논문 14-39B-11-09 The Journal of Korean Institute of Communications and Information Sciences '14-11 Vol.39B No.11
http://dx.doi.org/10.7840/kics.2014.39B.11.803

협력 무선인지 네트워크에서의 보안 채널 용량 분석

누엔반딘◆, 김 현 민*, 신 오 순°

On the Secrecy Capacity in Cooperative Cognitive Radio Networks

Van-Dinh Nguyen◆, Hyeon-Min Kim*, Oh-Soon Shin°

요 약

본 논문에서는 면허 사용자와 감청 사용자가 존재하는 인지무선 네트워크에서 릴레이 선택 기능을 이용한 물리 계층 보안 시스템을 제안하고 성능을 분석한다. 먼저 감청에 대한 보안성 확보를 위해 수신기 측에서의 채널 정보를 이용하는 기회적 최적 릴레이 선택 방법과 다중 안테나 다이버시티를 이용하는 시스템을 제안한다. 이러한 시스템에서 인지무선 네트워크의 보안 outage 확률을 정의하고 수학적으로 정확한 확률 식을 유도한다. 아울러 송신전력에 제한이 없는 경우에 대한 점근적 outage 확률을 구한다. 수치 해석 결과를 제시함으로써 유도한 확률식의 정확성을 검증한다.

Key Words : Secrecy Capacity, Cognitive Radio (CR), Cooperative Cognitive Radio Networks (CRNs), Relay, Secrecy Outage Probability

ABSTRACT

In this paper, we investigate physical layer security in a cooperative cognitive radio networks (CRN) with a relay selection in the presence of a primary user and an eavesdropper. To protect the CRN from wiretapping by the eavesdropper, we propose employing an opportunistic relay selection scheme and multiple antennas at the destination that work based on the availability of channel state information at the receivers. Under these configurations, we derive an exact closed-form expression for the secrecy outage probability of the CRN, and also derive an asymptotic probability. Numerical results will be presented to verify the analysis.

Ⅰ. Introduction

As the radio spectrum becomes crowded and scarce, efficient utilization of radio spectrum becomes increasingly important. Cognitive radio networks (CNRs), first proposed by Mitola[1], provide a solution for improving spectrum utilization in wireless networks through optimistic spectrum sharing. Under a CRN, secondary users need to sense the spectrum to detect spectrum holes that are not used by primary (licensed) users. When using the resources that primary users are using, the secondary users and to limit the harmful interference that may be caused to the primary users[2-4].

※ 본 연구는 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2013R1A2A2A01011222).
◆ First Author : School of Electronic Engineering, Soongsil University, nguyenvandinh@ssu.ac.kr, 학생회원
° Corresponding Author : School of Electronic Engineering, Soongsil University, osshin@ssu.ac.kr, 종신회원
* School of Electronic Engineering, Soongsil University, hminplus@ssu.ac.kr, 학생회원
논문번호 : KICS2014-11-448, Received November 3, 2014; Revised November 14, 2014; Accepted November 14, 2014

Recently, physical layer security has attracted significant interest in the research community as the information security becomes crucial for pervasive and personalized wireless devices[5-8]. With the help of relays, the secrecy capacity of a wireless system can be significantly improved. The secrecy capacity of the secondary system in a CRN was investigated in [9-11], where the secondary users exploit multiple antennas to protect the confidential signal. On the other hand, optimal relay selection (ORS) scheme can be adopted to improve the performance of wireless relaying[12,13]. In particular, it has been shown that the ORS can achieve optimal performance in terms of the outage probability and capacity for both decode-and-forward (DF) and amplify-and-forward (AF) protocols.

In this paper, we consider a CRN in which there exists an eavesdropper that can overhear the confidential signal transmitted from the secondary user. Passive eavesdropper is considered, where the channel state information (CSI) is not available at the secondary transmitter. We take into account the peak interference constraint at primary receiver and maximal transmit power at secondary transmitter. Particularly, the eavesdropper is equipped with multiple antennas to wiretap channel. To deal with it, we consider the ORS scheme based on the availability of CSI at the secondary receiver and multiple antennas at primary receiver to promote secure data transmission. With this in mind, we derive new exact and asymptotic expression in closed-form for the secrecy outage probability. Numerical results will be provided to verify the analysis.

