논문 13-38A-08-15

한국통신학회논문지 '13-08 Vol.38A No.08
http://dx.doi.org/10.7840/kics.2013.38A.8.733

다중 안테나 릴레이 기반의 Secure Amplify-and-Forward 전송 시스템의 보안 성능 분석

황 규 성◆, 주 민 철°

Secrecy Performance of Secure Amplify-and-Forward Transmission with Multi-Antenna Relay

Kyu-Sung Hwang◆, MinChul Ju°

요 약

본 논문에서는 증폭후전송 (amplify-and-forward, AF) 기반의 중계 전송 시스템에서 통신 정보를 도청하는 도청자가 존재하는 환경인 와이어탭 채널 (wiretap channel)에서의 물리 계층 보안에 대한 분석을 한다. 와이어탭 채널 환경에서 원천 노드, 목적지 노드, 중계 노드, 도청 노드가 각각 한 개씩 존재한다고 가정하며, 특히 중계 노드는 다수의 안테나를 가지고 있는 시스템을 고려한다. 중계 노드에서는 AF 전송시에 다이버시티 (diversity) 이득을 취하기 위한 안테나 선택 기법을 적용하였다. 구체적으로, 중계 노드에서 데이터 수·송신시 신호대잡음비를 최대화할 수 있는 안테나를 선택하여 동작한다. 보다 실질적인 환경을 고려하기 위하여 중계 노드에서 목적지 노드로 전송할 때 도청 노드에 대한 채널 정보는 없는 환경을 고려하였다. 제안된 시스템의 보안 성능 분석을 위하여 보안 불통 확률 (secrecy outage probability)를 한 개의 적분 형태로 구하였으며, 시뮬레이션 결과를 통하여 해당 성능 분석이 올바름을 보인다.

Key Words : Secrecy outage probability, wiretap channel, eavesdropper, amplify-and-forward, multi-antenna relay

ABSTRACT

In this paper, we consider a physical layer security of an amplify-and-forward (AF) transmission in a presence of an eavesdropper in a wiretap channel. The proposed wiretap channel consists of a source, a destination, a relay, and an eavesdropper. Specifically, we consider that the relay has multiple antennas to exploit a diversity gain and a receive/transmit antenna selection schemes are applied to maximize a signal-to-noise ratio. In a practical point of view, we focus on the practical scenario where the relay does not have any channel state information of the eavesdropper while performing an AF protocol at the relay. For a secrecy performance analysis, we analyze a secrecy outage probability of the proposed system in one-integral form and verify our analysis with the computer-based simulation.

Ⅰ. 서 론

최근에 무선 통신 시스템이 대중화됨에 따라, 점차 통신 보안에 관한 기술이 주목받고 있다. 전통적

※ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(2012R1A1A1041485)
◆ 주저자 : 경일대학교 사이버보안학과, kshwang@kiu.ac.kr, 정회원
° 교신저자 : 국민대학교 전자공학부, mcju@kookmin.ac.kr, 정회원
논문번호 : KICS2013-07-277, 접수일자 : 2013년 7월 2일, 최종논문접수일자 : 2013년 8월 6일

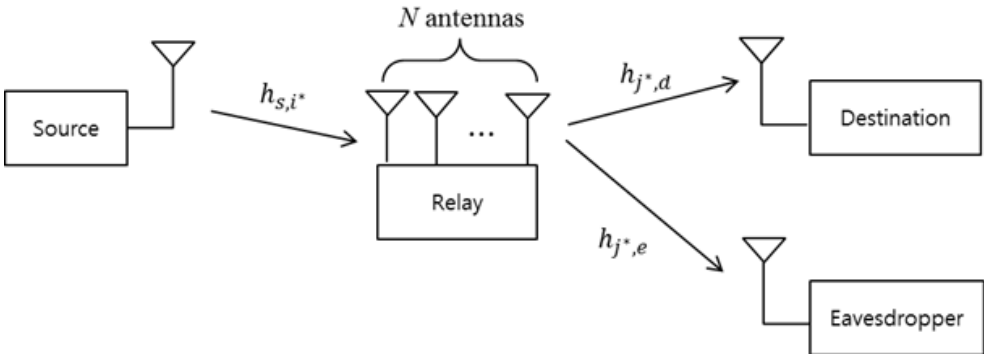


그림 1. 도청자가 있는 릴레이 시스템 모델
Fig. 1. Relay system model in the presence of an eavesdropper

