

군사 환경에서의 향상된 무선 네트워크 보안

김진우*, 신수용°

Enhanced Wireless Network Security in Military Environments

Jin Woo Kim*, Soo Young Shin°

요약

본 논문은 합법적 수신자와 불법적인 도청자가 함께 존재하는 Wire-Tap 채널 모델 하에서 HT-STBC (Hadamard Transformed-Space Time Block Codes)와 인위적 잡음 (Artificial Noise)을 이용한 보안 성능 향상 방법을 제안한다. 기존의 STBC와 인위적 잡음을 이용한 방법은 QPSK 이상의 변조 방식을 사용했을 때 수신자와 도청자 사이의 BER (Bit Error Rate) 차이가 제한적으로 증가하는 문제가 있다. 이를 해결하기 위해 Hadamard 변환과 STBC를 결합한 HT-STBC와 인위적 잡음을 이용하여 수신자의 BER을 기존 방법보다 감소시키고 수신자와 도청자 사이의 BER 차이 또한 증가함을 모의실험을 통해 입증하였다. 모의실험 결과, 본 논문에서 제안한 방법을 이용하면 기존의 STBC와 인위적 잡음을 이용한 방법에 비하여 약 3dB의 성능이 향상됨을 확인하였다.

Key Words : Physical layer, STBC, Hadamard transform, Artificial noise, MIMO

ABSTRACT

In this paper, we propose method to enhance security performance using HT-STBC with artificial noise under Wier-Tap channel model that exist with legitimate receiver and illegal eavesdropper. Conventional STBC with artificial noise scheme has a weakness that a limited increase in the BER of the difference between the receiver and an eavesdropper, when used over QPSK modulation. To solve this problem, we suggest HT-STBC combining hadamard transform and STBC with artificial noise for reduce BER of receiver than the conventional scheme and demonstrated through simulation that also increased BER difference between the receiver and an eavesdropper. By the simulation results, when used proposed scheme, showed approximately 3dB improvement in performance compared to the conventional scheme.

1. 서론

최근 무선 네트워크의 급격한 보급으로 인해 무선 인터넷 없는 생활은 상상할 수도 없게 되었다. 하지만 이와 더불어 무선 네트워크의 보안 역시 심각한 문제로 대두되고 있다. 전통적 관점의 보안은 주로 DES (Data Encryption Standard)와 같은 상위 계층에서의 정보 암호화를 뜻한다^[1]. DES는 데이터를 주고받는

두 유저가 서로 암호화 키를 가지고 있어야 성립하는데, 만약 암호화 키를 가지고 있지 않다면 키 교환을 위한 보안 채널이 필요하다. 물리 계층에서의 보안은 이러한 보안채널 제공을 통해 특정 장소나 장치를 이용하였을 때 보안을 제공하고 기존의 상위계층에서의 보안을 보완한다. 특히 기존의 상위 계층에서 보안과 달리 기존의 물리 계층 통신 기술들을 보안 목적으로 활용하기 때문에 추가적인 장비 또는 비용을 절약할

* 이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2015R1D1A1A01061075)

• First Author : Department of IT Convergence Engineering, Kumoh National Institute of Technology, rerua@kumoh.ac.kr, 학생회원

° Corresponding Author : Kumoh National Institute of Technology, wdragon@kumoh.ac.kr, 종신회원

논문번호 : KICS2016-09-246, Received September 5, 2016; Revised November 1, 2016; Accepted November 1, 2016

수 있다^[2]. 이러한 특징 때문에 최근에는 물리 계층에서의 보안에 대한 연구 또한 활발히 이루어지고 있다^[1].

참고문헌^[1]에서 물리 계층에서의 보안은 크게 이론적 보안 용량 (Theoretical Secure Capacity), 파워, 코드, 채널 그리고 신호 감지의 5가지 분야로 나눌 수 있다고 제안하였다. 특히 이론적 보안 용량 분야에서는 Shannon이 처음 완벽한 보안 (Perfect Secrecy)^[3]의 개념을 제시하였고, 참고문헌^[3]의 완벽한 보안 개념을 이용하여 1975년 Wyner가 합법적인 송신자와 수신자 그리고 도청자로 이루어진 Wire-Tap 채널 모델을 제안하였다^[4]. Wire-Tap 채널 모델에서 합법적인 사용자들은 주 채널을 이용하여 통신을 하고, 도청자는 주 채널에 비해 열화 된 채널을 이용한다.

