무선 탈중앙 네트워크에서 물리계층 인증을 위한 OFDM 다중 Tag 신호 삽입 기법

이지민, 한승남, 양재원, 임도현, 황의석*

광주과학기술원

{leejimin0127, snhan0911, wowonyang, latteisacat}@gm.gist.ac.kr, *euiseokh@gist.ac.kr

OFDM-Based Multi-Tag Embedding for Physical-Layer Authentication in Decentralized Wireless Networks

Jimin Lee, Seungnam Han, Jaewon Yang, Dohyeon Lim, Euiseok Hwang

Gwangju Institute of Science and Technology (GIST)

요 약

본 논문은 데이터 신호에 인증 태그를 중첩하여 전송하는 물리계층 인증(physical-layer authentication, PLA) 구조에서 무선 채널의 deep fading과 공격자의 우연적인 인증 통과로 인해 발생하는 신뢰성 저하 문제를 완화하기 위한 OFDM 기반 다중 tag 인증 기법을 제안한다. 기존 PLA 기법에서는 암호학적 hash 함수의 눈사태 효과로 인한 국소적인 복호 오류가 tag 전체의 불일치로 확산되어 높은 오경보율(false-alarm rate, FAR)을 초래할 수 있으며, 단일 tag 구조에서는 공격자가 우연히 인증 조건을 만족시킬 가능성도 존재한다. 제안 기법은 OFDM 환경에서 전송 symbol을 분할하여 서로 독립적인 다중 인증 tag를 생성하고 각 tag에 대해 개별적인 검증을 수행함으로써 일부 tag 오류가 인증 실패로 확산되는 것을 억제하는 동시에, 공격자가 모든 인증 조건을 동시에 만족해야만 인증을 통과할 수 있는 다중 검증 구조를 형성한다. 소프트웨어 정의 무선을 활용한 실험적 분석 결과, 실내 line-of-sight 환경에서 제안 기법은 단일 tag 기반 기법 대비 FAR을 11.99%에서 1.6%로, 미탐지율(miss-detection rate, MDR)을 4.9%에서 0.28%로 감소시킬 수 있다.

Ⅰ. 서 론

무선 탈중앙 네트워크 환경에서는 중앙화된 신뢰 주체 없이 노드 간 통신이 이루어지며, 전송 신호는 개방된 채널을 통해 전달되므로 통신 과정에서 메시지를 인증하는 문제가 중요하게 다루어지고 있다. 상위 계층 메시지 인증 기법은 전송된 메시지의 무결성을 보장하는 데 효과적이지만, 물리계층 신호 처리 이후에 수행되는 구조적 특성으로 인해 필연적인 지연을 수반한다. 지난 몇 년간 이러한 문제를 보완하기 위해, 인증 정보를 물리 신호에 직접 결합하여 수신 신호 처리 과정에서 활용하는 물리계층 인증 기법이 연구되어 왔다 [1-3].

예를 들어, 단일 tag 신호 삽입 기반 물리계층 인증(physical-layer authentication, PLA) [1]은 사전에 키를 공유하는 적법 사용자 Alice와 Bob이 hash 함수를 이용하여 tag 신호를 원본 메시지에 아주 약한 전력으로 삽입하는 방식을 제안하였다. 그러나 [1]에서 제안된 기법은 무선 채널의 deep fading으로 인해 수신 신호의 복호 오류가 발생할 수 있으며, 이러한 미세한 복호 오류가 hash 함수의 눈사태 효과에 의해 tag 불일치로 증폭되어 특정 환경에서 인증 신뢰성이 급격히 저하될 수 있다. 또한, 채널 환경에 따라 도청자가 임의로 생성한 tag 신호가 적법 사용자의 tag 신호와 유사하게 관측되는 경우도 존재할 수 있다.