The rest of this paper is organized as follows. Section II describes a CRN model and the optimal relay selection scheme. In Section III, the secrecy outage probability of the secondary system is derived for the CRN. In Section IV, numerical results are presented and discussed. Finally, conclusions are drawn in Section V.

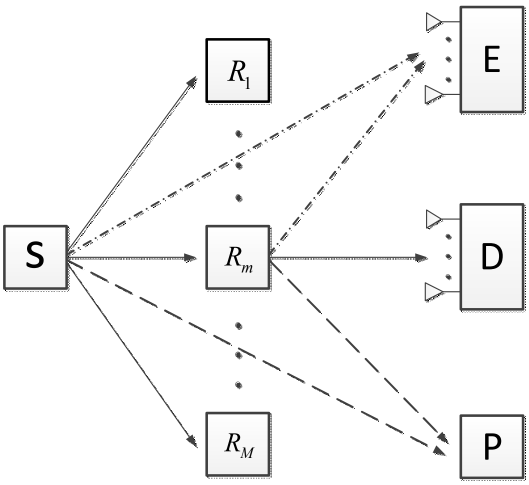

Fig. 1. A CRN with M relay nodes and an eavesdropper.

Ⅱ. System Model

As illustrated in Fig. 1, we consider a CRN with a secondary transmitter (S), a secondary receiver (D), a primary receiver (P), and an eavesdropper (E). We assume that there is no direct link between the secondary transmitter and the secondary receiver. Accordingly, the secondary transmitter sends data to the secondary receiver with the help of M secondary relays R_m, $m = 1, 2, ..., M$. We assume that the channel between any two nodes is assumed to be independent and flat Rayleigh fading channel, and that perfect CSI is available at the receiver. Each node is assumed to operate in half-duplex mode. The secondary receiver and the eavesdropper are equipped with N and K antennas, respectively, while each of the secondary transmitter, the primary receiver, and M relays, is equipped with a single antenna. The eavesdropper attempts to wiretap and decode the data of the secondary system.

Let $h_{SP}, h_{SRm}, h_{SE}, h_{R_mD}, h_{R_mP}$ and h_{R_mE} denote the channel coefficients of the links S → P, S → R_m, S → E, R_m → D, R_m → P, and R_m → E, respectively. The corresponding channel gains $|h_{XY}|^2$, $X \in \{S, R_m\}$ and $Y \in \{R_m, D, E, P\}$, will follow exponential distribution with a parameter Ω_{XY}. Therefore, the probability density function (PDF) of the random variable $|h_{XY}|^2$ is given as

$$f_{XY}(x) = \Omega_{XY}\exp(-\Omega_{XY}x) \tag{1}$$

where $\Omega_{XY} = E\{|h_{XY}|^2\} = d_{XY}^{\beta}$, d is the distance between two nodes X and Y, and β denotes the path loss exponent. Moreover, $n_Y \sim CN(0,1)$ denotes additive white Gaussian noise (AWGN) at the node Y. In an underlay CRN, the secondary system may simultaneously use the spectrum with the primary system. Therefore, the transmit power at S and R_m must satisfy a peak interference power constraint so that the interference at the primary receiver is less than threshold Q. We assume that antenna selection is employed at D and E to achieve full diversity gain[14]. During the first phase of relaying, S transmits to M relays and the corresponding signal-to-noise ratio (SNR) at R_m and E is respectively given as

$$\begin{aligned} \gamma_{1D} &= P_S |h_{SR_m}|^2, \\ \gamma_{1E} &= \max{}_{k=1,\dots,K} P_S |h_{SE_k}|^2, \end{aligned} \tag{2}$$

where P_S denote the transmit power of S. During the second phase, a relay transmits data to D and the SNR at D and E is respectively given as

$$\begin{aligned} \gamma_{2D} &= \max{}_{n=1,\dots,N} P_{R_m} |h_{R_m D_n}|^2, \\ \gamma_{2E} &= \max{}_{k=1,\dots,K} P_{R_m} |h_{R_m E_k}|^2, \end{aligned} \tag{3}$$

where P_{R_m} denotes the transmit power of R_m. Note that the transmit power P_S and P_{R_m} need to satisfy the interference constraint at P:

$$\begin{aligned} P_S &= \min\left(P_T, \frac{Q}{|h_{SP}|^2}\right), \\ P_{R_m} &= \min\left(P_T, \frac{Q}{|h_{R_m P}|^2}\right). \end{aligned}$$

