Secrecy Rate of Channel-Aware Randomized Secure Transmission Schemes in Multicarrier Systems

Jinho Choi
School of EECS, GIST
Email: *jchoi0114@gist.ac.kr*

***Abstract*—In this paper, we study channel-aware (CA) randomization for secure transmissions in a multicarrier system based on partial channel state information (CSI). In order to see the performance gain by CA randomization, we consider the secrecy rate and show that *i)* a positive secrecy rate can be obtained even if the channel to an adversary is stochastically more capable than the channel to a legitimate receiver and *ii)* the normalized secrecy rate can increase with the number of subcarriers. More importantly, it is shown that there is an additional gain due to CA randomization that allows a growth rate of the normalized secrecy faster than linear.**

***Index Terms*—physical layer security; channel-aware randomization; multicarrier systems**

I. Introduction

Physical layer security (PLS) is to exploit transmission channels for secure communications based on information-theoretic approaches [1]. In PLS, it is important to find the secrecy capacity or rate, which is the maximum data rate with perfect secrecy [2], for wiretap channels [3] [4] [5]. Channel coding plays a crucial role in PLS to achieve the secrecy rate [6] [7] and various approaches are proposed with existing codes, e.g., [8] [9].

While PLS will be more widely applied to various secure transmissions, there are key techniques that can improve the performance of PLS as follows.

Randomization: In [10] [11], randomized encryption is considered to improve cryptographic security at the cost of increasing bandwidth. In [12], an information-theoretic security evaluation is studied for a certain randomized encryption method. Wyner's coding schemes [3] [8] [13] [14] for wiretap channels can also be seen as randomization techniques for secure transmissions.

Channel Awareness: In wireless communications, randomization techniques can be effectively employed in conjunction with known channel state information (CSI) or channel awareness. The legitimate transmitter can have the CSI based on the channel reciprocity in time division duplexing (TDD) mode. This has been considered in various PLS schemes, e.g., for channel-aware (CA) encryption in wireless sensor networks (WSNs) in [15] [16] and beamforming with jamming signals to make the received signal at eavesdroppers deliberatively noisy in [17].

Multicarrier Systems: For a wideband channel, orthogonal frequency division multiplexing (OFDM) can be employed. In [18], the secrecy rate has been studied for OFDM or multicarrier systems. In [19], secret key transmission in a multicarrier system is considered to exploit the property that the samples of OFDM signals in the time domain look similar to Gaussian jamming signals, which makes an eavesdropper difficult to detect jamming signals. In [20], a channel reciprocity based secret key transmission scheme is proposed for a multicarrier system by exploiting the randomness of frequency-selective fading channels. Using sorted subcarrier interleaving, a secure transmission scheme for OFDM is proposed in [21]. To improve the security of compressive sensing (CS) based encryption, a PLS method is proposed in [22], which also relies on the rich randomness of frequency-selective fading channels.

In this paper, we study CA randomization for secure transmissions in a multicarrier system. Throughout the paper, it is assumed that a legitimate transmitter, called Alice, and a legitimate receiver, called Bob, know the CSI from Alice to Bob. The knowledge of partial CSI is exploited for randomization in secure transmissions. Thus, the proposed approach is similar to that in [21]. However, the main difference is that random signals are transmitted to confuse Eve in the proposed CA randomization, while it is not considered in [21]. To see the performance gain by CA randomization, we consider the secrecy rate and show that

i) a positive secrecy rate can be obtained even if Eve's channel is stochastically more capable than Bob's channel,

ii) the normalized secrecy rate can increase with the number of subcarriers, and

iii) there is an additional gain due to CA randomization that allows a growth rate of the normalized secrecy faster than linear.

To the best of our knowledge, the last finding is new and interesting as it shows the advantage of a wideband system over a narrowband system in terms of the secrecy rate. Although it is not studied in this paper, CA randomization can be applied to a multiple-input multiple-output (MIMO) channel that is converted into multiple parallel channels [1] [23].