인위적 잡음(Artificial Noise)은 무선통신 시스템에서의 물리 계층 보안을 향상시키는 방법 중 하나이다^[5]. 기본적인 원리는 인위적 잡음을 송신 신호에 더하여 도청자의 채널 환경을 나쁘게 만들고, 합법적 수신자의 채널엔 영향을 끼치지 않는 것이다. 이를 위해 인위적 잡음의 값은 수신자의 채널 정보를 기반으로 만들어 지고, 각 수신자 측에서는 인위적 잡음을 제거하고 신호를 수신하여 결론적으로 수신자의 BER (Bit Error Rate)에는 영향을 미치지 않는다. 반면 도청자 측에서 인위적 잡음은 일반적인 잡음으로 작용하는데, 이는 수신자와 도청자의 채널의 상태가 서로 다르기 때문이다.

국방 분야에서 또한 사이버 국방, 네트워크 중심 전 (Network Centric Warfare)의 분야에서 무선 네트워크 사용이 증가함에 따라 보안이 중요한 문제로 주목 받고 있다^[6,7]. 하지만 기존의 보안체제로 증가하는 보안 위협에 대응하기 위해서는 비용 증가, 새로운 설비 보강 등의 문제를 동반하기 때문에^[8] 이를 보완하기 위해 기존의 장비를 그대로 사용하면서도 보안을 강화시킬 수 있는 물리 계층 보안 방법을 참고문헌^[9]에서 제안하였다. 참고문헌^[9]에서는 STBC (Space-Time Block Code) 의 Diversity 이득과 인위적 잡음을 이용하여 보안을 강화시키는 방법을 제안하였다. 하지만 STBC와 인위적 잡음을 이용한 방법은 QPSK 이상의 변조 방식에서는 수신자와 도청자 간의 BER 차이가 제한적으로 증가하는 단점이 있다. 따라서 본 논문에서는 위 단점을 개선하고 기존의 방법보다 개선된 보안 성능을 갖는 hadamard 변환과 STBC를 결합한 HT-STBC와 인위적 잡음을 이용한 기법을 제안한다. HT-STBC는 hadamard 변환으로 인해 수신자 측에서는 기존과 같이 신호를 복조할 수 있지만, 도청자 측에서는 신호가 hadamard 변환 된 것을 알 수 없기 때

문에 기존과 같이 복조를 시도하게 된다. 즉, 심볼이 암호화되는 것과 같은 효과를 가지게 된다. 따라서 도청자 측 채널에선 BER이 크게 증가하게 되고, 수신자는 기존보다 감소된 BER을 가지게 되어 시스템의 전체적인 보안 성능이 향상되게 된다.

본 논문의 구성은 아래와 같다. 2장은 관련 연구로써 Alamouti Code와 Hadamard 변환, 그리고 Artificial Noise에 대해 설명하고, 3장에서 시스템 모델을 제시한다. 그리고 4장에서는 모의실험을 통해 제안된 방법의 성능을 확인하고, 5장에서는 결론을 기술한다.

II. 관련 연구

2.1 Alamouti Code

Alamouti 코드는 Full-rate, Full diversity를 만족하는 STBC로 송신 다이버시티에 의해 향상된 BER 성능을 갖는 전송 방법이다^[10].

그림 1은 2개의 송신안테나를 가정하였을 때의 심볼 블록도이다. 첫 타임 슬롯에서는 각 송신 안테나가 심볼 s_1 과 s_2 를 전송한다. 그리고 다음 타임 슬롯에서는 각각 $-s_2^*$, s_1^* 를 전송한다. 이때 수신 안테나는 1개로 가정한다. *는 공액 복소 연산이며, 수신된 신호 r_i 는 다음과 같이 표현할 수 있다.

$$r_1 = h_1s_1 + h_2s_2 + n_1 \tag{1}$$

$$r_2 = -h_1s_2^* + h_2s_1^* + n_2 \tag{2}$$

여기서 r_i 는 i 번째 타임 슬롯에서 수신된 신호이고, h_j 는 j 번째 송신 안테나에서 전송된 신호의 채널이다. n_i 는 i 번째 타임 슬롯에서의 AWGN (Additive White Gaussian Noise)이다.

