TDD 시스템에서 무선 채널 기반 물리 계층 인증에 관한 연구

서민재[§], 이채혁[§], Ivy Selorm Dogbey[†], 방인규[■†], 김태훈[■§]

[§]국립한밭대학교 컴퓨터공학과, [†]국립한밭대학교 지능미디어공학과

{20201738, 20242073, 30231229}@edu.hanbat.ac.kr, {ikbang, thkim}@hanbat.ac.kr

A Study on Physical Layer Authentication based on Wireless Channel in TDD Systems

Minjae Seo[§], Chaehyeok Lee[§], Ivy Selorm Dogbey[†], Inkyu Bang[■†], Taehoon Kim[■§]

[§]Department of Computer Engineering, Hanbat National University

[†]Department of Intelligence Media Engineering, Hanbat National University

요 약

5G, 와이파이 등의 무선 통신 기술의 확산으로 인해 무선 통신 시스템의 사용이 급증하며 도청, 위장 공격 등에 대한 취약점도 증가하는 추세이다. 본 연구는 TDD 시스템의 채널 상호성(Channel Reciprocity)을 이용한 비밀키 생성 및 공유 기법과 합법적인 송신자와 도청자를 구분하기 위한 임계값 기반의 인증 과정을 제안한다. 합법적인 송신자와 도청자를 구분하기 위한 임계값 설정이 인증 성능에 미치는 영향을 살펴보기 위해 MATLAB을 이용해 모의실험을 진행하고, 탐지 확률을 성능 평가 지표로 사용하여 임계값 변화에 인증 성능을 확인하였다.

Ⅰ. 서론

무선 통신 기술은 IoT(사물인터넷), 5G와 같은 차세대 네트워크 기술의 발전과 함께 폭발적으로 성장하고 있으며, 다양한 응용 분야에서 중요한 역할을 하고 있다. 동시에 무선신호가 범람하기 때문에 무선 통신 시스템은 도청(eavesdropping)이나 위장 공격(spoofing)과 같은 외부 공격에 쉽게 노출될 수 있는 취약점이 존재하는 것으로 보고되고 있다 [1]. 이러한 보안 취약점을 해결하기 위해 기존의 암호화 기반 보안 기법들이 사용되고 있지만, 높은 계산 복잡도와 제한된 자원을 가지는 IoT 장치에서 적용하기에는 실효성이 떨어지는 문제가 있다.

물리계층 보안은 무선 채널의 상호성(channel reciprocity) 및 채널의 고유 특성을 활용하여 보안을 강화하는 접근법으로, 기존의 암호화 기법과는 다른 차원의 보안성을 제공한다 [2]. 송신기와 수신기 간의 상호 신뢰성을 검증하고, 잠재적 도청자와 같은 비인가 사용자가 합법적인 채널을 모방하지 못하도록 방지하는 연구가 진행되고 있다 [2]. 특히 무선 채널의 위상(Phase) 정보를 활용한 인증 기법은 기존 방식보다 더 나은 성능을 발휘하며, 이러한 기법을 기반으로 한 다양한 연구 또한 활발히 이루어지고 있다 [3].

본 연구에서는 무선 채널 상태 정보를 이용해 비밀키 생성하고 공유하고, 이 킷값을 활용한 사용자 인증 기법을 제안한다. MATLAB 기반의 모의실험을 통해 인증하는 과정에서 합법적 송신자와 도청자를 구분하는 임계값 설정에 대한 영향을 집중적으로 분석한다.

Ⅱ. 무선 채널 기반 비밀키 공유 및 인증 기법

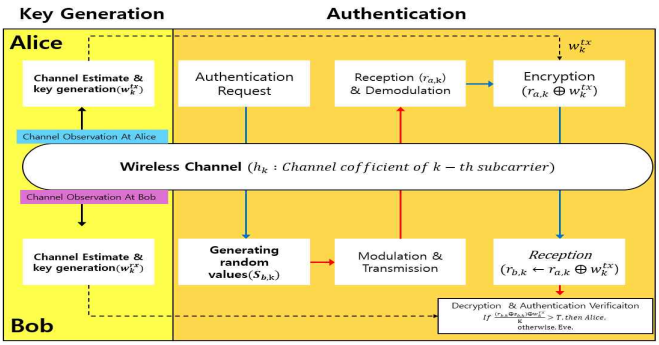

그림 1 물리 계층 인증 과정

본 연구에서는 송신기(Alice), 수신기(Bob), 도청자(Eve)가 있는 상황을 고려하고 있으며, 송신기(Alice)가 수신기(Bob)에게 인증 요청(Authentication Request)을 하는 과정을 고려하고 있다 (그림 1 참고) 송수신기는 무선채널 추정값을 이용하여 인증해 필요한 비밀키를 생성하고, 채널 상호성에 의해 자동으로 비밀키를 공유하고 있다고 가정한다 [4, 5]. 송신기는 인증 요청 시에 비밀키를 생성하고, 수신기는 인증 요청 수신 후 인증을 진행하는 중에 비밀키를 생성한다.