Ⅲ. PERFORMANCE ANALYSIS

For the physical layer security relying on multiple relays, the main objective is to maximize the SNR in the desired link and minimize the SNR in the eavesdropping link at the same time. We consider an optimal relay selection based on the available CSI at the receiver:

$$m^* = \arg\max{}_{m=1,\dots,M} \min(C_{1m}^s, C_{2m}^s), \tag{4}$$

where C_{1m} and C_{2m} are the secrecy capacity of the first hop and that of the second hop, respectively. We define the secrecy capacity of each hop as[15]

$$\begin{aligned} C_{1m}^s &= \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{1\mathrm{D}}}{1+\gamma_{1\mathrm{E}}}\right)\right]^+, \\ C_{2m}^s &= \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{2\mathrm{D}}}{1+\gamma_{2\mathrm{E}}}\right)\right]^+, \end{aligned} \tag{5}$$

where $[x]^+ \equiv \max(x,0)$. From (4) and (5), the secrecy outage probability of the optimal selection scheme is give by

$$P_{out}^s = \Pr(\max{}_{m=1,\dots,M} \min(C_{1m}^s, C_{2m}^s) < R_{th}), \tag{6}$$

where R_{th} is the threshold for the secrecy rate.

Let $T_{1m} = \dfrac{1+\gamma_{1D}}{1+\gamma_{1E}}$ and $T_{2m} = \dfrac{1+\gamma_{2D}}{1+\gamma_{2E}}$, then the following two lemmas can be derived.

Lemma 1. The exact cumulative distribution function (CDF) of T_{2m} is given as

$$\begin{aligned} F_{T_{2m}}(z) &= \sum_{n=0}^{N} \binom{N}{n} (-1)^n \cdot \\ &\left[\begin{aligned} &\exp\left(-\frac{n\Omega_{R_m D}(z-1)}{P_T}\right)\left(1-\exp\left(-\frac{\Omega_{R_m P}Q}{P_T}\right)\right) \\ &+ \frac{\Omega_{R_m P}P_T}{\Omega_{R_m P}P_T + n\Omega_{R_m D}(z-1)} \\ &\times \exp\left(-\frac{n\Omega_{R_m D}(z-1)+\Omega_{R_m P}Q}{P_T}\right) \end{aligned} \right] \\ &\times \sum_{k=1}^{K} \binom{K}{k} (-1)^{k+1} \frac{k\Omega_{R_m E}}{n\Omega_{R_m D} z + k\Omega_{R_m E}}. \end{aligned} \tag{7}$$

Proof:

Let $x_k \equiv |h_{R_m E_k}|^2$ and $y \equiv |h_{R_m P}|^2$, then the CDF of T_{2m} conditioned on x_k and y can be computed as

$$F_{T_{2m}}(z|x_k,y) = \Pr\left(\frac{1+\max_{n=1,\dots,N}\min(P_T,Q/y)|h_{R_mD_n}|^2}{1+\max_{k=1,\dots,K}\min(P_T,Q/y)x_k}<z\right) = F_U\left(\frac{z-1}{\min(P_T,Q/y)}+z\max_{k=1,\dots,K}x_k\right), \quad (8)$$

where $U\equiv\max_{n=1,\dots,N}|h_{R_mD_n}|^2$ and the CDF of U can be written as

$$F_U(u)=\sum_{n=0}^{N}\binom{N}{n}(-1)^n\exp(-n\Omega_{R_mD}u). \quad (9)$$

Substituting (9) into (8), we have

$$F_{T_{2m}}(z|x_k,y)=\sum_{n=0}^{N}\binom{N}{n}(-1)^n \exp\left(-n\Omega_{R_mD}\left(\frac{z-1}{\min(P_T,Q/y)}+z\max_{k=1,\dots,K}x_k\right)\right). \quad (10)$$

Next, the CDF of T_{2m} conditioned only on y is computed as

$$F_{T_{2m}}(z|y)=\int_0^\infty\sum_{n=0}^{N}\binom{N}{n}(-1)^n \exp\left(-n\Omega_{R_mD}\left(\frac{z-1}{\min(P_T,Q/y)}+zx\right)\right)f_X(x)dx, \quad (11)$$

where $X\equiv\max_{k=1,\dots,K}x_k$ and the PDF of X is given as

$$f_X(x)=\sum_{k=1}^{K}\binom{K}{k}(-1)^{k+1}k\Omega_{R_mE}\exp(-k\Omega_{R_mE}x). \quad (12)$$

