논문 21-46-02-09 The Journal of Korean Institute of Communications and Information Sciences '21-02 Vol.46 No.02
https://doi.org/10.7840/kics.2021.46.2.261

# 물리계층 보안을 위한 채널 반전 기반의 변조 난독화 기법

방 인 규◆, 김 태 훈*

# Channel Inversion Based Modulation Obfuscation Scheme for Physical-Layer Security

Inkyu Bang◆, Taehoon Kim*

요 약

본 논문에서는 무선 송신기, 무선 수신기, 무선 도청기가 존재하는 무선 도청 네트워크에서 채널 반전 기반의 보안 변조 기법을 제안한다. 제안 기법은 데이터 전송 전에 송신기와 수신기 사이의 무선채널을 측정하고 이를 비밀 키 값 전송에 사용한다. 전송된 비밀 키 값은 데이터 전송의 변조 과정에서 성상도를 난독화하는데 사용된다. 모의실험을 통해 제안 기법의 비밀 키 전송 및 변조 난독화에 대한 보안 성능을 각각 보안 중단 확률 및 비트 오류율 관점에서 평가한다.

**Key Words** : wireless security, physical-layer security, modulation, obfuscation

ABSTRACT

In this paper, we propose a channel inversion based modulation obfuscation scheme in wiretap networks. The proposed scheme shares secret value during the channel estimation and utilizes it to obfuscate locations of constellation points. Through simulations, we verify the secrecy performance of the proposed scheme in terms of secrecy outage probability and BER (bit error rate).

## Ⅰ. 서 론

5G로 대표되는 차세대 이동통신 표준의 상용화와 함께 다양한 기기를 활용한 무선통신은 일상생활의 필수 요소가 되었다. 그러나 다양하고 많은 무선 기기의 사용은 여러 무선 보안 문제를 초래하였고 무선 네트워크 보안의 필요성이 더욱 대두되고 있다. 물리계층 보안(physical-layer security)은 무선 네트워크 보안 문제를 정보이론 관점에서 접근하는 연구 분야로써 주목을 받고 있다.

일반적으로 물리계층 보안에서는 송신기, 수신기와 함께 도청기가 동시에 존재하는 무선 네트워크 환경을 가정한다. 최근에는 다중(MIMO) 안테나 기술, 다중 사용자 다양성(multiuser diversity) 등을 활용한 물리계층 보안 연구가 많이 진행되고 있다[1-3]. 기존 연구에서는 특정 물리계층 기술이 사용되었을 때 무선통신 시스템의 보안 전송률(secrecy rate), 보안 중단 확률(secrecy outage probability)등을 분석하였다. 기존 연구들은 정보이론 관점에서 상세한 분석 결과를 제공하지만, 실제 무선통신 시스템에 적용 가능한 보안성이 높은 통신 방법(예: 변조/복조)에 대해서는 구체적으로 논의하지 않고 있다.

본 논문에서는 채널 반전(channel inversion) 기반의 보안 변조(modulation) 기법을 제안한다. 송신기와 수신기는 파일럿을 통해 채널을 추정하고 여기서 측정된 채널 계수는 송신기와 수신기 사이의 비밀 키(secret key) 공유를 위해 사용된다. 송신기는 공유된 비밀 키 값을 이용하여 변조 시에 사용되는 성상도(constellation)를 난독화(obfuscation)하고 수신기는 같은 키 값을 이용하여 난독화된 성상도를 복호한다. 최종적으로 모의실험을 통해, 제안 기법의 성능을 보안 중단 확률 및 비트 오류율(bit error rate 또는 BER) 관점에서 평가한다.