MRRC (Maximal Ratio Receiver Combining) 방식을 이용하여 수신된 신호 r_i 로부터 원 신호 s_1 , s_2 를 검출할 수 있다. 이때 원 신호 s_1 , s_2 를 간단한 선형 계산으로 검출 가능함을 식 (3),(4)를 통해 알 수 있다.

$$\begin{aligned} \tilde{s}_1 &= h_1^*r_1 + h_2r_2^* \\ &= h_1^*(h_1s_1 + h_2s_2 + n_1) + h_2(-h_1^*s_2 + h_2^*s_1 + n_2^*) \\ &= (|h_1|^2 + |h_2|^2)s_1 + h_1^*n_1 + h_2n_2^* \end{aligned} \tag{3}$$

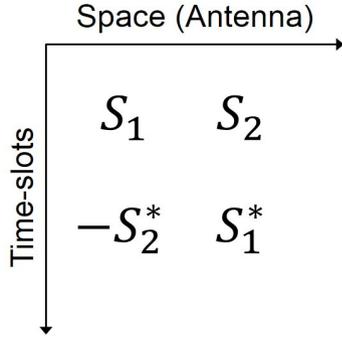


그림 1. 2개의 송신안테나를 이용하였을 때 Alamouti 코드의 심볼 블록도
Fig. 1. Symbol block diagram of Alamouti code using 2 transmit antennas

$$\begin{aligned} \tilde{s}_2 &= h_2^* r_1 - h_1^* r_2 \\ &= h_2^* (h_1 s_1 + h_2 s_2 + n_1) - h_1^* (-h_1^* s_2 + h_2^* s_1 + n_2^*) \\ &= (|h_1|^2 + |h_2|^2) s_2 + h_2^* n_1 - h_1^* n_2^* \end{aligned} \tag{4}$$

Alamouti 코드는 높은 BER 성능을 가지면서 간단한 선형 계산으로 신호를 검출 가능하기 때문에 LTE를 비롯해 여러 부분에서 활용되고 있다.

2.2 Hadamard 변환

Hadamard 변환은 일반화된 Fourier 변환의 한 종류로 직교성, 대칭성, 대합성 등의 특성을 가진다^[11]. Hadamard 변환식은 일반적으로 아래와 같이 나타낼 수 있다.

$$y = Hx \leftrightarrow x = Hy \tag{5}$$

위 식에서 H 는 hadamard 행렬, x 및 y 는 입력, 출력 행렬이다.

행렬 x 에 hadamard 행렬 H 를 곱하면 행렬 y 를 얻을 수 있는데, 이는 hadamard 행렬을 다시 곱하면 원래 신호를 다시 복구할 수 있음을 뜻한다. 이때 hadamard 행렬을 (k, n) 크기라 하면 아래의 식 (6),(7),(8)과 같이 정의할 수 있다. 여기서 m 은 hadamard 행렬의 차수이다.

$$(H_m)_{k,n} = \frac{1}{\sqrt{m}} (-1)^{\sum_i k_i n_i} \tag{6}$$

$$k = \sum_{i=0}^{m-1} k_i 2^i = k_{m-1} 2^{m-1} + k_{m-2} 2^{m-2} + \dots + k_1 2 + k_0 \tag{7}$$

$$n = \sum_{i=0}^{m-1} n_i 2^i = n_{m-1} 2^{m-1} + n_{m-2} 2^{m-2} + \dots + n_1 2 + n_0 \tag{8}$$

아래의 식을 통해 $m = 2$ 인 경우와 일반화된 hadamard 변환식을 확인할 수 있다.