으로 보안 기술이라고 하면 암호학 (cryptograghy) 관점에서 논의가 많았으나, 최근에는 무선 통신 물리 계층 영역에서의 보안에 관련된 주제가 많이 연구되고 있다[1]. 물리 계층 영역에서의 보안이란 도청자가 존재할 때 신뢰성 있는 통신 메시지 (confidential communication message)의 전송 능력을 채널 용량 관점에서 접근한 것이다. 도청자가 존재하는 시스템의 채널 모델을 1975년도에 Wyner가 와이어탭 채널 (wiretap channel) 모델을[2] 발표하였으며, 많은 이전의 연구에서 송신자, 수신자, 도청자가 존재하는 환경에서의 보안 성능 (secrecy performance) 분석이 이루어 졌다. 수신자의 채널 용량이 도청자의 채널 용량보다 클 때 Wiretap channel에서 완벽한 보안이 가능하다는 관점에서의 성능 분석 연구가 많이 수행되었다. 중계 전송 (relay transmission)는 통신 영역 확장 및 저전력 통신을 가능하게 해주는 기술로 릴레이를 중계 노드로 사용하여 데이터를 수신단에 전송하는 기술이다[3]. 중계 전송에는 대표적으로 두 가지 종류가 있는데, 릴레이에서 수신된 신호를 복원한 후 다시 인코딩하여 전송하는 복호후전송 (decode-and-forward, DF) 방식과 릴레이에서 수신된 신호를 단순히 증폭한 후 수신단에 전송하는 증폭후전송 (amplify-and-forward, AF) 방식이 있다[4]. 최근에 연구된 논문에서[5], 위와 같은 중계 전송 시스템 하에서 도청자가 존재하는 와이어탭 채널 환경에서의 보안 성능 분석에 대한 연구가 이루어졌으며, 다중입출력 (multiple-input multiple output, MIMO) 와이어탭 채널 환경에서 송신 안테나 선택 기법을 고려한 연구가 진행되었다[6].

본 논문에서는 위에 언급한 중계 전송 시스템에서 수신자 이외에 도청자가 존재하는 와이어탭 채널 모델에서의 보안 성능 분석을 고려하였으며, 특히 최근 다이버시티 (diversity) 이득을 얻기 위하여 많이 연구되었던 다중 안테나 릴레이 (multi-antenna relay) 환경을 고려하였다. 다중 안테나 릴레이의 효율적인 활용을 위한 송·수신 안테나 선택 기법을 고려하였다. 제안된 환경 하에서 보안 불통 확률 (secrecy outage probability, SOP)를 구하기 위한 수식적인 접근법을 제안하였으며, 최종적으로 보안 불통 확률을 한 개의 적분 형태로 계산하였다. 마지막으로 모의 실험을 통하여 제안한 시스템의 성능 측정 및 이론적 분석에 대한 검증을 제시하였다.

Ⅱ. 시스템 모델

본 논문에서는 그림 1에서와 같이 원천 노드 (source node, S), 중계 노드 (relay node, R), 목적지 노드 (destination node, D) 및 도청 노드 (eavesdropper node, E) 로 구성된 와이어탭 채널 모델링을 고려한다. 원천 노드와 목적지 노드 사이 및 원천 노드와 도청 노드 사이의 직접 통신은 무시되는 시스템을 고려하며, 중계 노드는 N개의 안테나를 가지고, 나머지 노드들은 한 개의 안테나만을 갖는 시스템을 고려한다. 한 개의 데이터 프레임 (data frame) 전송을 위해서 두 개의 시간 슬롯이 필요한 듀얼 홉 시스템 (dual-hop system)을 고려하며, 중계 노드에서의 전송 방식은 증폭후전달 방식을 사용한다. 첫 번째 시간 슬롯에서는 원천 노드에서부터 중계 노드로의 데이터 전송이 이루어지며, 이때 중계 노드에서는 다수의 수신 안테나 중 가장 우수한 안테나를 선택하여 사용하는 선택 결합 (selection combining, SC)[7] 기법을 적용한다. 첫 번째 시간 슬롯에서의 수신 신호는 다음과 같이 표현될 수 있다.