## Ⅱ. 시스템 모델

본 논문에서는 그림 1과 같이 무선 송신기(Alice)와 무선 수신기(Bob)로 구성된 TDD (time duplex division) 무선통신 시스템에서 무선 도청기(Eve)가

※ 이 논문은 2019학년도 한밭대학교 교내학술연구비의 지원을 받았음.(This research was supported by the research fund of Hanbat National University in 2019)
◆ First Author : (ORCID:0000-0001-7109-1999) Hanbat National University Department of Information and Communication Engineering, ikbang@hanbat.ac.kr, 조교수, 정회원
* Corresponding Author : (ORCID:0000-0002-9353-118X) Hanbat National University Department of Computer Engineering, thkim@hanbat.ac.kr, 조교수, 정회원
논문번호 : 202011-289-A-LU, Received November 20, 2020; Revised Deccember 24 2020; Accepted Deccember 29, 2020

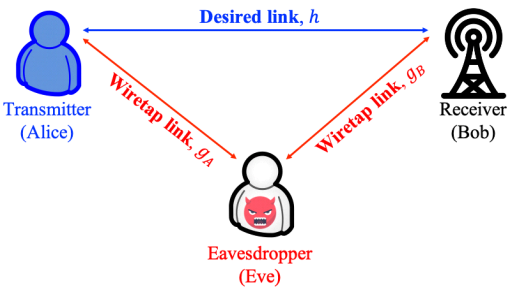


그림 1. 무선 송신기(Alice), 무선 수신기(Bob) 및 무선 도청기(Eve)가 존재하는 도청 네트워크 모델
Fig. 1. A wiretap network which consists of a wireless transmitter (Alice), a wireless receiver (Bob), and a wireless eavesdropper (Eve)

존재하는 기본적인 도청 네트워크 모델을 가정한다. 송신기는 매 시간 슬롯(time slot)마다 새롭게 데이터를 전송할 수 있다. 하나의 시간 슬롯은 다음의 세 단계 (1) 채널추정을 위한 파일럿(pilot) 전송(Alice → Bob), (2)비밀 키 전송(Bob → Alice), (3) 비밀 키 값에 따른 변조 난독화 및 데이터 전송(Alice → Bob)으로 구성된다. 이는 3장에서 자세히 논의한다.

$h$는 송신기와 수신기 사이의 주요 무선링크의 채널 계수를 나타내며, $g_A$, $g_B$는 도청기와 송신기 및 도청기와 수신기 사이의 도청링크의 채널 계수를 각각 나타낸다. 각 채널 계수는 독립 가우시안 분포를 따르는 레일리 블록 페이딩 채널 모델을 가정한다. 즉 $h \sim CN(0,\sigma_h^2)$, $g_A \sim CN(0,\sigma_{g_A}^2)$, $g_B \sim CN(0,\sigma_{g_B}^2)$이 된다. 여기서 $\sigma_h^2$, $\sigma_{g_A}^2$, $\sigma_{g_B}^2$는 각 무선링크의 평균 채널 이득이 값을 나타낸다. 각 채널계수($h$, $g_A$, $g_B$)는 하나의 시간 슬롯 동안은 변하지 않으며 매 시간 슬롯마다 독립적으로 변한다. Alice가 $x$을 전송할 때, 수신기와 도청기의 수신 신호는 다음과 같다.

$$y_B = hx + n_B, \tag{1-1}$$
$$y_E = g_A x + n_E, \tag{1-2}$$

여기 아래첨자 B, E는 Bob, Eve를 대표하며, 변수 $n$은 가산 백색 가우시안 잡음(AWGN)을 나타낸다. 분석의 편의상 단일 안테나를 기준으로 설명하였으나, maximum ratio combining (MRC) 기술 등을 활용할 경우 (Bob과 Eve의) 다중 수신 안테나의 경우로 자연스럽게 확장이 가능하다.

## Ⅲ. 채널 반전 기반의 변조 난독화 기법

본 논문에서 제안하는 채널 반전 기반의 변조 난독화(Channel Inversion based Modulation Obfuscation 또는 CIMO) 기법은 다음 세 단계로 구성되며, 매 시간 슬롯마다 반복된다.

