부 채널 연관 환경에서 무선 채널 기반 물리계층 인증 기법의 보안 취약점 분석

고경연, 한승남, 황의석
광주과학기술원

{ruddus0712, snhan0911, euiseokh}@gist.ac.kr

Security vulnerability analysis of wireless channel based physical layer authentication in correlated subchannels

Kyoungyeon Go, Seungnam Han, Euiseok Hwang
Gwangju Institute of Science and Technology (GIST)

요 약

본 논문은 다중 반송파 전송 시스템에서 무선 채널을 기반으로 하는 물리계층 사용자 인증 기법의 취약점을 분석한다. 일반적으로 무선 채널에서 가정하는 Rayleigh fading 모델은 다중 반송파의 부 채널 주파수 응답을 독립적으로 간주하지만, 실제 환경에서는 서로 연관이 있다. 실제 물리적 환경의 채널 정보를 무선 프로토타이핑 장비를 이용하여 측정하고, 부 채널 연관에 의한 인증키 노출을 확인한다. 실험적 분석 결과, 공격자가 적법한 사용자들 사이에 교환되는 신호를 도청하여 99.05% 확률로 정확한 인증키를 추정하였고, 추정한 인증키를 바탕으로 적법한 사용자를 가장하여 인증을 시도했을 때 수신자 조작 특성 그래프의 넓이는 0.5020 로 확인되었다.

I. 서 론

물리계층 사용자 인증 기법은 무선 통신의 고유한 물리적 정보를 사용하여 사용자를 인증하는 기법으로, 기존의 암호학 기반 인증 기법에 비해 요구되는 연산량이 적다고 알려져 있다. 이러한 이유로, 물리 계층 사용자 인증 기법은 제한된 하드웨어 자원을 보유하는 무선 장치를 위한 인증 기법으로 큰 관심을 받고 있다 [1-3]. PHY-PCRAS (physical-layer challenge-response authentication scheme) [3]는 무선 채널을 활용한 물리계층 기반 사용자 인증 기법 중 하나로, 사용자의 위치에 따라 다르게 측정되는 무선 채널의 위상 응답을 활용하여 적법한 사용자들이 공유하는 인증키를 은닉한다. PHY-PCRAS 의 보안 성능 분석을 진행한 Rayleigh fading 환경에서는 무선 채널의 부 반송파 주파수 응답이 독립적이기 때문에 공격자가 사용자의 신호를 도청해도 인증키를 추정하기 어렵지만, 부 채널 간의 연관이 있는 실제 무선 채널 환경의 경우 공격자가 인증키를 추정할 가능성이 있다.

본 논문에서는 실제 통신 환경에서 부 채널의 연관에 의한 PHY-PCRAS 의 보안 취약점을 분석한다. 이를 위하여 무선 프로토타이핑 장비인 USRP (universal software radio peripheral)를 이용하여 무선 채널 정보를 측정하고, 공격자가 도청한 신호를 이용하여 인증키를 추정할 수 있는지 확인한다. 또한, 공격자가 추정한 인증키를 기반으로 적법한 사용자를 가장하여 인증을 시도했을 때의 인증 성공률을 분석한다.

II. PHY-PCRAS 의 시스템 모델 [3]

그림 1 은 적법한 사용자 Alice (A)와 Bob (B), 그리고 공격자 Eve (E)로 이루어진 PHY-PCRAS 의 시스템 모델을 나타낸다. A 와 B 는 N개의 부 채널을 사용하는 다중 반송

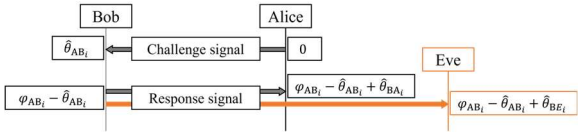


그림 1. PHY-PCRAS 의 시스템 모델과 공격자의 도청

파 전송 시스템에서 사전에 적법한 사용자들에게 분배된 인증키 $\boldsymbol{\varphi}_{\mathrm{AB}} = [\varphi_{\mathrm{AB}_1}, \varphi_{\mathrm{AB}_2}, \cdots, \varphi_{\mathrm{AB}_N}]^T$ $(\varphi_{\mathrm{AB}_i} \in \{0, \pi\})$ 를 공유한다. B 가 A 에게 인증을 요청하면 A 는 B 에게 모든 부 채널의 위상이 0 인 challenge 신호를 송신한다. 이 때, 무선 채널을 통해 송·수신되는 i 번째 부 채널의 주파수 응답은 다음과 같이 표현할 수 있다:

$$h_{\mathrm{AB}_i} = |h_{\mathrm{AB}_i}| e^{j\theta_{\mathrm{AB}_i}} \qquad (i = 1, 2, \cdots N),$$