$$\mathbf{y}_r = \mathbf{h}_{s,r} x_s + \mathbf{n}_r. \quad (1)$$

여기서 x_s는 전송 신호이며 분산값은 $\mathrm{E}\left[x_s^H x_s\right] = P$ 이다. $\mathbf{h}_{\mathrm{s,r}} = \left[\mathrm{h}_{\mathrm{s},1}, \mathrm{h}_{\mathrm{s},2}, \cdots, \mathrm{h}_{\mathrm{s,N}}\right]^{\mathrm{T}}$은 복소 원형 대칭 가우시안 (complex circularly symmetric Gaussian) 채널이며 공분산 매트리스 (covariance matrix)는 $\mathbf{C}_{s,r} = diag\left\{\bar{\gamma}_{s,1}, \bar{\gamma}_{s,2}, \cdots, \bar{\gamma}_{s,N}\right\}$ 이다. $\mathbf{n}_{\mathrm{r}}$는 부가 백색 가우시안 잡음으로, 공분산 매트리스는 $\mathrm{E}\left[\mathbf{n}_r^H \mathbf{n}_r\right] = \mathrm{I}_N N_0$ 이다. $\mathbf{n}_{\mathrm{r}}$의 공분산 매트리스 I_{N}은 $N \times N$ 단위 행렬 (unit matrix) 이며, N_0는 중계 노드에서의 잡음 세기 (noise power)이다.

중계 노드에서 SC를 사용한다고 가정할 때, 식 (1)는 다음과 같이 나타 낼 수 있다.

$$y_{i^*} = h_{s,i^*} x_s + n_{i^*}. \quad (2)$$

식 (2)에서 $i^* = \arg\max_r \left\{|h_{s,r}|^2\right\}$ 이다. 중계 노드에서 목적지 노드로 정보를 전달할 때는 다수의 송신 안테나 중에서 가장 채널 환경이 우수한 안테나를 선택하여 전송하는 방식인 송신 안테나 선택 (transmit antenna selection, TAS)을[8] 사용하며, 증폭 이득 G를 고려하여 증폭후전송한다. 목적지 노드에서 수신 신호는 다음과 같다.

$$y_d = h_{j^*,d} G y_{i^*} + n_d. \quad (3)$$

식 (3)에서 $h_{j^*,d}$는 TAS에 의하여 선택된 중계 노드와 목적지 노드 사이의 채널이며 수학적으로는 $j^* = \arg\max_r \left\{|h_{r,d}|^2\right\}$ 로 표시된다. 증폭 이득 G는 $G = 1/\sqrt{\mathrm{E}\left[|y_{i^*}|^2\right]}$ 이다. 이 경우 목적지 노드에서의 수신 신호대잡음비 (instantaneous signal-to-noise ratio, SNR) 값은 다음과 같이 나타 낼 수 있다[4].

$$\gamma_d = \rho \frac{|h_{s,i^*}|^2 |h_{j^*,d}|^2}{|h_{s,i^*}|^2 + |h_{j^*,d}|^2 + 1/\rho}. \quad (4)$$

식 (4)에서 $\rho = P/N_0$ 이다. 비슷한 방식으로 도청 노드에서 수신되는 SNR 값은 다음과 같이 구할 수 있다[4].

$$\gamma_e = \rho \frac{|h_{s,i^*}|^2 |h_{j^*,e}|^2}{|h_{s,i^*}|^2 + |h_{j^*,e}|^2 + 1/\rho}. \quad (5)$$