Notation: The superscripts T and H denote the transpose and complex conjugate transpose, respectively. For a vector $\mathbf{a}$, $\mathrm{diag}(\mathbf{a})$ is the diagonal matrix with the diagonal elements from $\mathbf{a}$. For a matrix $\mathbf{X}$ (a vector $\mathbf{x}$), $[\mathbf{X}]_n$ ($[\mathbf{x}]_n$) represents

This work was supported by Agency for Defense Development (the title of the project is *PHY/MAC-NETWORK Technologies Against Jamming Attack and Eavesdropping*.

the nth column (element, resp.). If $\mathcal{A}$ is a set of indices, $[\mathbf{x}]_{\mathcal{A}}$ is a subvector of $\mathbf{x}$ obtained by taking the corresponding elements. $\mathbb{E}[\cdot]$ denotes the statistical expectation. $\mathcal{CN}(\mathbf{a}, \mathbf{R})$ represents the distribution of circularly symmetric complex Gaussian (CSCG) random vectors with mean vector $\mathbf{a}$ and covariance matrix $\mathbf{R}$.

II. System Model and Assumptions

Suppose that there is a pair of legitimate transmitter and receiver, called Alice and Bob, respectively, and an adversary (or an eavesdropper), called Eve. We consider a multicarrier system for secure transmissions from Alice to Bob with L subcarriers over a wideband channel. Suppose that Alice transmits a block of signal over L subcarriers, which is denoted by $\mathbf{s} \in \mathbb{C}^{L \times 1}$. Then, the received signal at Bob is given by

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{n}, \tag{1}$$

where $\mathbf{n} \sim \mathcal{CN}(0, N_0 \mathbf{I})$ is the background noise vector and $\mathbf{H} = \mathrm{diag}(H_0, \ldots, H_{L-1})$ is a diagonal (frequency-domain) channel matrix. Here, H_l denotes the channel coefficient over the lth subcarrier from Alice to Bob.

Similarly, the received signal at Eve is given by

$$\mathbf{z} = \mathbf{G}\mathbf{s} + \mathbf{w}, \tag{2}$$

where $\mathbf{w} \sim \mathcal{CN}(0, N_0 \mathbf{I})$ is the background noise vector and $\mathbf{G} = \mathrm{diag}(G_0, \ldots, G_{L-1})$ is a diagonal (frequency-domain) channel matrix. Here, G_l represents the channel coefficient over the lth subcarrier from Alice to Eve. In Fig. 1, we illustrate the system model with Alice, Bob, and Eve.

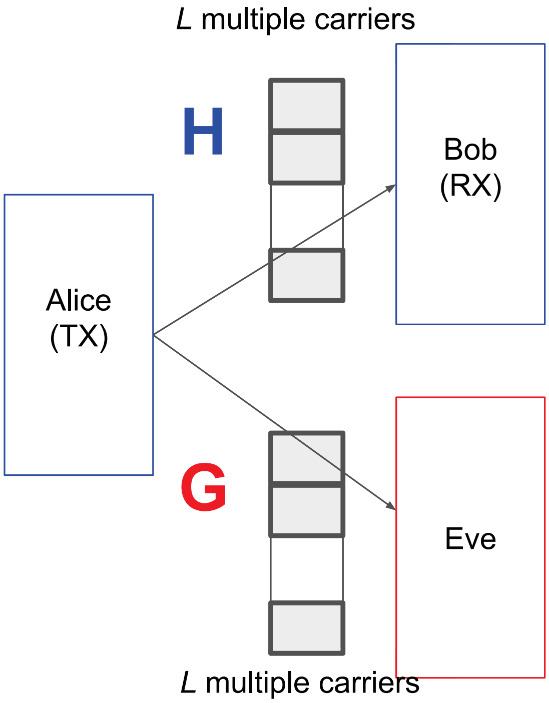


Fig. 1. A wiretap channel model for multicarrier systems with a pair of legitimate transmitter (Alice) and receiver (Bob) and an eavesdropper (Eve).