### 3.1 채널추정

Alice는 채널추정을 위해 미리 설계된 파일럿 신호 $p$을 Bob에게 전송한다. Bob은 수신신호와 $p$의 관계를 이용하여 Alice와 채널 값 $h$을 추정한다.(Eve 역시 동일한 방법으로 $g_A$을 추정할 수 있다.) 단, 채널 추정오류는 없다고 가정한다.

### 3.2 비밀 키 전송

Bob은 변조 난독화에 사용될 비밀 키 값 $s$을 Alice와의 채널 값 $h$의 역수와 곱하여(즉, $x = s/h$) 전송한다. Alice와 Eve의 수신 신호는 다음과 같다.

$$y_A = h\left(\frac{s}{h}\right) + n_A = s + n_A, \tag{2-1}$$
$$y_E = g_B\left(\frac{s}{h}\right) + n_E, \tag{2-2}$$

여기서 송신 전력이 충분히 크다고 가정했을 때(즉, $n_A = n_E = 0$), Alice는 채널반전 효과로 인해 비밀 키 값 $s$을 바로 수신한다. 반면, Eve는 $s$값에 $1/h$와 $g_B$ 값이 곱해진 값을 수신한다. Eve는 채널추정 단계에서 $g_A$값은 측정할 수 있지만, 다른 채널 값인 $h$와 $g_B$ 값은 측정할 수 없으며, 이 값들은 복소수이기 때문에 추측도 매우 어렵다. Eve 입장에서 $s$ 값 추측에 대한 확률은 4장에서 구체적으로 논의한다. Alice는 안정적인 $s$ 값의 무선 전송을 위해 QPSK 변조와 LDPC 채널코딩 등을 이용할 수 있다. 또한 채널반전 효과로 인해 $h$ 값에 따라 순간 전송 전력이 증가하는 단점이 발생한다. 여기서, 평균 전송 전력 제약 하에 순간 전송 전력의 제약은 없다고 가정한다.

### 3.3 변조 난독화 전송 및 복조(demodulation)

Alice는 Bob으로부터 수신한 비밀 키 값 $s$을 이용하여 전송 데이터의 변조에서 사용되는 성상도를 난독화한다. 예를 들어, QPSK 변조 방식에 그레이 코드(Gray code)가 사용되었을 경우, 성상도의 제 1~4 사분면의 각 점에는 '11', '01', '00', '10'에 해당하는 데이터 비트가 고정으로 할당된다. 그러나 난독화가

적용되면 같은 변조 방식을 사용하더라도 $s$값에 따라 성상도의 각 점에 할당되는 데이터 비트가 달라진다. 같은 QPSK를 사용하더라도 서로 다른 $s_1$, $s_2$ 값에 따라 성상도의 제 1 사분면에 '11' 또는 '00'도 할당될 수 있다. 성상도의 각 점에 할당되는 데이터 비트가 $s$값에 따라 무작위로 바뀌기 때문에, $s$값을 알고 있는 Bob은 Alice가 전송한 데이터를 올바르게 복조할 수 있다. Eve는 $s$값을 모르기 때문에 모든 성상도 조합을 복조에 시도해야 데이터를 복조할 수 있다. 예를 들어, QPSK의 경우 총 $4! = 16$개의 조합만이 존재하기 때문에 Eve는 쉽게 데이터 도청이 가능하다. 그러나 16-QAM, 64-QAM의 경우 $16! \approx 2.0 \times 10^{13}$, $64! \approx 1.2 \times 10^{89}$개의 조합이 존재한다. 따라서 CIMO 기법은 높은 차수의 변조 기법과 함께 사용될 경우 계산 복잡도에 의한 보안을 제공할 수 있다.