본 논문에서는 [1]의 기법을 직교 주파수 분할 다중 통신(orthogonal frequency division multiplexing, OFDM)으로 구현하여 deep fading 및 눈사태 효과에 의한 tag 오류에 대처하고, 다중 tag의 삽입과 검출을 통해 인증 신뢰성을 향상시키는 기법을 제안한다. 제안된 기법은 실내 환경에서 소프트웨어 정의 무선을 활용하여 실험적으로 분석되었으며, 공격자 오경보율(false-alarm rate, FAR) 및 미탐지율(miss-detection rate, MDR)을 기준으로 인증 신뢰성을 검증한다.

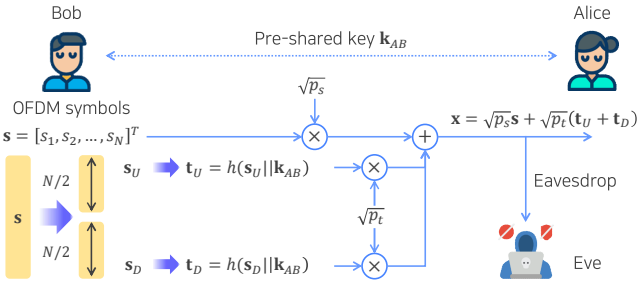

그림 1. 적법 사용자와 도청자로 이루어진 인증 시나리오.

Ⅱ. 시스템 모델

본 논문에서는 그림 1과 같이 적법 사용자 Bob과 Alice가 사전에 대칭키 $\mathbf{k}_{AB}$를 공유하고 있고, Bob이 Alice에게 메시지 인증을 시도하는 시나리오를 고려한다. 이때, 시스템 변수인 메시지 전력 계수 p_s및 인증 tag 전력 계수 p_t는 공개되어 있으며, $p_t \ll p_s$와 $p_t + p_s = 1$를 만족하도록 설정된다. Eve는 무선 채널을 통해 전송 신호를 관측할 수 있으나, $\mathbf{k}_{AB}$에 대한 정보는 알지 못한다고 가정한다. 먼저 Bob은 N개의 부반송파로 구성된 OFDM symbol $\mathbf{s} = [s_1, s_2, \cdots, s_N]^T$를 생성한 뒤, 이를 두 개의 동일한 크기의 부분 벡터 $\mathbf{s}_U = [s_1, s_2, \cdots, s_{N/2}]^T$와 $\mathbf{s}_D = [s_{N/2+1}, \cdots, s_N]^T$로 분할한다. 다음으로, 각 부분 벡터에 대해 Bob은 hash 함수 $h(\cdot)$와 공유 키 $\mathbf{k}_{AB}$를 이용하여 두 개의 인증 tag 신호 $\mathbf{t}_U = h(\mathbf{s}_U \| \mathbf{k}_{AB})$와 $\mathbf{t}_D = h(\mathbf{s}_D \| \mathbf{k}_{AB})$를 생성한다.

마지막으로, 생성된 tag는 전력 계수로 보정되어 원본 OFDM symbol에

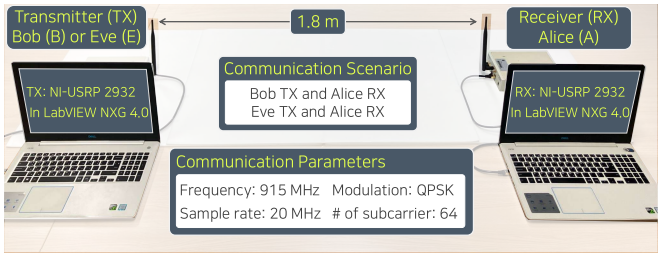

그림 2. 제안 기법의 실험적 분석을 위한 USRP test-bed.