Throughout this paper, we consider the following assumption.

A) The channel coefficients in the frequency domain are

$$H_l \sim \mathcal{CN}(0, \sigma_H^2) \text{ and } G_l \sim \mathcal{CN}(0, \sigma_G^2), \tag{3}$$

where σ_H^2 and σ_G^2 the (frequency-domain) channel power gains of Bob's and Eve's channels, respectively, that absorb the large scale fading terms. In addition, H_l and G_l are independent.

Let $\alpha_l = |H_l|^2$ and $\beta_l = |G_l|^2$. We also assume TDD mode for CA secure transmissions [24] [22]. Bob can transmit a pilot signal to allow Alice to estimate the Bob's CSI, $\mathbf{H}$. In addition, Alice sends a pilot signal to Bob so that Bob can estimate his CSI, $\mathbf{H}$. Note that due to the pilot signal from Alice, Eve can also estimate her CSI, $\mathbf{G}$. Therefore, throughout the paper, we assume that both Alice and Bob know $\mathbf{H}$, but not $\mathbf{G}$, and Eve knows $\mathbf{G}$, but not $\mathbf{H}$.

III. Secrecy Rates for CA Randomized Transmissions

In this section, in order to see the performance gain by CA randomization, we study the secrecy rates under the assumption of $\mathbf{A}$ for three different schemes: *i)* the conventional scheme (without CA); *ii)* the CA scheme; *iii)* the CA randomized scheme.

A. Secrecy Rate of a Multicarrier System

From (1) and (2), the ergodic sum rates at Bob and Eve, denoted by R_B and R_E, can be found as

$$\begin{aligned} R_\mathrm{B} &= \sum_{l=0}^{L-1} \mathbb{E}\left[\log_2\left(1 + \frac{P\alpha_l}{N_0}\right)\right] \\ R_\mathrm{E} &= \sum_{l=0}^{L-1} \mathbb{E}\left[\log_2\left(1 + \frac{P\beta_l}{N_0}\right)\right], \end{aligned} \tag{4}$$

where P is the transmission power per subcarrier. Since the conditional secrecy rate for given $\mathbf{H}$ and $\mathbf{G}$ is a secrecy rate of Gaussian wire-tap channel [1] [25], a lower-bound on ergodic secrecy rate becomes

$$\begin{aligned} R_\mathrm{S} &= \mathbb{E}\left[\left(\sum_{l=0}^{L-1} \log_2(1 + P\alpha_l/N_0) - \log_2(1 + P\beta_l/N_0)\right)^+\right] \\ &\geq \underline{R}_\mathrm{S} = (R_\mathrm{B} - R_\mathrm{E})^+, \end{aligned} \tag{5}$$

where $(x)^+ = \max\{0, x\}$ and the inequality is due to Jensen's inequality. Hereafter, unless stated otherwise, the secrecy rate means as the ergodic secrecy rate. If Eve's CSI, $\{\beta_l\}$, is available, the power allocation can be considered to maximize $\underline{R}_\mathrm{S}$ at Alice as in [18]. However, since Eve's CSI may not be available, we do not assume any knowledge of Eve's CSI throughout the paper, as mentioned earlier.

From [26], it can be shown that

$$\begin{aligned} \Pi(x) &= \int_0^\infty \log_2(1 + xt) e^{-t} dt \\ &= \frac{1}{\ln 2} e^{1/x} E_1(1/x), \end{aligned} \tag{6}$$

where $E_1(x) = \int_1^\infty \frac{e^{-tx}}{t} dt$. Thus, from (4) under the assumption of $\mathbf{A}$, we can show that

$$R_{\rm B} = L\Pi(\gamma_{\rm B}) \text{ and } R_{\rm E} = L\Pi(\gamma_{\rm E}),$$

where $\gamma_{\rm B} = \frac{\sigma_H^2 P}{N_0}$ and $\gamma_{\rm E} = \frac{\sigma_G^2 P}{N_0}$ are the signal-to-noise ratios (SNRs) at Bob and Eve, respectively. Since $\Pi(x)$ is an increasing function of x, we can claim that

$$\underline{R}_{\rm S} = L\left(\Pi(\gamma_{\rm B}) - \Pi(\gamma_{\rm E})\right)^+ > 0, \text{if } \gamma_{\rm B} > \gamma_{\rm E}. \tag{7}$$