Ⅲ. 보안 성능 분석

3.1. 증폭후전송 환경에서 와이어탭 채널 모델

본 논문에서는 와이어탭 채널 모델을 고려한다. 특히, 도청 노드는 수동적인 형태의 단순 도청 방식으로 동작한다고 가정한다.[6] (이는 중계 노드와 도청 노드 간의 피드백 (feedback) 통신은 없는 것으로 간주한다.) 중계 노드-목적지 노드 (R-D) 및 중계 노드-도청 노드 (R-E) 채널들은 느린 블록 페이딩 (slow block fading) 환경 및 블록 길이가 충분히 길다고 가정할 때 달성 가능한 보안 데이터 비 (achievable secrecy rate, ASR) C_s 는 다음과 같이 표현될 수 있다[1].

$$C_s = \left[C_d - C_e\right]^+. \quad (6)$$

식 (6)에서 $[x]^+ = \max[0, x]$ 이고, C_d 및 C_e는 $S-R-D$ 경로 및 $S-R-E$ 경로의 채널 용량이며 $C_d = \frac{1}{2}\log_2(1+\gamma_d)$ 및 $C_e = \frac{1}{2}\log_2(1+\gamma_e)$ 으로 계산된다. 식 (6)를 식 (4) 및 (5)를 이용하여 순간 신호대잡음비 (instantaneous SNR) 형태로 다시 표현하면 다음과 같다.

$$C_s = \left[\frac{1}{2}\log_2\left(\frac{1 + \dfrac{\gamma_{s,i^*}\gamma_{j^*,d}}{\gamma_{s,i^*} + \gamma_{j^*,d} + 1}}{1 + \dfrac{\gamma_{s,i^*}\gamma_{j^*,e}}{\gamma_{s,i^*} + \gamma_{j^*,e} + 1}}\right)\right]^+. \quad (7)$$

식 (7)에서 $\gamma_A = \rho |h_A|^2$ 이다.

3.2. 보안 불통 확률

와이어탭 채널 환경에서 시크리시 불통 확률 SOP는 ASR이 목표 보안 데이터 비 (target secrecy data rate, TSR, R)보다 작을 확률로 정의될 수 있다.[1] 수식적으로 표현하면,

$$P_{out}(R) = \Pr[C_s < R]$$

$$= \Pr\left[\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{s,i^*}\gamma_{j^*,d}}{\gamma_{s,i^*}+\gamma_{j^*,d}+1}}{1+\frac{\gamma_{s,i^*}\gamma_{j^*,e}}{\gamma_{s,i^*}+\gamma_{j^*,e}+1}}\right) < R\right] \quad (8)$$

$$= \Pr\left[\frac{\frac{(\gamma_{s,i^*}+1)(\gamma_{j^*,d}+1)}{\gamma_{s,i^*}+\gamma_{j^*,d}+1}}{\frac{(\gamma_{s,i^*}+1)(\gamma_{j^*,e}+1)}{\gamma_{s,i^*}+\gamma_{j^*,e}+1}} < T\right].$$

식 (8)에서 $T = 2^{2R}$ 이다. 이후부터는 간략한 수식 정리를 위해서 $\gamma_1 = \gamma_{s,i^*}$, $\gamma_2 = \gamma_{j^*,d}$ 및 $\gamma_3 = \gamma_{j^*,e}$ 이라고 표시한다. 식 (8)은 아래와 같이 다시 쓸 수 있다.

$$P_{out}(R) = \mathrm{E}_{\gamma_3 = z}\left[\Pr\left[\frac{\frac{(\gamma_1+1)(\gamma_2+1)}{\gamma_1+\gamma_2+1}}{\frac{(\gamma_1+1)(z+1)}{\gamma_1+z+1}} < T\right]\right] \quad (9)$$

$$= \mathrm{E}_{\gamma_3 = z}[\Pr[(\gamma_1-(T-1)(z+1))\gamma_2 < T(z+1)(\gamma_1+1)-(\gamma_1+z+1)]].$$