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, H_m = \begin{bmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{bmatrix} (m > 0) \tag{9}$$

Hadamard 변환에서 PSK나 QAM 신호의 complex constellation 점을 c 라 하면, hadamard 변환으로부터 다음의 식을 얻을 수 있다.

$$\vec{s} = H_m \vec{c}, \vec{c} = [c_1 \ c_2]^T \tag{10}$$

여기서 $(.)^T$ 는 전치행렬을 의미한다.

식 (10)과 같이 hadamard 변환된 신호는 complex constellation의 신호 검출 영역이 확장되게 되어 신호의 검출률이 증가하게 되고, 이는 BER의 감소로 이어진다^[12].

2.3 Artificial Noise

인위적 잡음은 물리적 계층의 보안 방법 중 하나로 신호에 인위적인 잡음을 추가하여 불법적인 수신자의 수신율을 저하시키는 방법이다. 불법적 수신자의 경우에도 채널 정보를 수집하는 것이 가능하기 때문에 변조 방법이나 통신 방법을 확보한 경우에는 도청이 가능하다. 그러나 인위적 잡음을 이용하면 이러한 정보들이 노출될지라도 보안을 강화시킬 수 있다. 또한 인위적 잡음을 이용하면 기존의 장비를 변경·추가하지 않고도 보안을 강화시킬 수 있는 장점이 있다.

참고문헌^[13]에서는 SISO와 MIMO 채널 모델인 경우에 Diversity가 미치는 영향과 Relay 전송 모델에서 인위적 잡음이 보안 성능에 미치는 영향을 중심으로 평가하였다. 그리고 참고문헌^[14]에서는 최적 전력 분배를 이용하여 개선되는 보안성능을 평가하였다.

기존의 연구들은 외부적인 요소나 최적 전력 분배와 같은 복잡한 연산이 필요하지만 본 논문에서 제안하는 HT-STBC를 이용한 방법은 기존 방법 대비 간단한 연산만으로도 Diversity 이득을 얻는 것이 가능하다.

III. 시스템 모델

3.1 정찰 임무 시나리오

본 논문에서는 아군이 적 지역으로 정찰 침투 임무 중의 상황을 가정하였다. 이때 적의 도청자는 Eve, 아군의 수신자는 Bob, 그리고 통신을 시도하는 아군은 Alice이다. 그림 2와 같이 적 지역에서 아군과 통신을 시도한다면 도청자가 아군의 신호를 도청할 수 있다. 만약 Eve가 도청에 성공한다면 Alice의 위치 및 목적이 발각되게 되고 이는 임무의 성패뿐만 아니라 Alice의 생존 문제와도 직결된다. 이를 막기 위해 본 논문에서는 물리적 계층을 이용한 향상된 무선 네트워크 보안을 제공하는 방법을 제안하였다.

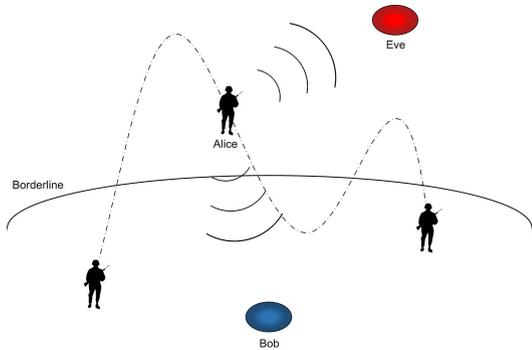


그림 2. 정찰 임무 시나리오
Fig. 2. Scenario of reconnaissance mission

3.2 채널 모델

본 논문에서는 인위적 잡음을 이용하여 도청자가 수신자에 비해 높은 BER을 갖는 HT-STBC를 이용한 전송 방법을 제안한다. 이를 위해 송신자와 합법적 수신자, 그리고 도청자를 갖는 Wire-Tap 채널 모델^[4]을 가정하였다. 이때 Alamouti 코드를 만족하기 위하여 2개의 송신 안테나를 가지는 송신자를 Alice, 각각 하나의 안테나를 가지는 합법적 수신자와 도청자를 Bob

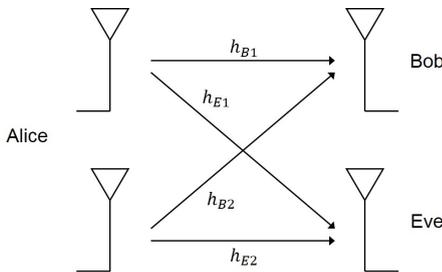


그림 3. 채널 모델
Fig. 3. Channel model

과 Eve라 칭하였다. 이는 그림 3에서 확인할 수 있다.