송수신기는 K개의 부반송파(subcarrier)를 이용해 통신을 수행한다고 가정할 때, $h_k (k \in \{1, \cdots, K\})$는 k번째 부반송파의 채널 계수(channel coefficient)를 나타내며, $h_k \sim CN(0,1)$이다. 각 송수신기기는 이진화(binarization) 과정을 거쳐 비밀키를 생성하게 되는데, 다음과 같다.

■ Corresponding Authors: Inkyu Bang (ikbang@hanbat.ac.kr), Taehoon Kim (thkim@hanbat.ac.kr)

$$w_k^{\mathrm{x}} = \begin{cases} 0, \text{if } \left|\hat{h}_k^{\mathrm{x}}\right|^2 \le \alpha, \mathrm{x} \in \{\mathrm{tx}, \mathrm{rx}\} \\ 1, \text{otherwise} \end{cases} \quad (1)$$

본 연구에서는 메시지를 변복조하는 과정에 Binary Phase Shift Keying (BPSK)만 사용하는 것을 가정하고, 비밀키 길이는 부반송파의 개수와 동일하다고 가정한다.

인증 요청을 받은 Bob은 무작위 이진값(s_b)을 생성한 후, 해당 값을 변조(modulation) 후 Alice에게 송신함으로써 인증 과정을 진행한다. Alice는 수신한 신호를 복조(demodulation)하여 Bob이 송신한 비트 정보를 획득($r_{a,k}$)하고, 이 획득한 비트 정보에 Alice가 무선 채널로부터 추정한 킷값(w_k^{tx})을 XOR 연산을 거쳐 변조 후 송신한다($r_{a,k} \oplus w_k^{\mathrm{tx}}$).

Bob은 수신한 신호를 복조 후 획득한 값($r_{b,k}$)에 Bob 측에서 생성했던 무작위 값($s_{b,k}$)로 XOR 연산하여 Alice가 전송한 비밀키를 복원한다($r_{b,k} \oplus s_{b,k}$). 이후 Alice가 송신한 킷값과 Bob에서 측에서 추정한 킷값을 비교하여 일치율이 임계값(T)보다 크면 Alice라고 판단하고 그렇지 않으면 도청자(Eve)라고 판단한다. 수신기가 판단한 인증 요청자(Authentication Clkient)를 수식으로 표현하면 다음과 같이 표현할 수 있다.

$$\text{Authentication Client} = \text{if} \frac{(\mathrm{r_{b,k}} \oplus \mathrm{s_{b,k}}) \oplus \mathrm{w_k^{rx}}}{\mathrm{K}} > \mathrm{T}, \text{then Alice} \quad (2)$$
$$\text{otherwise, Eve}$$

Ⅲ. 성능 평가

본 연구에서 제안하는 기법의 성능을 검증하기 위해 MATLAB을 활용하여 모의실험을 수행하였고, 그래프의 각 데이터 포인트마다 10만번의 반복 실험을 통해 평균값을 계산하였다. 무선채널 기반의 인증 성능을 평가하기 위해 탐지 성공 확률을 성능 평가 지표로 사용하였다.

