서는 위와 같은 보안 문제를 해결하기 위해 수신 신호세기를 이용하여 실외로부터 노드의 접속을 차단하는 IEEE 802.11i 에서의 무선 노드 인증 기술을 제안하였다.

2. 시스템 모델

본 논문에서 제안하는 기술은 수신 신호세기를 이용한 무선 노드 인증 기술이다. 그림 1 은 제안하는 무선 노드 인증 기술의 활용 예를 나타낸다.

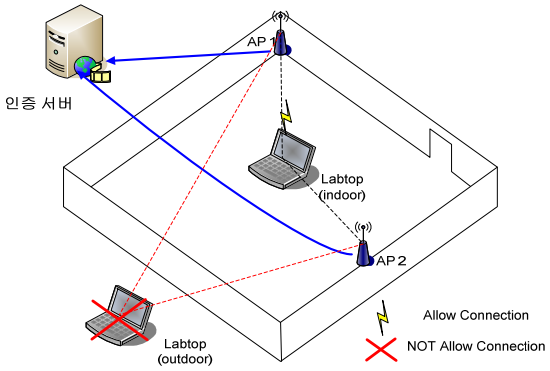

그림 1. 제안하는 무선 노드 인증 기술의 활용 예

이 기술을 통해 그림 1 과 같은 실내 환경에서, AP 는 실내에 있는 노드의 접속을 허용하고, 실외에 있는 노드의 접속을 차단할 수 있다. 그림 2 는 제안하는 인증 기술에서 노드, AP, 그리고 인증서버의 동작 절차를 나타낸 것이다. 먼저 노드-AP 간의 인증과 접속 요청 절차가 끝나면, 노드는 AP 에게 EAP-Start 메시지를 전송함으로써, IEEE 802.11i 표준의 보안 과정을 시작한다[3]. AP 는 노드의 존재를 인지하기 위해 EAP Request/Identity 메시지를 전송하고, 노드는 EAP Response/Identity 메시지를 전송하여 자신의 존재를 AP 에게 인지시킨다. AP 는 인증서버-노드 간의 상호 인증을 위해 Radius-Access-Request 메시지를 인증서버에게 전송하고, 인증서버는 AP 에게 Radius-Access-Challenge 메시지를 전송하여 수신 신호세기를 측정하도록 요청한다. 요청 받은 AP 는 노드에게 주변 AP 로부터 수신하는 Beacon 신호의 수신 신호세기를 측정하도록 Signal Strength Data Request 메시지를 전송한다. 노드는 주변 AP 로부터 수신한 Beacon 신호의 신호세기를 측정하여 각각의 AP 에게 Signal Strength Data 메시지를 전송하면, 각각의 AP 는 송신 신호세기와의 차를 구하여 path-loss 를 측정하고, 인증서버에게 Path-loss Data 를 전송한다.