T는 항상 양수이기 때문에 식 (9)의 확률 부분을 다시 $I(z)$라는 표현으로 정리하면 아래와 같다.

$$I(z) = \Pr[(\gamma_1-(T-1)(z+1))\gamma_2 < T(z+1)(\gamma_1+1)-(\gamma_1+z+1)]$$
$$= \Pr[\gamma_1 \le (T-1)(z+1)] + \Pr[\gamma_2 < A(\gamma_1, T, z), \gamma_1 > (T-1)(z+1)] \quad (10)$$

식 (10)에서

$$A(\gamma_1, T, z) = \frac{T(z+1)(\gamma_1+1)-(\gamma_1+z+1)}{\gamma_1-(T-1)(z+1)}$$

이다. 챕터 2에서 제안된 다중 안테나 중계 노드에서 SC/TAS 알고리듬을 적용하면, 안테나들에게 할당된 채널이 서로 독립적으로 동일한 분포를 갖는 (independent identically distributed, I.I.D.) Rayleigh 페이딩 채널 환경이라고 가정하면, 식 (10)에서 γ_1 및 γ_2의 확률 밀도 함수 (probability density function, pdf)는 다음과 같이 표현할 수 있다.

$$f_{\gamma_1}(x) = N\sum_{i=1}^{N}\binom{N-1}{i-1}\frac{(-1)^{i+1}}{\bar{\gamma}_1}e^{-\frac{ix}{\bar{\gamma}_1}}. \quad (11)$$

$$f_{\gamma_2}(x) = N\sum_{j=1}^{N}\binom{N-1}{j-1}\frac{(-1)^{j+1}}{\bar{\gamma}_2}e^{-\frac{jx}{\bar{\gamma}_2}}. \quad (12)$$

식 (11) 및 (12)에서 $\bar{\gamma}_X = \mathrm{E}[\gamma_X]$이다. 식 (11) 및 (12)의 γ_1 및 γ_2의 확률 밀도 함수를 이용하여 식 (10)를 풀어보면 다음 페이지의 식 (13) 같이 나타낼 수 있다. 식 (13)에서 $y = x-(T-1)(z+1)$ 의 변수변환 (change of variable)를 행하고, 참고문헌 [9]의 [Eq. 8.432]를 이용하여 다시 정리하면 다음 페이지의 식 (14) 같은 결과를 얻을 수 있다.

최종적으로 (14)식의 $I(z)$값을 이용하여 시크리시 불통 확률 SOP를, $P_{out}(R)$, 아래와 같은 한 개의 적분 형태로 계산할 수 있다.

$$P_{out}(R) = \int_0^{\infty} I(z)\frac{e^{-z/\bar{\gamma}_3}}{\bar{\gamma}_3}dz. \quad (15)$$

Ⅳ. 수치적 분석 결과

이번 장에서는 2장에서 제안한 와이어탭 채널 환경에서 다중 안테나 중계 노드에 SC/TAS 알고리듬이 적용된 시스템의 SOP의 성능을 실험하고, 3장에서 구한 분석값과 일치함을 검증한다. 성능 분석을 위한 시뮬레이션 환경으로는 몬테 카를로 (Monte Carlo) 방식을 사용하였으며, I.I.D.한 Rayleigh 페이딩 모델을 고려하였다.

그림 2에서 중계 노드에 사용된 안테나 수는 $N = 1, 2, 4, 6$인 경우를 고려하였으며, TSR는 $R = 2$ bps/Hz 이다. 본 실험에서 평균 신호대잡음비 (average SNR)은 $\bar{\gamma} = \bar{\gamma}_1 = \bar{\gamma}_2$ 및 $\bar{\gamma}_3 = 5$

$$I(z)=1-N\sum_{i=1}^{N}\sum_{j=1}^{N}(-1)^{i+1}(-1)^{j}\binom{N-1}{i-1}\binom{N}{j}\int_{(T-1)(z+1)}^{\infty}\frac{1}{\bar{\gamma}_1}\exp\left(-\frac{j}{\bar{\gamma}_2}A(x,T,z)-\frac{ix}{\bar{\gamma}_1}\right)dx. \quad (13)$$