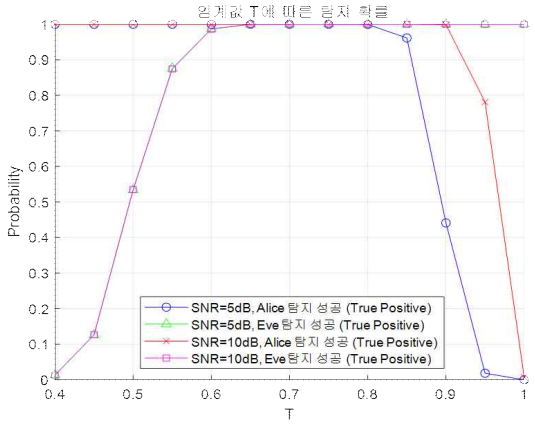

그림 2 T에 따른 인증 성공 확률

그림 2는 송신 신호 대 잡음비(signal-to-noise ratio: SNR)가 10dB, 부반송파 개수는 128, 수신기가 수신한 Alice와 Eve의 상대적 신호 강도는 동일한 상황에서, 임계값(T)에 따른 탐지 확률을 보여주고 있다. T값이 낮을수록 Eve가 Alice로 잘못 탐지되는 오탐율이 증가하였고, SNR값과 무관하게 T값 특정 범위 이상일 경우 Eve를 Alice로부터 정확하게 탐지할 수 있었다. T값이 과도하게 높아진 경우, Alice를 Eve로 잘못 탐지하는 오탐율도 증가하였으나 SNR값이 커지면 Alice에 대한 오탐율이 감소하며, 더 넓은 T의 범위에서 Alice를 올바르게 탐지할 수 있었다.

그림 3은 SNR = 5dB, K = 128로 가정한 상황에서, 수신 세기 비율 변화에 따른 탐지 성공 확률을 보여주고 있다. T값이 낮을수록 Alice의 신호 세기가 Eve보다 적은 상태에서도 Alice를 잘 탐지하였으나, T가 증가하면 Alice의 신호 세기가 Eve의 신호 세기보다 더 크게 요구되는 것을 확인할 수 있다. 반면, 도청자의 경우 합법적인 송수신기 사이의 무선 채널을 통해 합법적인 송수신기간의 킷값을 획득할 수 없으므로 킷값을 무작위 예측 (random guess) 할 수밖에 없는 상황이다. 그로 인해 T값을 너무 낮지 않게 설정하면 Eve를 매우 효과적으로 탐지할 수 있고, 도청자로부터의 공격을 성공적으로 차단할 수 있다.

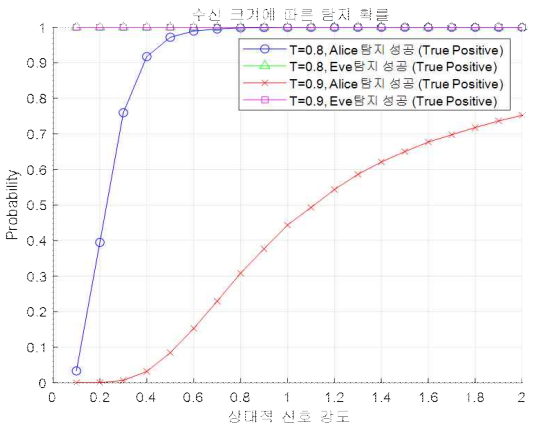

그림 3 상대적 신호 강도에 따른 인증 성공 확률

Ⅳ. 결론

본 연구에서는 TDD 시스템에서 무선 채널 기반의 킷값 생성을 활용한 물리계층 인증 기법을 제안하고, 이 기법의 성능을 평가하였다. 특히, 무선 채널 상호성을 기반으로 생성된 키를 이용하여 합법적인 송신자(Alice)와 도청자(Eve)를 구분하는 과정에서, 임계값 설정이 인증 성능에 미치는 영향을 분석하였다.

ACKNOWLEDGMENT

본 연구는 국립한밭대학교 공학교육혁신센터의 「창의융합형공학인재양성지원사업」의 지원 및 2024년 과학기술정통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음 (2022-0-01068)

참 고 문 헌

[1] 최지환, 김종엽, 주창희, “물리계층 보안 성능 향상을 위한 재밍 조건,” 전자공학회논문지, 제 56권, 2호, pp. 3-9, 2019.

[2] Lee, J., and K. Lee. "Secure communication via untrusted relay with channel estimation error." J. KICS 44.7 (2019): 1295-1298.

[3] X. Lu, J. Lei, Y. Shi, and W. Li, "Improved Physical Layer Authentication Scheme Based on Wireless Channel Phase," *IEEE Wireless Communications Letters*, vol. 11, no. 1, pp. 198-202, Jan. 2022.

[4] 서민재, 권정은, Manjoro Ashleigh Tatenda, 방인규, 김태훈, “TDD 시스템에서 무선 채널 기반 비밀키 공유에 관한 연구,” 한국통신학회 학술대회 논문집, 2023.

[5] I. Bang and T. Kim, "Secure Modulation Based on Constellation Mapping Obfuscation in OFDM Based TDD Systems," in IEEE Access, vol. 8, pp. 197644-197653, 2020.