그림 3에서 Alice는 BS (Base Station) 또는 AP (Access Point)이고, Bob과 Eve는 사용자이다. 그리고 도청자인 Eve는 수동적임을 가정하였다. 따라서 Eve는 오직 수신만 가능하다.

3.3 시스템 모델

Alice는 그림 4와 같은 과정을 통해 신호를 전송 신호를 생성한다. 입력신호 $x(t)$ 를 hadamard 변환하고 변환된 신호를 바탕으로 인위적 잡음을 발생시킨 후 신호에 더한다. 그리고 STBC Mapper를 이용하여 신호를 STBC 변환한다.

그림 3의 채널 모델을 통해 동일한 타임 슬롯에서 Bob과 Eve가 수신한 신호는 식(11)과 같이 주어진다.

$$\begin{aligned} Y_B &= (h_{B1} + h_{B2})x + n_B \\ Y_E &= (h_{E1} + h_{E2})x + n_E \end{aligned} \quad (11)$$

위의 수식에서 h_{B_i} 는 Alice와 Bob 사이의 채널이고 h_{E_i} 는 Alice와 Eve 사이의 채널이며, n_B, n_E 는 각각 Bob과 Eve의 잡음이다. 본 시스템의 채널은 Rayleigh Fading 채널이고, 각 타임 슬롯은 독립이며, 모든 잡음은 AWGN으로 가정하였다. 그리고 이때의 각 채널과 잡음은 iid (independent and identically distributed random variables)이고 $CN(0,1)$ 인 분포를 따른다. 또한 본 시스템 모델은 시뮬레이션의 간략화와 보다 명확한 비교를 위하여 Bob이 채널 h_B 의 정보를 모두 알고 있는 완벽한 CSI (Channel State Information)상태를 가정하였다. 하지만 Eve는 수신만 가능한 수동적 도청자를 가정하였기 때문에 Eve는 채널 h_E 의 상태를 알 수 없다.

제안된 전송 방법에서 인위적 잡음은 Alice와 Bob 사이의 채널 h_B 에서는 null space로, Alice와 Eve 사이의 채널 h_E 에서는 잡음으로 작용하여야 한다. 따라서 이때의 인위적 잡음은 채널 h_B 의 정보를 기반으로 만들어져야 한다.

인위적 잡음이 추가된 신호 X 는 식 (12)와 같이 표현할 수 있다.

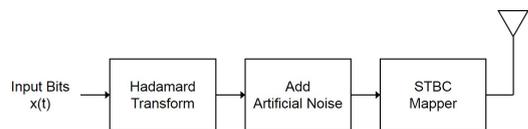


그림 4. 송신단 모델
Fig. 4. The Transmitter Model

$$X = S + W \quad (12)$$

여기서 S 는 신호, W 는 인위적 잡음을 나타낸다. 위의 과정을 거친 수신 신호는 다음과 같다.

$$Y_B = h_B X + n_B = h_B S + h_B W + n_B \quad (13)$$

S 는 2x2 크기의 STBC 심볼 블록이므로 식 (14)와 같이 표현할 수 있다.

$$S = \begin{bmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{bmatrix} \quad (14)$$

여기서 hadamard 변환을 s_1, s_2 에 적용시키면 식 (15)를 얻는다.

$$\begin{aligned} s_1 &= c_1 + c_2 \\ s_2 &= c_1 - c_2 \end{aligned} \quad (15)$$

위의 식을 신호 S 에 적용시키면 아래의 신호 S' 를 얻을 수 있다.

$$S' = \begin{bmatrix} c_1 + c_2 & -(c_1 - c_2)^* \\ c_1 - c_2 & (c_1 + c_2)^* \end{bmatrix} \quad (16)$$