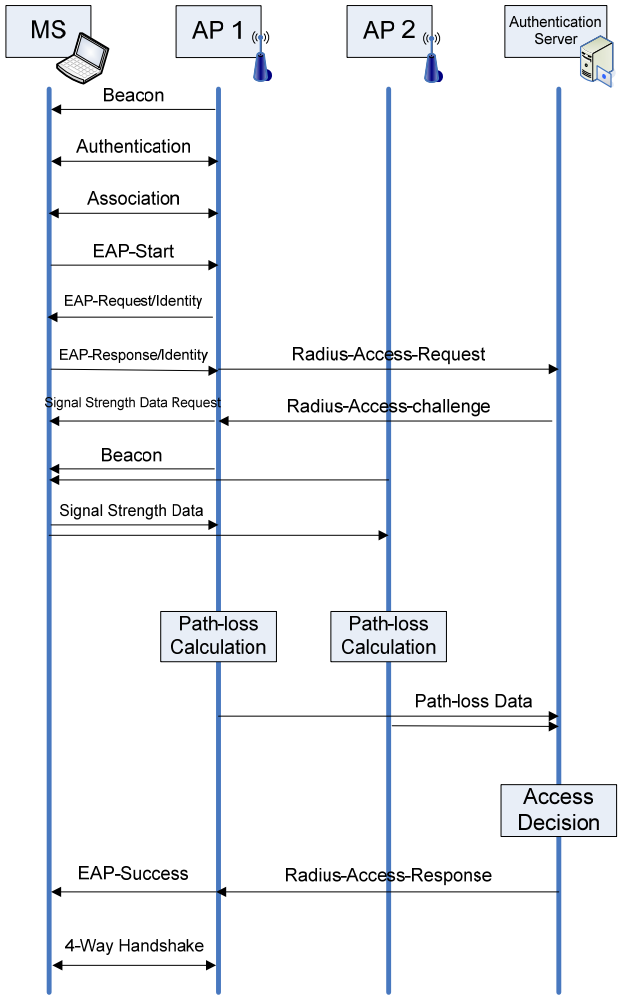

그림 2. 무선 노드 인증 기술 절차

노드의 접속 허용 여부를 결정하는 절차는 인증서버에서 이루어진다. 인증서버는 각각 AP 에서 전송한 노드의 수신 신호세기의 평균을 계산하고 실내 수신 신호세기 기준(PL_{indoor})과 비교하여 노드의 접속을 허가할 것인지 차단할 것인지를 결정한다. PL_{indoor} 은 선험적(a priori)으로 얻어지는 값으로, 노드-AP 간의 path-loss 가 PL_{indoor} 보다 작을 경우 인증서버는 노드의 접속을 허용하고, 클 경우에는 접속을 차단하는 결정(Access Decision)을 하여, 그 결과를 Radius-Access-Response 메시지를 통해 AP 에게 전송한다. AP 는 결과 데이터를 바탕으로 접속을 시도한 노드에게 EAP-Success/Failure 메시지를 전송한다. 또한 노드의 이동성을 고려해서, 지속적으로 수신 신호세기를 측정하여 서비스 제공 여부를 결정한다.

3. 성능 분석 결과

제안하는 무선 노드 인증 기술의 성능을 평가하기 위해, 그림 3 과 같이 AP 가 설치된 실내 환경(22 X 18m)과 이를 포함한 주변(26 X 22m) 1000 개의 임의 좌표에서 노드가 접속을 시도하는 것을 가정하였다.

실내 환경에 설치된 AP 에 노드가 접속을 시도할 때 고려할 수 있는 채널 모델은 실내와 실외로 구분할 수 있으며, AP 와 노드가 모두 실내에 존재할 경우의 경로손실 모델은 식 (1)과 같다.

$$PL(dB) = 18\log_{10}(d) + 46.8 + L_{shadowing} \quad (1)$$

이 때, PL 은 경로손실, d 는 AP 와 노드 간의 거리를 나타내며, $L_{shadowing}$ 은 shadowing 에 의한 손실을 나타낸다. 노드가 실외에 위치할 경우 벽과 같은 장애물에 의한 감쇄가 증가할 뿐만 아니라 shadowing 도 증가한다. 따라서 [6]에서 제안하고 있는 실내-실외일 때의 경로손실 모델을 가정하였고, 이 때의 경로손실 모델은 식 (2)와 같다.

$$PL(dB) = 22.7\log_{10}(d) + 41.0 + L_{shadowing} + L_{excess} \quad (2)$$

이 때, L_{excess} 는 실내에서 실외로 신호를 전송할 때 추가로 발생하는 경로손실로, 평균이 $18+3\,n_{walls}$ (n_{walls} 은 벽의 개수)이고, 표준편차가 8dB 인 normal 분포를 따른다고 가정하였다. 또한 각 경로손실 모델의 유형에 따른 shadowing 은 평균이 0 이고, 표준편차가 표 1 과 같은 log-normal 분포를 따른다고 가정하였다[6].