## Ⅳ. 성능 평가

그림 2는 CIMO 기법의 2단계에서 비밀 키 값 $s$을 전송할 때 발생할 수 있는 주요 링크의 SNR 변화에 따른 보안 중단 확률(보안 전송률이 $R_0$보다 작을 확률로 정의)의 결과이다. CIMO 기법에서는 $R_0 = 0$의 값을 사용하여 $s$값에 대한 일부 정보도 노출되지 않을 확률을 나타내도록 하였다. 즉, Eve 입장에서 $s$ 값 추정 확률의 상한을 나타낸다. 모의실험을 위해 $\sigma_h^2 = \sigma_{g_B}^2 = 0$dB (즉, Alice와 Eve는 Bob으로부터 거리가 동일), 도청 링크의 SNR은 0dB로 설정하였다. 주요 링크의 잡음이 반영된 SNR 증가에 따라 $s$값의 노출 확률이 줄어드는 것을 확인할 수 있다.

그림 3은 CIMO 기법의 3단계에서 16-QAM 기반의 변조 난독화가 적용되었을 때, 주요 링크의 잡음이 반영된 SNR 변화에 따른 Bob (2개 안테나)과 Eve (4

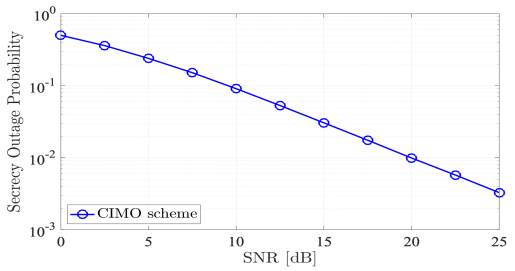


그림 2. $R_0 = 0$ bps/Hz일 때 주요 무선링크 SNR 변화에 따른 CIMO 기법의 보안 중단 확률
Fig. 2. Secrecy outage probability os CIMO scheme for varying main link's SNR when $R_0 = 0$ bps/Hz

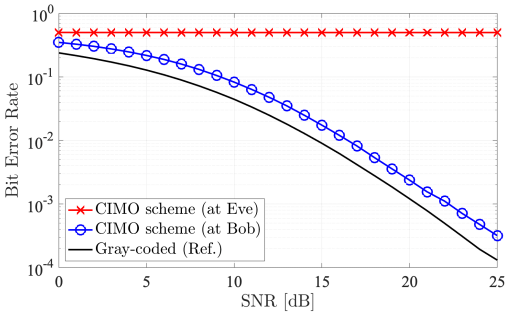


그림 3. CIMO 기법의 BER 성능 대 SNR
Fig. 3. BER performance of CIMO scheme vs. SNR

개 안테나)의 BER 결과이다.(즉, 강력한 Eve 시나리오) 앞서 논의한 것처럼 Eve는 $s$값을 유추할 수 없기 때문에 임의 추측에 가까운 0.5의 BER 성능을 가진다. 반면 Bob은 $s$값을 이용하여 일반적인 BER 성능을 달성할 수 있다. CIMO 기법은 Gray-coded 결과와 비교했을 때, 난독화의 결과로 항상 최적의 bit-symbol 매핑을 보장하지 않기 때문에 BER 성능 열화가 존재한다. 그러나 BER이 아닌 symbol error rate 관점에서는 두 결과가 동일한 성능을 보인다.(공간 제약으로 결과 생략)

## Ⅴ. 결 론

본 논문에서 채널 반전 기반의 보안 변조 기법(CIMO)을 제안하였다. 제안 기법은 채널 반전 효과를 이용해 비밀 키를 안전하게 전송하고 변조 난독화를 통해 계산 복잡성 기반의 보안을 달성할 수 있다.

## References

[1] S. H. Chae, I. Bang, and H. Lee "Physical layer security of QSTBC with power scaling in MIMO wiretap channels," *IEEE Trans. Vech. Tech.*, vol. 69, no. 5 pp. 5647-5651, May 2020.

[2] I. Bang, S. M. Kim, and D. K. Sung "Artificial noise-aided user scheduling from the perspective of secrecy outage probability," *IEEE Trans. Vech. Tech.*, vol. 67, no. 8 pp. 7816-7820, Aug. 2018.

[3] I. Bang, B. C. Jung, and D. K. Sung, "A power control scheme for improving secrecy rate in multi-cell uplink networks," *J. KICS*, vol. 42, no. 1, pp. 39-41, Jan. 2017.