Substituting (12) into (11) and integrating (11) with respect to x, we have

$$F_{T_{2m}}(z|y)= \left(\sum_{n=0}^{N}\binom{N}{n}(-1)^n\exp\left(-n\Omega_{R_mD}\frac{z-1}{\min(P_T,Q/y)}\right)\right) \times\left(\sum_{k=1}^{K}\binom{K}{k}(-1)^{k+1}\frac{k\Omega_{R_mE}}{n\Omega_{R_mD}z+k\Omega_{R_mE}}\right) \quad (13)$$

Finally, the CDF of T_{2m} with respect to y is computed as

$$F_{T_{2m}}(z) =\sum_{n=0}^{N}\binom{N}{n}(-1)^n \cdot \left[\exp\left(-\frac{n\Omega_{R_mD}(z-1)}{P_T}\right)\times\int_0^{Q/P_T}\Omega_{R_mP}\exp(-\Omega_{R_mP}y)dy + \int_{Q/P_T}^{\infty}\Omega_{R_mP}\exp\left(-\frac{n\Omega_{R_mD}(z-1)y}{Q}\right)\exp(-\Omega_{R_mP}y)dy\right] \times\sum_{k=1}^{K}\binom{K}{k}(-1)^{k+1}\frac{k\Omega_{R_mE}}{n\Omega_{R_mD}z+k\Omega_{R_mE}} \quad (14)$$

After some manipulations, the CDF of T_{2m} is derived as (7).

Lemma 2. The exact CDF of T_{1m} is given as

$$F_{T_{1m}}(z)=1-\sum_{k=1}^{K}\binom{K}{k}(-1)^{k+1}\frac{k\Omega_{SE}}{\Omega_{SR_m}z+k\Omega_{SE}} \times\left[\exp\left(-\frac{\Omega_{SR_m}(z-1)}{P_T}\right)\left(1-\exp\left(-\frac{\Omega_{SP}Q}{P_T}\right)\right) +\frac{\Omega_{SP}P_T}{\Omega_{SP}P_T+\Omega_{SR_m}(z-1)}\exp\left(-\frac{\Omega_{SR_m}(z-1)+\Omega_{SP}Q}{P_T}\right)\right] \quad (15)$$

Proof:

The CDF of T_{1m} follows directly from (7) by exchanging the parameters Ω_{R_mD} to Ω_{SR_m}, Ω_{R_mE} to Ω_{SE}, Ω_{R_mP} to Ω_{SP} with single antenna at R_m.

Proposition 1. The exact secrecy outage probability of the proposed secondary system is given as

$$P_{out}^{s} = 1-\sum_{i=1}^{M}(-1)^{i+1}\sum_{\substack{m_1=\cdots=m_i=1\\ m_1<\cdots<m_i}}^{M}\prod_{t=1}^{i}\sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1} \left[\exp\left(-\frac{n\Omega_{R_{m_t}D}(\rho-1)}{P_T}\right)-\frac{n\Omega_{R_{m_t}D}(\rho-1)}{\Omega_{R_{m_t}P}P_T+n\Omega_{R_{m_t}D}(\rho-1)} \times\exp\left(-\frac{n\Omega_{R_{m_t}D}(\rho-1)+\Omega_{R_{m_t}P}Q}{P_T}\right)\right] \times\sum_{k=1}^{K}\binom{K}{k}(-1)^{k+1}\frac{k\Omega_{R_{m_t}E}}{n\Omega_{R_{m_t}D}\rho+k\Omega_{R_{m_t}E}} \times\sum_{k=1}^{K}\binom{K}{k}(-1)^{k+1}\frac{k\Omega_{SE}}{\Omega_{SR_{m_t}}\rho+k\Omega_{SE}}$$

$$\times\left[\begin{array}{l}\exp\left(-\frac{n\Omega_{R_{m_t}D}(\rho-1)}{P_T}\right)-\frac{\Omega_{R_{m_t}}(\rho-1)}{\Omega_{SP}P_T+\Omega_{SR_{m_t}}(\rho-1)} \\ \times\ \exp\left(-\frac{\Omega_{SR_{m_t}}(\rho-1)+\Omega_{SP}Q}{P_T}\right)\end{array}\right] \tag{16}$$

where $\rho\equiv 2^{2R_{th}}$.