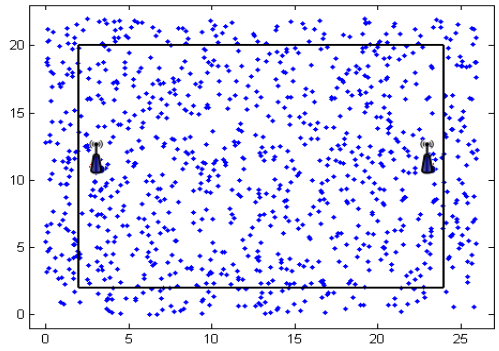

그림 3. 시뮬레이션 환경

표 1. 경로손실 모델의 유형에 따른 표준편차

유형	실내-실내		실내-실외	
표준편차 (dB)	LOS	NLOS	LOS	NLOS
	3.1	3.5	2.3	3.1

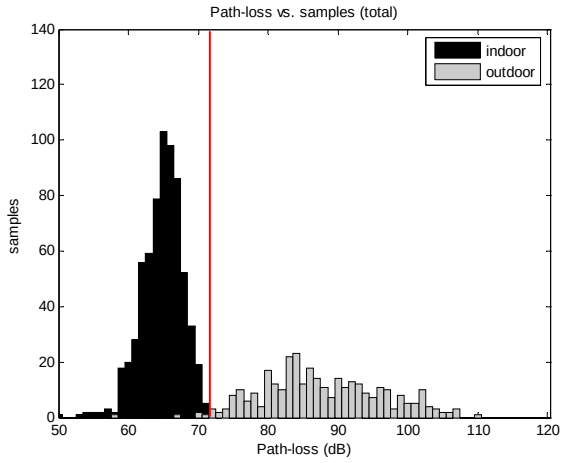

그림 4. 노드의 접속 위치에 따른 수신 신호세기의 분포도

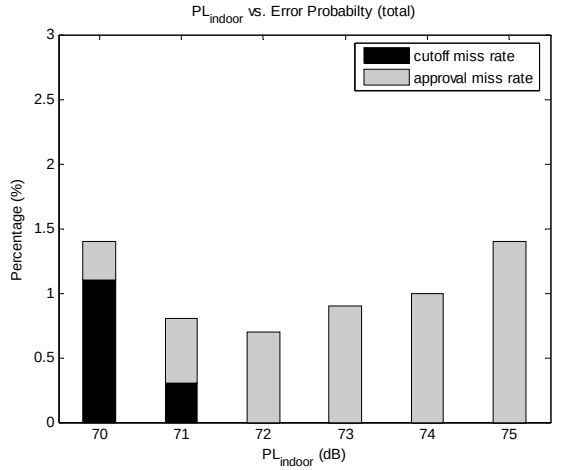

그림 5. $PL_{indoor}(dB)$ **에 따른 오차율**

그림 4 는 노드의 접속 위치가 실내일 때(indoor)와, 실외일 때(outdoor)를 구별하여 측정한 노드의 path-loss 평균값 분포도이다. 두 분포도를 살펴보면 수신 신호세기 평균값이 약 70~75dB 일 때를 기준으로, 노드의 접속 위치에 따라 path-loss 평균값의 분포가 나누어 지는 것을 관찰할 수 있다. 그림 5 는 지정한 PL_{indoor} 에 따른 오차율을 나타낸 것이다. PL_{indoor} 을 72dB 로 지정하였을 때, 오차가 가장 적게 발생하는 것을 확인할 수 있다.

4. 결론

본 논문에서는 수신 신호세기를 이용하여 실외의 노드의 접속을 차단하는 무선 노드 인증 기술을 제안하였다. 제안하는 기술은 노드가 각각의 주변 AP 들로부터 받은 신호의 수신 신호세기를 측정하고, 이를 토대로 AP 는 path-loss 를 계산하여, 평균값이 PL_{indoor} 을 초과할 경우 접속을 차단하여 실외에서 노드가 AP 에 접속할 수 없도록 하는 기술이다. 성능 분석 결과 $PL_{indoor} = 72dB$ 일 때, 오차율이 1% 미만으로 발생하는 것을 확인하였다. 이 기술이 무선 네트워크 서비스를 이용하는 사무실, 연구소, 학교 등의 기관에 도입할 경우 내부 데이터가 외부로 유출되는 보안 사고를 사전에 방지할 수 있을 것으로 기대된다.

5. 참고 문헌

[1] J. Chen, M. Jiang, and Y. Liu, “Wireless LAN Security and IEEE 802.11i,” *IEEE Wireless Commun.*, vol. 3, no. 1, pp. 27-36, Feb. 2005.

[2] J. Lee, J. Kim, J. Park, and K. Moon, "A Secure Wireless LAN Access Technique for Home Network," in *proc. IEEE Vehicular Technology. Conf. 2006,* vol. 2, pp. 818-822, May 2006.

[3] X. Xinyu, S. Elhadi, B. Darcy, and S. Tarek, “Security Analysis and Authentication Improvement for IEEE 802.11i Specification,” in *proc. IEEE Global Telecommun. Conf. 2008*, pp. 1-5, Nov. 2008.

[4] S. Eum and H. Choi, “EAP-Kerberos II: An Adaptation of Kerberos to EAP for Mutual Authentication,” IEEE *International Conf. on ITS Telecommun. 2008*, pp. 78-83, Oct. 2008.

[5] “Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i,” *NIST Special Publication 800-97*, Feb. 2007.

[6] “Multi-hop Relay System Evaluation Methodology [Channel Model and Performance Metrics],” *IEEE 802.16j-06/013rl*, Feb. 2007.

[7] T. Kitasuka, K. Hisazumi, and T. Nakanishi, “WiPS: Location and Motion Sensing Technique of IEEE 802.11 Devices,” in *proc. IEEE Information Technology and Applications. Conf. 2005,* vol. 2, pp. 346-349, Jul. 2005.

[8] K. Kaemarungsi, “Distribution of WLAN Received Signal Strength Indication for Indoor Location Determination,” *IEEE Wireless Pervasive Computing*, pp. 6, Jan. 2006.

[9] J. Liu, X. Ye, J. Zhang, and J. Li, “Security Verification of 802.11i 4-Way Handshake Protocol,” *IEEE International Conf. on commun. 2008*, pp. 1642-1647, May 2008.