최종적으로 수신 신호는 식(17)과 같다.

$$Y_B = h_B S' + h_B W + n_B \quad (17)$$

이때 인위적 잡음 W 가 고정된 특정 값이면 Bob이나 Eve 양 쪽 모두에게 잡음으로 작용되거나, Eve에게 상대적으로 작은 잡음으로 작용하게 된다. 따라서 인위적 잡음의 효율을 극대화하기 위해 W 의 값이 Bob의 채널환경에 따라 변화해야 한다. 그리고 인위적 잡음 W 가 $h_B W \approx 0$ 인 값이 되어야 Bob에는 영향을 미치지 않고 Eve에만 영향을 미치게 된다.

이를 위해 W 를 아래와 같이 정의 할 수 있다.

$$W = NV \quad (18)$$

이때 N 은 채널 h_B 의 null vector 행렬이고, V 는 iid인 가우시안 랜덤 잡음이다. 완벽한 CSI를 가정하였기 때문에 $h_B W$ 를 0으로 만드는 null vector 행렬 N 을 그림 5의 과정을 통해 계산할 수 있다.

그림 5의 과정을 통해 계산된 인위적 잡음은 h_B 의

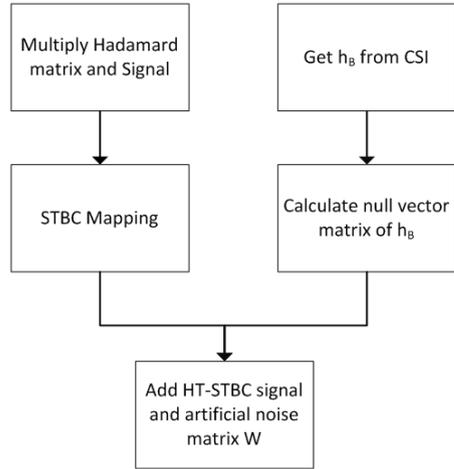


그림 5. Null vector 생성 플로우 차트
Fig. 5. Flow chart of method for generating the null vector

null vector이기 때문에 Alice와 Bob이 통신할 때에는 아무런 영향을 미치지 못한다. 하지만 Eve가 Alice의 신호를 도청할 때에는 강력한 잡음으로 작용하기 때문에 Eve가 원래의 신호를 검출하지 못하게 된다.

또한 hadamard 변환을 통해 신호가 변조되었기 때문에 Alice가 hadamard 변환을 사용하는 것을 모르는 Eve가 인위적 잡음 W 를 유사하게 추정하였다 하더라도 또 다른 인위적 잡음으로 작용하기 때문에 기존의 STBC와 인위적 잡음을 이용한 전송방법보다 개선된 보안성능을 제공한다.

IV. 모의실험 결과

본 장에서는 제안한 시스템과 기존의 STBC를 이용한 인위적 잡음 기법과의 검출 성능을 비교하였다. 이때 각 전송 신호는 독립적인 Rayleigh Fading 채널을 거치며 수신단에서 완벽한 채널 값들을 추정 가능하다고 가정하였다.

본 모의실험에서는 각각 BPSK, QPSK, 16-PSK로 변조하여 도청자와 합법적 수신자의 BER을 비교하였다. 그리고 이때 동일한 Eb/No (energy bit to noise ratio) 환경을 이용하였다.

그림 6은 BPSK 변조를 이용하고 STBC와 HT-STBC 및 인위적 잡음을 사용하였을 때의 BER 성능 비교이다. BER 10^{-3} 을 기준으로 제안하는 방법이 기존 방법 대비 3dB 만큼 성능이 향상됨을 확인할 수 있었다. Eb/No=5dB 일때 합법적 수신자와 도청자의 BER은 STBC를 이용하였을 때는 각각 0.18%,