여기에서 각각 h_{AB_i}는 A 와 B 사이의 채널 주파수 응답, $|h_{\mathrm{AB}_i}|$는 채널 이득, θ_{AB_i}는 채널 위상을 나타낸다. 이 때, B 가 수신한 신호는 다음과 같이 표현할 수 있다:

$$r_{\mathrm{B}_i} = |h_{\mathrm{AB}_i}| e^{j(\theta_{\mathrm{AB}_i} + w_i)} = |h_{\mathrm{AB}_i}| e^{j\hat{\theta}_{\mathrm{AB}_i}},$$

여기에서 각각 w_i는 잡음이고, $\hat{\theta}_{\mathrm{AB}_i}$는 B 가 추정한 채널 위상 정보이다. B 는 추정한 위상 정보를 바탕으로 다음과 같이 인증키를 은닉하여 A 에게 response 신호를 송신한다:

$$s_{\mathrm{B}_i} = e^{j(\varphi_{\mathrm{AB}_i} - \hat{\theta}_{\mathrm{AB}_i})}.$$

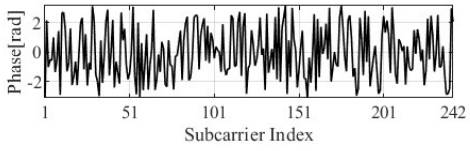
A 가 수신한 B 의 response 신호는 다음과 같이 표현된다:

$$r_{\mathrm{A}_i} = |h_{\mathrm{BA}_i}| e^{j(\varphi_{\mathrm{AB}_i} - \hat{\theta}_{\mathrm{AB}_i} + \theta_{\mathrm{BA}_i} + w_i)},$$

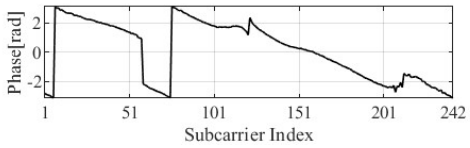
여기에서 채널 호혜성 $(\hat{\theta}_{\mathrm{AB}_i} \approx \theta_{\mathrm{BA}_i} + w_i)$을 기반으로 A 는 검정 통계량 ζ을 다음과 같이 계산한다:

$$\zeta = \left| \sum_{i=1}^{N} r_{\mathrm{A}_i} \cdot e^{j\varphi_{\mathrm{AB}_i}} \right|.$$

이 때, A 는 두 벡터의 내적은 위상이 유사할수록 더 큰 값을 가진다는 성질을 이용하여 검정 통계량의 크기로



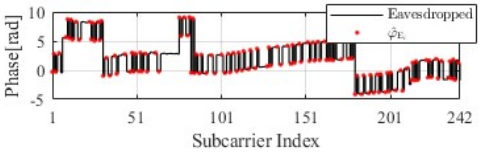
(a)



(b)

그림 2. (a) Rayleigh fading 환경에서의 두 사용자 사이의 채널 위상, (b) 실제 환경에서의 채널 위상

(a)



(b)

그림 3. (a) 인증키의 위상, (b) 실제 통신 환경에서 E 가 도청한 B 의 response 신호와 E 가 추정한 인증키.

사용자의 적법성을 판단한다.

III. USRP 를 이용한 PHY-PCRAS 의 보안 취약점 분석

실제 무선 채널에 의한 PHY-PCRAS 의 보안 취약점을 분석하기 위하여 LabVIEW Communications 소프트웨어의 IEEE 802.11 framework 을 기반으로 동작하는 USRP 를 활용하여 사용자 간의 채널을 측정하였다. 실험에서의 변수는 다음과 같이 설정하였고, 총 2110 번 진행하였다.

표 1. USRP 실험 환경 변수 설정

Bandwidth	80 MHz
# of subcarrier	242
Center frequency	1.0 GHz
Transmission power	20 dBm

그림 2(a)와 그림 2(b)는 각각 Rayleigh fading 채널과 실험을 통해 측정된 두 사용자 사이의 무선 채널을 나타낸다. Rayleigh fading 에서의 채널 위상 정보는 각 반송파에 대해 독립적인 값을 가지기 때문에 인증키를 효과적으로 은닉할 수 있지만, 실제 채널 정보는 부 채널 간 연관이 있으므로 공격자가 다음 수식을 이용하여 인증키를 추정할 수 있다:

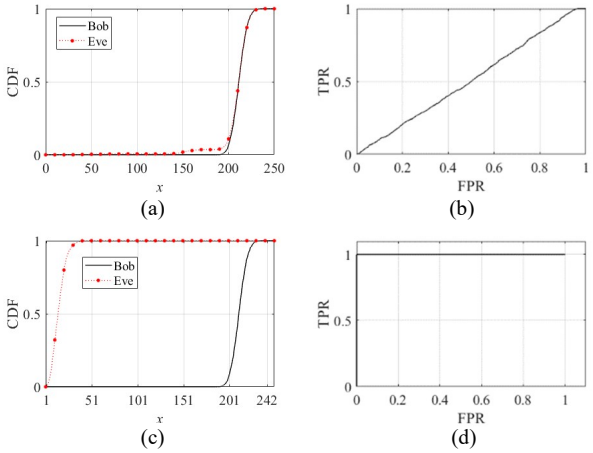
$$|\hat{\varphi}_{\mathrm{E}_i} - \hat{\varphi}_{\mathrm{E}_{i-1}}| = \begin{cases} 0, & \text{if } |\tilde{\theta}_{\mathrm{E}_i} - \tilde{\theta}_{\mathrm{E}_{i-1}}| < 2 \\ \pi, & otherwise \end{cases},$$

여기에서 $\hat{\varphi}_{\mathrm{E}_i}$는 E 가 추정한 A 와 B 사이의 인증키 위상, $\tilde{\theta}_{\mathrm{E}_i}$는 E 가 도청한 B 의 신호의 unwrap 처리한 위상이다. E 가 도청한 B 의 신호는 다음과 같이 표현된다:

$$r_{\mathrm{E}_i} = |h_{\mathrm{BE}_i}| e^{j\left(\varphi_{\mathrm{AB}_i} - \hat{\theta}_{\mathrm{AB}_i} + \theta_{\mathrm{BE}_i} + w_i\right)}.$$

그림 3(a)는 인증키의 위상을, 그림 3(b)는 E 가 도청한 B 의 response 신호와 위 수식을 이용하여 E 가 추정한 인증키를 나타낸다.

실험 결과, E 는 2110 개의 인증키 중 2090 개를 100% 추출하는 데 성공했다. 그림 4(a)는 (b)는 추정한 인증키를 이용하여 PHY-PCRAS 와 동일한 인증 프로토콜을 진행했을 때 B 와 E 의 검정 통계량을 각각 CDF (cumulative distribution function)로 나타낸 것이고, (b)는 ROC (receiver operating characteristics) curve 이다. 그림 4(c)와 (d)는 인증키



(a) (b) (c) (d)

그림 4. (a) E 가 추정한 인증키를 이용하여 인증을 시도했을 때의 CDFs, (b) ROC curve, (c) 인증키 추정 없이 인증을 시도했을 때 CDFs, (d) ROC curve.

추정 없이 인증 프로토콜을 진행했을 때 B 와 E 의 CDF 와 ROC curve 이다. False positive rate (FPR)은 E 를 B 로 판단할 확률, true positive rate (TPR)는 B 를 B 라고 판단할 확률이고, 그래프의 넓이는 0.5020 이다. ROC curve 의 넓이가 0.5 에 가까울수록 A 가 B 와 E 를 구분하지 못한다고 판단할 수 있다.

IV. 결론

본 논문에서는 실제 무선 통신 환경의 부 채널 연관으로 발생하는 무선 채널 기반 물리계층 사용자 인증 기법의 보안 취약점을 실험적으로 분석하였다. 이를 위하여, USRP 를 이용한 무선 통신 실험으로 적법한 사용자들과 신호 도청을 시도하는 공격자를 구현하였다. 실험적 분석 결과, 95% 이상의 확률로 공격자가 도청을 통해 적법한 사용자의 인증키를 정확하게 추정할 수 있고, 추정한 인증키로 적법한 사용자를 가장하여 공격을 시도했을 때 ROC 곡선의 밑넓이가 0.5 에 가까운 공격 성능을 달성할 수 있음을 관찰하였다. 이러한 결과를 통해, PHY-PCRAS 를 실제 통신 환경에서 사용하기에는 적절하지 않다는 것을 확인하였다.

ACKNOWLEDGMENT

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2021-2021-0- 01835) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation), and this work was supported by GIST Research Institute (GRI) grant funded by the GIST in 2023.

참 고 문 헌

[1] PAUL, L. Yu et al., “Physical-layer authentication”, *IEEE Transactions on Information Forensics and Security*, 2008, 3.1: 38-51.

[2] HAN, Seungnam, et al. “Lightweight Physical Layer Aided Key Agreement and Authentication for the Internet of Things”, *Electronics*, 2021, 10.14: 1730.

[3] WU, Xiaofu et al., “Physical-layer authentication for multi-carrier *transmission”, IEEE Communications Letters, 2014, 19.1: 74-77.*