$$I(z)=1+N\sum_{i=1}^{N}\sum_{j=1}^{N}(-1)^{i+1}(-1)^{j}\binom{N-1}{i-1}\binom{N}{j}2(z+1)\sqrt{\frac{T(T-1)j}{\bar{\gamma}_1\bar{\gamma}_2 i}} \times\exp\left(-\left(\frac{(T-1)(z+1)i}{\bar{\gamma}_1}+\frac{(T(z+1)-1)j}{\bar{\gamma}_2}\right)\right)K_1\left(2(z+1)\sqrt{\frac{T(T-1)ij}{\bar{\gamma}_1\bar{\gamma}_2}}\right). \quad (14)$$

dB 으로 설정하였다. 그림 2에서 제안된 시스템의 보안 불통 확률 SOP는 평균 신호대잡음비 이 증가할수록 그리고 중계 노드에서의 이용 가능한 안테나 개수가 증가할수록 감소함을 확인할 수 있다. 또한, 4장에서 풀이한 분석이 타당함을 검증하였다.

그림 3은 중계 노드 위치에 따른 보안 불통 확률 SOP의 변화를 확인하고, 중계 노드 위치의 영향에 대하여 평가한다. 본 실험 환경에서는 원천 노드와 목적지 모드 $S-D$의 거리를 기준으로 정규화 시킨다. 중계 노드에 사용된 안테나 수는 $N=1,2,3,4$인 경우를 고려하였으며, TSR는 $R=1$ bps/Hz 이다. 평균 신호대잡음비은 $\bar{\gamma}=20$ dB로 설정하였으며, 각 경로당 평균 신호대잡음비은 $\bar{\gamma}_1=d^{-\alpha}\bar{\gamma}$, $\bar{\gamma}_2=(1-d)^{-\alpha}\bar{\gamma}$, $\bar{\gamma}_3=0.1(1.5-d)^{-\alpha}\bar{\gamma}$ 으로 설정하였다. 위 평균 신호대잡음비에서 d는 원천 노드와 중계 노드 사이의 정규화 거리 (normalized distance)이며, $1-d$는 중계 노드와 목적이 노드 사이의 정규화된 거리를 의미한다. α는 경로 손실 지수 (path loss exponent)으로 $\alpha=3$으로 설정하였다. 본 실험에서는 주어진 채널 환경에서 최적의 중계 노드 위치에 대한 분석을 하였으며, 수식적인 분석이 타당함을 검증하였다.

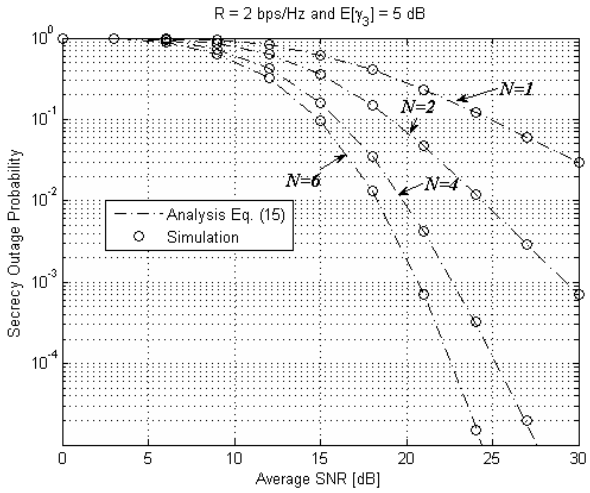


그림 2. 제안 시스템의 시크리시 불통 확률
Fig. 2. Secrecy outage probability of the proposed system