This implies that a positive secrecy rate can be achieved if Bob's channel is better than Eve's channel in terms of their SNRs, which is often difficult to achieve as Eve can be close to Alice for better eavesdropping.

B. Secrecy Rate of CA Scheme

Suppose that Alice has the CSI to Bob, i.e., $\{H_l\}$. Alice can transmit signals through a subset of the subcarriers of the power gains greater than or equal to τ. Here, τ is positive and a design parameter. The resulting simple CA scheme relies on the following partial CSI:

$$D_l = \mathbb{1}(\alpha_l \ge \tau),$$

where $\mathbb{1}(S)$ is the indicator function that becomes 1 if the statement S is true and 0 otherwise. In this case, the sum rate at Bob becomes

$$R_{\rm B;CA}(\tau) = \sum_{l=0}^{L-1} \mathbb{E}\left[D_l \log_2\left(1 + \frac{\alpha_l P}{N_0}\right)\right]. \tag{8}$$

For convenience, let

$$\mathcal{I} = \{l \,|\, D_l = 1\} = \{l \,|\, \alpha_l \ge \tau\}.$$

A lower-bound on the secrecy rate of the CA scheme becomes

$$\underline{R}_{\rm S;CA}(\tau) = \left(R_{\rm B;CA}(\tau) - R_{\rm E;CA}(\tau)\right)^+, \tag{9}$$

where $R_{\rm E;CA}(\tau)$ is the sum rate at Eve, which is given by

$$R_{\rm E;CA}(\tau) = \sum_{l=0}^{L-1} \mathbb{E}\left[D_l \log_2\left(1 + \frac{\beta_l P}{N_0}\right)\right]. \tag{10}$$

Lemma 1. *Under the assumption of* $\mathbf{A}$*, we have*

$$R_{\rm B;CA}(\tau) = Le^{-\bar\tau}\left(\log_2\left(1+\gamma_\tau\right) + \Pi\left(\frac{\gamma_{\rm B}}{1+\gamma_\tau}\right)\right) \tag{11}$$

$$R_{\rm E;CA}(\tau) = Le^{-\bar\tau}\Pi(\gamma_{\rm E}), \tag{12}$$

where $\bar\tau = \frac{\tau}{\sigma_H^2}$ *and* $\gamma_\tau = \frac{\tau P}{N_0} = \bar\tau\gamma_{\rm B}$.

Proof: See Appendix A. ■

Substituting (11) and (12) into (9), we have

$$\begin{aligned}\underline{R}_{\rm S;CA}(\tau) &= \left(R_{\rm B;CA}(\tau) - R_{\rm E;CA}(\tau)\right)^+ \\ &= Le^{-\bar\tau}\Bigg(\log_2(1+\gamma_\tau) + \Pi\left(\frac{\gamma_{\rm B}}{1+\gamma_\tau}\right) \\ &\qquad - \Pi(\gamma_{\rm E})\Bigg)^+, \end{aligned} \tag{13}$$

which is a closed-form expression for the secrecy rate of the CA scheme. From (13), it can be shown that $\underline{R}_{\rm S;CA}(\tau)$ can be positive even if Eve's channel is stochastically more capable than Bob's channel.