중첩되며, 최종 전송 신호는 다음과 같이 표현된다:

$$\mathbf{x}=\sqrt{p_s}\mathbf{s}+\sqrt{p_t}\,(\mathbf{t}_U+\mathbf{t}_D).$$

수신자 Alice는 채널 등화와 OFDM 복조를 수행하여 $\hat{\mathbf{x}}$및 $\hat{\mathbf{s}}$를 복원한 뒤, 송신 측과 동일하게 $\hat{\mathbf{s}}$를 두 개의 부분 $\hat{\mathbf{s}}_U$ 및 $\hat{\mathbf{s}}_D$로 분할하여 tag 추정 신호 $\hat{\mathbf{t}}_U$ 및 $\hat{\mathbf{t}}_D$를 생성하고, 추정된 각각의 tag 신호에 대해 $\hat{\mathbf{r}}_U=\frac{(\hat{\mathbf{x}}-\sqrt{p_s}\,\hat{\mathbf{s}}-\sqrt{p_t}\,\hat{\mathbf{t}}_U)}{\sqrt{p_t}}$ 및 $\hat{\mathbf{r}}_D=\frac{(\hat{\mathbf{x}}-\sqrt{p_s}\,\hat{\mathbf{s}}-\sqrt{p_t}\,\hat{\mathbf{t}}_D)}{\sqrt{p_t}}$와의 벡터 내적을 부반송파 수로 정규화한 값을 검정 통계량으로 정의한다:

$$\tau_i=\frac{\mathcal{R}e(\hat{\mathbf{r}}_i^T\,\hat{\mathbf{t}}_i)}{N}\quad(i\in\{U,D\}).$$

여기에서 $\mathcal{R}e$는 복소수의 실수 성분을 의미한다. 이 통계량을 기반으로, Alice는 τ_U와 τ_D로 이루어진 2차원 평면에서 신뢰 구간을 고려하여 결정 경계를 정의할 수 있다. 본 논문에서는 MATLAB의 soft margin fitcsvm 함수를 이용하여 결정 경계를 정의한다.

Ⅲ. 제안 기법의 실험적 분석

제안 기법은 그림 2와 같이 실내 환경에서 적법 사용자(A 및 B)와 공격자(E)로 이루어진 무선 통신 환경을 고려하여 실험적으로 분석되었다. 실험은 수신자 (A, 오른쪽)와 송신자 (B 및 E, 왼쪽)가 1.8 m의 거리를 두고 무선으로 통신하는 상황에서 다음의 두 가지 scenario를 수행하는 것으로 구성되는데, 먼저 적법한 인증키 $\mathbf{k}_{AB}$를 가진 송신자 B가 A에게 10,000 packet의 인증 신호를 전송하고 이후 거짓 인증키 $\mathbf{k}_E$를 가진 송신자 E가 A에게 같은 수만큼의 인증 신호를 전송한다. 여기에서는 NI-USRP 2932 두 대와, 이를 운용할 수 있는 LabVIEW NXG 4.0 개발환경이 사용되었다. 변조 방식은 [1]와 같은 QPSK를 채택하고, OFDM 신호 전송이 802.11a 표준에 부합하도록 64개의 부반송파와 20 MHz의 sample rate를 설정하였으나, 실험환경 내의 상용 Wi-Fi 신호들로 인한 간섭을 고려하여 중심 주파수는 연구 및 교육 목적으로 사용할 수 있는 902-928 MHz 대역 중 가운데인 915 MHz로 설정하였다. 이에 따라, 해당 중심 주파수 신호를 전송하기 위해 VERT 900 안테나가 사용되었다.

Ⅳ. 실험 결과

그림 3은 총 10,000개의 수신 패킷에 대해 계산된 두 인증 통계량의 분포와, 이에 기반한 결정 경계를 나타낸다. Bob의 경우 두 통계량이 모두 큰 값을 갖는 영역에 밀집되는 반면, Eve의 경우 원점 근처에 분포하는 경향을 보인다. 이러한 분포 차이로 인해 두 통계량의 2차원 공간에서는 선형 결정 경계를 통해 두 집단을 효과적으로 분리할 수 있음을 확인할 수 있다. 그림 4는 단일 tag 기반 OFDM 인증 기법과 제안된 다중 tag 기반 기법의 인증 오류율을 비교한 결과를 나타낸다. 단일 tag 기법의 경우 FAR 11.99%, MDR 4.9%를 기록하지만, 제안된 다중 tag 기법은 FAR 1.6% 및 MDR 0.28%로 오류율이 감소한 것을 확인할 수 있다.

