물리계층 보안을 위한 인공 페이딩과 비밀 키 생성에 관한 연구

이규호[1], 서민재[1], 방인규[2]■, 김태훈[1]■

[1]국립한밭대학교 컴퓨터공학과, [2]국립한밭대학교 지능미디어공학과

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

A Study on Artificial Fading and Secret Key Generation for Physical Layer Security

Gyuho Lee[1], Minjae Seo[1], Inkyu Bang[2]■, Taehoon Kim[1]■

[1]Dept. of Computer Engineering, Hanbat National University

[2]Dept. of Intelligence Media Engineering, Hanbat National University

요 약

물리계층 보안은 무선 채널의 무작위성을 활용해 비밀 키를 생성하는 분야이며, 이러한 제한된 연산 능력과 전력 용량 속에서도 데이터의 무결성과 기밀성을 보호하기 위해 적합하다. 본 연구에서는 정적인(static) 채널에서 인공 페이딩을 통해 안정적으로 비밀 키를 생성하는 방안에 대해 연구한다.

Ⅰ. 서론

최근 6G Vision Recommendation이 발표됨에 따라 6G 네트워크의 모습이 점차 구체화되고 있다. 공중 네트워크를 지원하기 위해 드론, 무인 항공기(unmanned aerial vehicle; UAV) 등의 활용방안에 대한 관심이 커지고 있으며, Ubiquitous Connectivity 실현을 위해 사물인터넷(internet-of-things; IoT)에 대한 관심은 여전하다. UAV와 IoT 기기는 무선 네트워크 환경에서 통신하기 때문에 악의적인 공격자로부터 데이터를 지키기 위한 보안 전송이 매우 중요한데, 크기가 작고 경량화된 UAV 또는 IoT 기기에서는 복잡도가 높은 프로토콜 기반의 암호 체계를 적용하는데에는 한계가 있을 수 있다.

물리계층 보안은 무선 채널의 무작위성(randomness)을 활용해 비밀 키를 생성하는 분야이며, 이러한 제한된 연산 능력과 전력 용량 속에서도 데이터의 무결성과 기밀성을 보호하기 위해 적합하다. 하지만, 무선 통신 환경이 정적인(stationary) 경우 무작위성이 감소하여 비밀키를 생성하는 것에 어려움이 있을 수 있다 [2]. Aldaghri와 Hessam는 인공 페이딩(artificial fading; AF)이라는 개념을 제안하여 이러한 문제를 극복하고자 한 바 있다. 본 연구에서는 인공 페이딩을 적용하고 수신 신호 강도(received signal strength; RSS)를 활용한 비트 추출과 SHA-256을 사용해 비밀 키를 생성하는 방안에 대해 연구한다.

Ⅱ. 본론

합법적인 사용자 Alice와 Bob, 수동적인 공격자 Eve가 OFDM 신호를 송수신하는 통신 환경을 고려하며 Alice는 OFDM 심볼에 프리앰블을 추가하여 Bob에게 전송한다. 이때, 비밀 키의 암호 강도를 강화하고 중복 키 생성을 방지하며 합법적인 사용자와 공격자 사이의 채널 상관관계를 저하시켜 공격자가 사용자의 채널을 정확하게 추정할 수 없도록 채널의 무작위성을 증가시키기 위해 미리 생성해둔 인공 페이딩 $\dot{H}$를 적용하여 전송한다. 수신기에서의 수신 신호는 $y = H\dot{H}x + w$로 표현되며, H는 Rician Fading 채널의 계수이고 w는 백색 가우시안 잡음이다. 합법적인 사용자는 인공 페이딩 계수를 이미 알고 있다고 가정하고 있으므로 수신기는 프리앰블에서 채널 계수를 정확하게 추정할 수 있지만, 공격자는 수신 신호에서 인공 페이딩 계수를 제거할 수 없어 채널 계수를 정확하게 추정할 수 없다. 채널 계수가 추정되면 RSS에서 비밀 키 생성에 사용할 비트를 추출할 수 있다 [1]. $|y|$를 내림차순으로 정렬하고 임계값(z^-,z^+)를 기준으로 z^-보다 작은 값과 z^+보다 큰 값을 제외한 나머지 값을 제거하고, z^+보다 큰 값은 1로 z^-보다 작은 값은 0으로 변환한다. 마지막으로 정렬했던 값들을 원래 순서로 복원하면 비트 추출이 마무리된다. 이렇게 추출한 비트 스트림을 SHA-256 해시 함수를 적용하여 프라이버시를 증폭해 비밀 키로 사용할 수 있다.

Ⅲ. 결론

정적 채널에서 안전한 비밀 키 생성을 위해 AF를 적용하고 비트 추출과 SHA-256을 활용한 비밀 키 생성 방안에 대해 연구했다. 사용자 사이의 비트 추출 결과는 유사하지만 공격자의 경우 큰 차이가 발생하는 것을 확인 할 수 있었다. 하지만 송수신기 사이의 비트 추출 결과가 같아야 비밀 키 생성에 사용할 수 있기 때문에 잡음에 의해 발생하는 에러 비트의 정정(correction) 정확도가 전체 성능을 크게 좌우할 것이다.

ACKNOWLEDGMENT

본 연구는 2024년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음 (2022-0-01068)

참 고 문 헌

[1] Assaf, Tasneem, *et al.,* "High-rate secret key generation using physical layer security and physical unclonable functions." in IEEE Open Journal of the Communications Society, vol. 4, pp. 209-225, 5 Jan 2023

[2] N. Aldaghri and M. Hessam, "Fast secret key generation in static environments using induced randomness." in 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, Dec 2018.

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