Proof:

When T_{1m} and T_{2m} are independent, we obtain the outage probability by combining (6), (7) and (15) as

$$P_{out}^{s}= \prod_{m=1}^{M}\left(F_{T_{1m}}(\rho)+F_{T_{2m}}(\rho)-F_{T_{1m}}(\rho)F_{T_{2m}}(\rho)\right) \tag{17}$$

After some manipulations, we can obtain the result in (16).

Lemma 3. An asymptotic expression for P_{out}^{s} when $P_T\to\infty$ is given as

$$\begin{aligned}P_{out}^{\infty}= & \\ 1-\sum_{i=1}^{M}(-1)^{i+1}&\sum_{\substack{m_1=\cdots=m_i=1\\ m_1<\cdots<m_i}}^{M}\prod_{t=1}^{i}\sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1} \\ \times\sum_{k=1}^{K}\binom{K}{k}&(-1)^{k+1}\frac{k\Omega_{R_{m_t}E}}{n\Omega_{R_{m_t}D}+k\Omega_{R_{m_t}E}} \\ \times\sum_{i=1}^{M}\binom{K}{k}&(-1)^{k+1}\frac{k\Omega_{SE}}{\Omega_{SR_{m_t}}\rho+k\Omega_{SE}}\end{aligned} \tag{18}$$

Proof:

It is not difficult to obtain (18) by letting P_T to infinity in (16).

Ⅳ. SIMULATION RESULTS

In this section, we use the closed-form expressions for the secrecy outage probability in (16) and (18) to evaluate the system performance. In particular, we investigate the impact of the number of relay nodes, the number of antennas at the destination D, and number of antennas at the eavesdropper E. We assume that the source S, the relay R_m, the destination D, the eavesdropper E, and the primary receiver P are located at $(0,0)$, $(x_m,0)$, $(1,0)$, $(1,-0.5)$, and $(1,0.5)$, respectively. The corresponding distances between certain two nodes are calculated as $d_{SR_m}=x_m$, $d_{SE}=d_{SP}=\sqrt{1.25}$, $d_{R_mD}=1-x_m$, and $d_{R_mE}=d_{R_mP}=\sqrt{(1-x_m)^2+0.25}$. The path loss exponent β is assumed to be equal to 4.

In Fig. 2, we investigate the effect of the maximum transmit power P_T on the secrecy outage probability when the number of antennas at the destination $N=1$, the threshold $R_{th}=0.3$, and the peak interference $Q=2P_T$. M relays are assumed to be deployed in the same location $(0.5,0)$. As expected, when the number of relay nodes M increases, the secrecy outage probability is found to decrease. In contrast, when the number of antennas at the eavesdropper increases, the secrecy outage probability is found to increases, since the chance of overhearing will increase accordingly. Fig. 2 also verifies that the simulation results and analytical results have an exact agreement.

In Fig. 3, the number of relays are fixed to 3 and they are assumed to be located at $(0.6,0)$. The parameters R_{th} and Q are set to 0.3 and 2, respectively. It can be seen that the secrecy outage

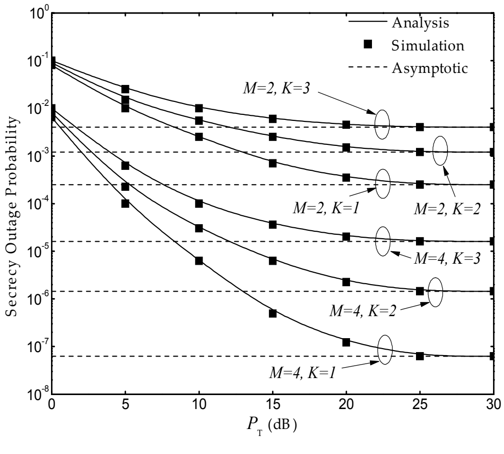

Fig. 2. Secrecy outage probability versus P_T for $M=2, 4$ and $K=1, 2, 3$ ($R_{th}=0.3$, $Q/P_T=2$, $x_m=0.5$, $N=1$).