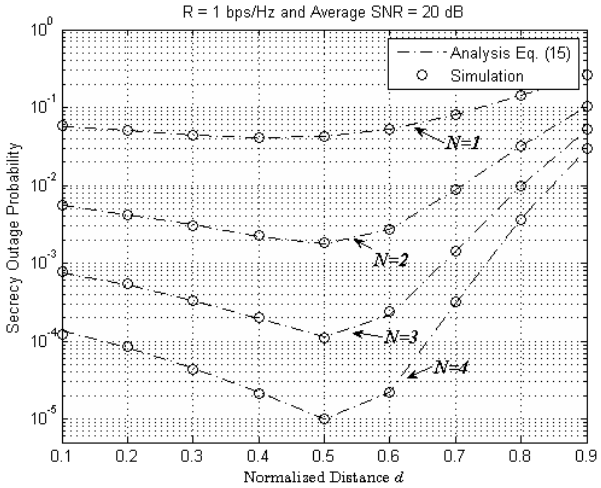


그림 3. 정규화 거리 d에 대한 제안 시스템의 시크리시 불통 확률
Fig. 3. Secrecy outage probability of the proposed system against the normalized distance d

V. 결 론

본 논문에서는 AF 중계 전송 시스템에서 도청자가 존재하는 와이어탭 채널에서의 보안 불통 확률 SOP를 분석하였으며, 특히 중계 노드에서 다중 안테나를 사용하는 중계 노드 방식을 고려하였다. 효율적인 안테나 사용을 위하여 중계 전송시의 최적의 송·수신 안테나를 선택하는 SC/TAS 알고리듬을 적용하였다. 보안 불통 확률 SOP를 분석하기 위하여 수식적인 접근법을 제안하였으며, 최종적으로 보안 불통 확률을 한 개의 적분 형태로 계산하였다. 최종적으로 수치석 실험을 통하여 본 논문에 제시된 분석에 대한 검증을 하였다.

References

[1] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, June 2008.

[2] A. Wyner, "The wire-tap channel," *Bell Syst. Technol. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] K. Almuradov, J.-B. Park, and Y. H. Kim, "A performance bound of multi-hop multi-relay wireless communication system with optimal path selection," *J. KICS*, vol. 36, no. 1, pp. 1-7, Jan. 2011.

[4] B. Rankov and A. Wittneben, "Spectral efficient protocols for half-duplex fading relay channels," *IEEE J. Select. Areas Commun.*, vol. 25, no. 2, pp. 379-389, Feb. 2007.

[5] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.

[6] N. Yang, P. L. Yoeh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channel," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144-154, Jan. 2013.

[7] T. Eng, N. Kong, and L. B. Milstein, "Comparison of diversity combining techniques for Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 44, no. 9, pp. 1117-1129, Sep. 1996.

[8] Z. Chen, J. Yuan, and B. Vucetic, "Analysis of transmit antenna selection/maximal-ratio combining in Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 54, no. 4, pp. 1312-1321, July 2005.

[9] I. S. Gradshteyn and I. M. Ryzhikt, *Table of Integrals, Series and Products*, 6th Ed., Academic Press, 2000.

황 규 성 (Kyu-Sung Hwang)

2004년 8월 고려대학교 전기전자전파공학부 공학사

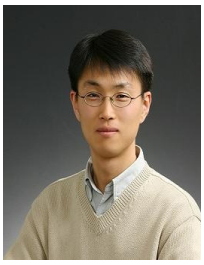
2010년 2월 고려대학교 전자컴퓨터공학과 공학박사

2010년 1월~2011년 8월 전자부품연구원 선임연구원

2011년 9월~현재 경일대학교 사이버보안학과 조교수

<관심분야> 통신이론, 신호처리, 디지털통신시스템

주 민 철 (MinChul Ju)



1997년 2월 POSTECH 전자공학과 공학사

1999년 2월 KAIST 전자공학과 공학석사

2010년 10월 Queen's University 전자컴퓨터공학과 공학박사

1999년 3월~2011년 8월 전자부품연구원 선임연구원

2011년 9월~현재 국민대학교 전자공학부 조교수

<관심분야> 통신이론, 신호처리, 디지털통신시스템