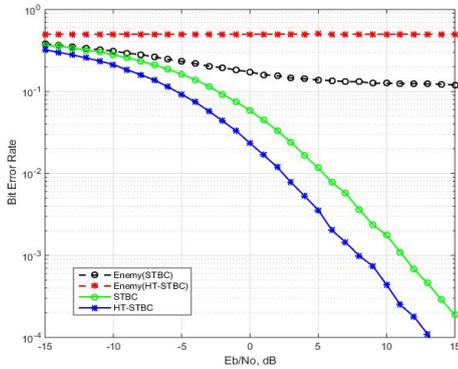


그림 6. BPSK 변조를 사용하였을 때의 수신자와 도청자의 BER 성능 비교
Fig. 6. BER performance comparison of receiver and eavesdropper on BPSK modulation

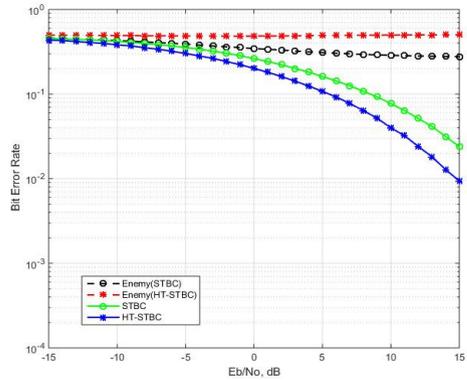


그림 8. 16-PSK 변조를 사용하였을 때의 수신자와 도청자의 BER 성능 비교
Fig. 8. BER performance comparison of receiver and eavesdropper on 16-PSK modulation

12.61%, HT-STBC를 이용하였을 때는 0.04%, 49.92%이다. 이때 도청자가 수신자에 비해 높은 BER 값을 가진다. 따라서 도청자는 전송된 신호를 추출할 수 없고, 정보의 보안상태 또한 높게 유지된다. 이때 HT-STBC가 STBC에 비해 뛰어난 성능을 갖는데 이는 도청자 측에서는 추가된 인위적 잡음뿐만 아니라 hadamard 변환된 신호로 인해 원래의 신호를 쉽게 추출할 수 없기 때문이다. HT-STBC를 사용할 때에는 추가된 인위적 잡음과 hadamard 변환이 이중의 인위적 잡음으로 작용한다.

그림 7, 8은 QPSK, 16-PSK 변조를 이용하였을 때의 BER 성능 비교이다. 각 그림에서 볼 수 있듯이 고차 변조에서도 제안하는 방법의 BER이 기존의 방법보다 감소하고, 수신자와 도청자 간의 BER 차이 또한 증가했음을 확인 할 수 있다.

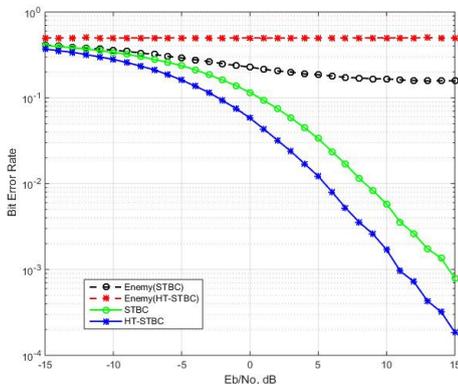


그림 7. QPSK 변조를 사용하였을 때의 수신자와 도청자의 BER 성능 비교
Fig. 7. BER performance comparison of receiver and eavesdropper on QPSK modulation

그림 9는 Eb/No이 5dB일 때 STBC와 HT-STBC를 사용하였을 때의 BER 차이 비교이며, STBC를 사용하였을 때 보다 HT-STBC를 사용하였을 때 BER 차이가 크음을 확인할 수 있었다. 그리고 각각 BPSK, QPSK, 16-PSK를 사용하였을 때 제안된 방법이 0.3709, 0.3356, 0.2353의 차이를 보임을 확인 하였다. 여기서 BER 차이는 합법적 사용자인 Bob과 도청자인 Eve, 두 사용자 사이의 수신 성능 차이로 차이가 클수록 보안성능이 뛰어남을 뜻한다.