Lemma 2. *Under the assumption of* $\mathbf{A}$*, if*

$$\bar\tau \ge \sqrt{1 + \left(\frac{1+\gamma_{\rm E}}{\gamma_{\rm B}}\right)^2} - \left(1 + \frac{1}{\gamma_{\rm B}}\right), \tag{14}$$

the secrecy rate of the CA scheme becomes positive, i.e., $\underline{R}_{\rm S;CA}(\tau) > 0$.

Proof: See Appendix B. ■

Lemma 2 demonstrates that although $\gamma_{\rm E} > \gamma_{\rm B}$, it is possible to achieve a positive secrecy rate by exploiting the partial CSI in the CA scheme.

C. Ergodic Secrecy Rate of CA Randomized Scheme

In the CA scheme, Alice does not transmit any signals through the subcarriers of the channel power gains less than τ, i.e., there is no signal through subcarrier $l \in \mathcal{I}^c$. In this case, Eve also knows that those subcarriers do not deliver any useful information. Thus, in order to improve the secrecy rate further by confusing[1] Eve, Alice can transmit random signals through subcarrier $l \in \mathcal{I}^c$, which results in a CA randomized scheme.

Suppose that Alice transmits a random signal through subcarrier $l \in \mathcal{I}^c$, which has the same statistical properties as the secret signal transmitted through a subcarrier in $\mathcal{I}$. Since Bob knows $\mathcal{I}$, he disregards the signals transmitted through the subcarriers of $\mathcal{I}^c$. On the other hand, since Eve does know $\mathcal{I}$, she has to guess which subcarriers deliver the secret signal. Thus, Eve may need to choose M subcarriers out of L subcarriers, where $M = |\mathcal{I}|$, under the assumption that M is known to Eve. This assumption is might be optimistic to Eve (or pessimistic to Bob and Alice) as Eve does not know Bob's CSI as well as τ. For given M, the achievable rate at Eve can be found. However, since M is a random variable (that depends on $\{H_l\}$), this achievable rate is a conditional random variable. Thus, the average achievable rate at Eve is to be found by taking the expectation with respect to M, which is shown in the following result.

Lemma 3. *Suppose that random signals are transmitted through the subcarriers* $l \in \mathcal{I}^c$ *such that decoding gives rise to a different codeword from any different selection of* M *subcarriers out of* L *subcarriers. Under the assumption of* $\mathbf{A}$ *and the assumption that* M *is known to Eve, the achievable rate at Eve in the CA randomized scheme is given by*

$$R_{\rm E;CAR}(\tau) = \frac{1 + (L-1)e^{-\bar\tau}}{L} R_{\rm E;CA}(\tau). \tag{15}$$

Proof: See Appendix C. ■

Since the achievable rate at Bob in the CA randomized scheme, which is denoted by $R_{\rm B;CAR}(\tau)$, is the same as that

[1] The way to use random signals is different from that in [17] [27] [28] where random signals (or artificial noise) are used to generate interfering signal at Eve so that her SNR becomes lower.

in the CA scheme, from (15), we can show that the CA randomization can increase the lower-bound on the secrecy rate as follows:

$$\underline{R}_{\mathrm{S;CAR}}(\tau) = (R_{\mathrm{B;CAR}}(\tau) - R_{\mathrm{E;CAR}}(\tau))^+ \\ \geq \underline{R}_{\mathrm{S;CA}}(\tau) = (R_{\mathrm{B;CA}}(\tau) - R_{\mathrm{E;CA}}(\tau))^+ \quad (16)$$

where $R_{\mathrm{B;CAR}}(\tau) = R_{\mathrm{B;CA}}(\tau)$, because $R_{\mathrm{E;CAR}}(\tau) \leq R_{\mathrm{E;CA}}(\tau)$ from (15). From (11) and (15), it follows

$$\frac{\underline{R}_{\mathrm{S;CAR}}(\tau)}{L} = \left(e^{-\bar{\tau}} \left(\log_2(1+\gamma_\tau) + \Pi\left(\frac{\gamma_{\mathrm{B}}}{1+\gamma_\tau}\right) \right. \right. \\ \left. - e^{-\bar{\tau}} \Pi(\gamma_{\mathrm{E}}) \right) \\ \left. - \frac{e^{-\bar{\tau}}(1-e^{-\bar{\tau}})\Pi(\gamma_{\mathrm{E}})}{L} \right)^+ . \quad (17)$$