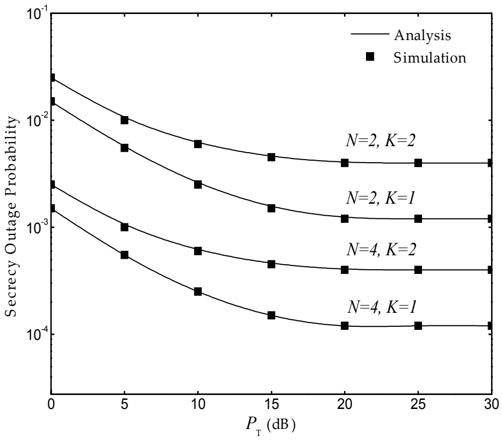

Fig. 3. Secrecy outage probability versus P_T for $N=2, 4$ and $K=1, 2$ ($R_{th}=0.3$, $Q/P_T=2$, $x_m=0.6$, $M=3$).

probability decreases as the number of antennas at the destination increases. Similarly to Fig. 2, the secrecy outage probability is seen to increase as the number of antennas at the eavesdropper increases.

V. Conclusion

In this paper, we have considered an optimal relay selection scheme with multiple antennas at the destination and eavesdropper in a cognitive radio networks. We have derived exact analytical expressions for the secrecy outage probability in the presence of multiple relay nodes. Numerical results have been provided to validate the analysis. It has been shown that in order to improve the performance of the system, it is necessary to distribute many relay nodes and multiple antennas at the destination rather than to increase the transmit power of the source.

References

[1] J. Mitola and J. Q. Magire, Jr., "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13-18, Aug. 1999.

[2] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[3] J. P. Seo, C. S. Yang, and J. H. Chung, "An active interference management scheme for cognitive radio systems," *J. KICS*, vol. 38B, no. 10, pp. 843-850, Oct. 2013.

[4] R. M. Choe and Y. S. Byun, "User selection scheme for the performance improvement of the secondary system in cognitive radio systems using underlay mode," *J. KICS*, vol. 38A, no. 3, pp. 249-257, Jan. 2013.

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

[6] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inform. Theory 2006 (ISIT 2006)*, pp. 356-360, Seattle, USA, July 2006.

[7] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. Anual Allerton Conf. Commun., Control, Computing,* UIUC, Ilinois, USA, Sept. 2008

[8] V. Aggarwal, L. Sankar, A. Calderbank, and H. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP J. Wirel. Commun. Net.,* pp. 1-14, 2009.

[9] Y. Pei, Y. C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wirel. Commun.*, vol. 9, no. 4, pp. 1494-1502, Apr. 2010.

[10] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877-1886, Jun. 2010.

[11] Y. Pei, Y. C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.,* vol. 59, no. 4, pp.

1683-1693, Apr. 2011.

[12] A. Bletsas, H. Shin, M. Z. Win, and A. Lippman, "Cooperative diversity with opportunistic relaying," in *Proc. IEEE Wirel. Commun. Net. Conf. (IEEE WCNC 2006)*, pp. 1034-1039, Las Vegas, USA, Apr. 2006.

[13] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wirel. Commun.*, vol. 6, no. 9, pp. 3450-3460, Sept. 2007.

[14] J. B. Cho, S. J. Jang, W. S. Jung, and J. M. Kim "Projection of spatial correlation-based antenna selection for cognitive radio systems in correlated channels," *J. KICS*, vol. 37A, no. 1, pp. 8-16, Jan. 2012.

[15] P. Gopala, L. Lai, and H. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

누엔반딘 (Van-Dinh Nguyen)

2012년 2월 : 베트남 호치민 과학기술대 (공학사)

2013년 3월~현재 : 숭실대학교 전자공학과 석사과정

<관심분야> 통신시스템, 통신이론, Cognitive Radio, Massive MIMO

김 현 민 (Hyeon-Min Kim)

2012년 8월 : 숭실대학교 정보통신전자공학부 (공학사)

2012년 9월~현재 : 숭실대학교 전자공학과 석·박사통합과정

<관심분야> 통신시스템, 통신이론, D2D 통신

신 오 순 (Oh-Soon Shin)

1998년 2월 : 서울대학교 전기공학부 (공학사)

2000년 2월 : 서울대학교 전기공학부 (공학석사)

2004년 2월 : 서울대학교 전기·컴퓨터공학부 (공학박사)

2004년 3월~2005년 9월 : 미국 Harvard University 박사후연구원

2006년 4월~2007년 8월 : 삼성전자 통신연구소 책임연구원

2007년 9월~현재 : 숭실대학교 정보통신전자공학부 부교수

<관심분야> 통신시스템, 통신이론, 통신신호처리