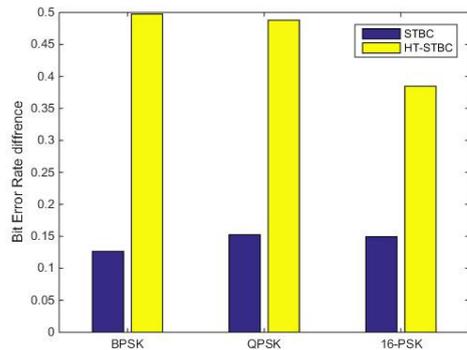


그림 9. 모듈레이션 방식에 따른 BER 성능 차이 비교
Fig. 9. BER performance differences comparison according to modulation scheme

V. 결론

본 논문에서는 HT-STBC와 인위적 잡음을 이용하여 물리 계층의 보안성을 개선하는 방법을 제안하였다. 기존의 STBC와 인위적 잡음을 이용하는 방법은 QPSK 이상의 변조 방식을 사용했을 때 BER 차이가

제한적으로 증가하는 문제가 있다. 그리고 Eb/No이 5dB일 때 BPSK 변조된 신호를 전송하면 기존의 STBC와 인위적 잡음을 이용하는 방법 대비 BER 차이가 0.37 증가함을 모의실험을 통해 확인하였다. hadamard 변환된 심볼이 인위적 잡음과 같이 작용하기 때문에 신호가 hadamard 변환된 것을 알지 못하는 도청자는 원래의 방법대로 복조를 시도하게 되고, 이로 인해 BER 차이가 증가된다. BER 차이의 증가는 도청자와 합법적 수신자 사이의 수신 신호 품질 차이의 증가로, 이는 해당 채널의 보안성능이 증가했음을 의미한다. 향후 보다 뛰어난 보안성능을 요구하는 전자상거래, 군용통신 등의 분야에 활용 할 수 있을 것으로 예상된다.

References

[1] Y.-S. Shiu, et al., "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66-74, Apr. 2011.

[2] J. Choi, J. Ha, and H. Jeon, "Physical layer security for wireless sensor networks," *IEEE PIMRC*, pp. 1-6, 2013.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical J.*, vol. 28, no. 4, pp. 656-715, 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell System Technical J.*, vol. 54, no. 8, pp. 1355-1387, 1975.

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, 2008.

[6] I. Son, I. Kim, J. Yang, and N. Lee, "Smart device security technology for cyber defense," *J. KICS*, vol. 37, no. 10, pp. 986-992, Oct. 2012.

[7] J.-K. Hong, "The analysis of crypto communication relay effect in the security framework technique of network centric warfare environment," *J. Korea Academia-Ind. Cooperation Soc.*, vol. 8, no. 4, pp. 788-794, 2007.

[8] S. Corson and J. Macker, *Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considera-*

tions, No. RFC 2501, 1998.

[9] S. Y. Shin and I. A. Wicaksono, "Improving wireless physical layer security using alamouti code and artificial noise," *ICTC*, pp. 1061-1064, 2013.

[10] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas in Commun.*, vol. 16, no. 8, pp. 1451-1458, 1998.

[11] S.-Y. Jin, J.-H. Kim, K.-H. Park, and H.-Y. Song, "Equivalence of hadamard matrices whose rows Form a vector space," *J. KICS*, vol. 34, no. 7, pp. 635-639, Jul. 2009.

[12] T. S. Siadari and S. Y. Shin, "Joint hadamard transform and alamouti scheme for wireless communication system," *AEU-Int. J. Electron. Commun.*, vol. 68, no. 9, pp. 889-891, 2014.

[13] Y. Zou, et al., "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42-48, 2015.

[14] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831-3842, 2010.

김진우 (Jin Woo Kim)



2014년 2월 : 국립금오공과대학교 전자공학부 졸업
 2015년 3월~현재 : 국립금오공과대학교 IT융복합공학과 석사과정
 <관심분야> 무선통신, MIMO, NOMA

신 수 용 (Soo Young Shin)



1999년 2월 : 서울대학교 전기
공학부 졸업

2001년 2월 : 서울대학교 전기
공학부 석사

2006년 2월 : 서울대학교 전기
컴퓨터공학부 박사

2010년~현재 : 국립금오공과대
학교 전자공학부 교수

<관심분야> 5G and FRA, Wireless Communi-
cation/Network, Internet of Things, signal
processing, etc.