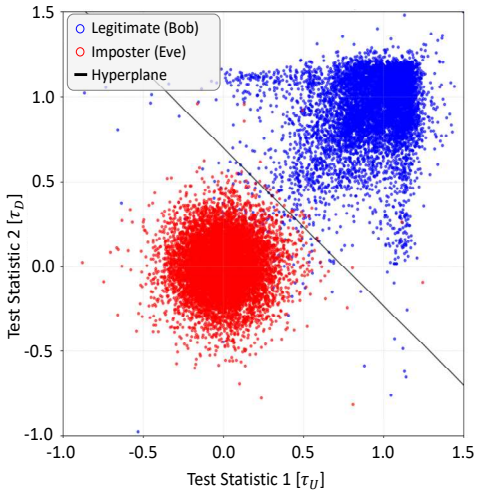

그림 3. 인증 신호 10,000 packets에 대한 검정 통계량 τ_U및 τ_D의 2차원 산점도 분포와 결정 경계면(Hyperplane).

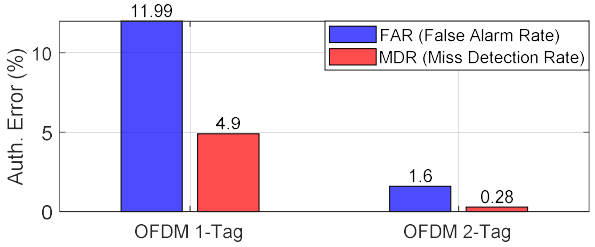

그림 4. 단일 tag와 다중 tag 기반 OFDM 인증 기법의 FAR 및 MDR 비교 결과.

Ⅴ. 결론

본 논문에서는 무선 탈중앙 네트워크 환경에서 PLA의 신뢰성을 향상하기 위해 OFDM 다중 tag 신호 삽입 기법을 제안하였다. 제안한 OFDM 다중 tag 삽입 기법은 deep fading으로 인한 오류의 확산을 억제하는 동시에 다중 인증 구조를 형성함으로써 PLA의 신뢰성 저하를 완화한다. 소프트웨어 정의 무선을 활용한 실내 실험 결과, 제안된 기법은 단일 tag 기반 기법 대비 FAR과 MDR의 측면에서 인증 신뢰성을 유의미하게 향상시킬 수 있음을 확인하였다. 본 연구에서는 이중 tag의 경우를 논의하였지만, 향후 다중 tag의 삽입과 검출을 위해 수반되는 신호처리 비용 대비 인증 신뢰성의 이율에 관해서도 연구할 필요가 있다.

ACKNOWLEDGEMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학 ICT 연구센터(ITRC)의 지원을 받아 수행된 연구임 (IITP-2026-RS-2021-II211835).

참 고 문 헌

[1] G. Verma, P. Yu, and Sadler, B. M. Sadler, “Physical layer authentication via fingerprint embedding using software-defined radios,” *IEEE Access*, vol. 3, pp. 81-88, Jan. 2015.

[2] S. Han, H. Lee, J. Choi, and E. Hwang, “Multi-frequency band physical-layer authentication in indoor environment,” in Proc. *IEEE global communication conference (GLOBECOM)*, Dec. 2023, pp. 1741-1746.

[3] S. Yoon, S. Han, and E. Hwang, “Joint heterogeneous PUF-based security-enhanced IoT authentication,” *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 18082-18096, May 2023.