From the last term on the right-hand-side (RHS) in (17), we can observe that the normalized lower-bound on the secrecy rate of the CA randomized scheme is improved as L increases. That is, $\frac{\underline{R}_{\mathrm{S;CAR}}(\tau)}{L}$ increases with L, while the normalized lower-bounds on the secrecy rates of the CA scheme and the conventional scheme are invariant with respect to L as shown in (7) and (13), respectively. Consequently, we can see that the CA randomization can provide additional performance gain for a wider bandwidth (i.e., more subcarriers).

IV. Numerical Results

In this section, we present numerical results to show the (lower-bounds[2]) on the secrecy rates of the conventional scheme, the CA scheme, and the CA randomized scheme under the assumption of **A**.

Fig. 2 shows the normalized secrecy rates, $\frac{R_{\mathrm{S}}}{L}$, of the three schemes for various values of γ_{E} when $L = 128$, $\gamma_{\mathrm{B}} = 10$ dB, and $\bar{\tau} = 0.5$. If $\gamma_{\mathrm{E}} > \gamma_{\mathrm{B}}$, the secrecy rate of the conventional scheme becomes 0, while the CA schemes can provide positive secrecy rates. We can observe that the secrecy rate of the CA randomized scheme is higher than that of the CA scheme, which confirms (16).

In Fig. 3 (a), the secrecy rates of the CA scheme and CA randomized scheme are shown for different values of $\bar{\tau}$ when $L = 128$ and $\gamma_{\mathrm{B}} = \gamma_{\mathrm{E}} = 10$ dB. It is possible to maximize the secrecy rate by adjusting τ or $\bar{\tau}$ if σ_G^2 is known (which allows us to determine γ_{rmE}). With optimal values of $\bar{\tau}$ (that are obtained for each value of γ_{E}), we can show that the secrecy rates can be improved as in Fig. 3 (b). Note that in practice γ_{E} may not be known. In this case, we may need to set a target value of γ_{E} (which is the maximum allowed Eve's SNR for secure transmissions at the secrecy rate obtained by optimized $\bar{\tau}$).

In order to see the impact of L on the secrecy rate, we show the normalized secrecy rates for different values of L in Fig. 4 when $\gamma_{\mathrm{B}} = \gamma_{\mathrm{E}} = 10$ dB. Clearly, in this case, the secrecy rate of the conventional scheme is zero. As shown in (13), the normalized secrecy rate of the CA scheme is independent of L for both fixed $\bar{\tau} = 1$ and optimized $\bar{\tau}$. On the other hand, the normalized secrecy rate of the CA randomized scheme can increase with L.

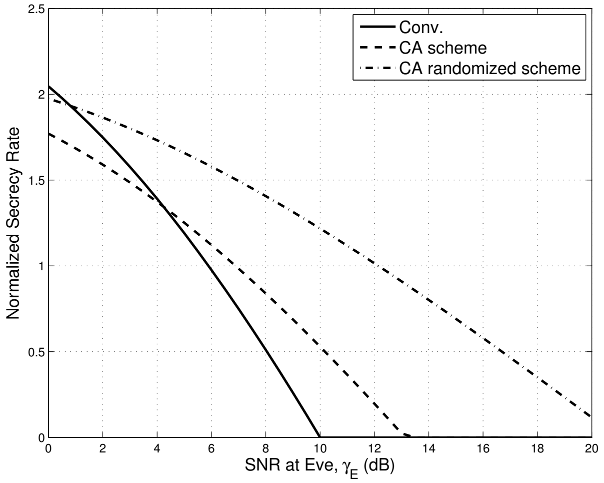
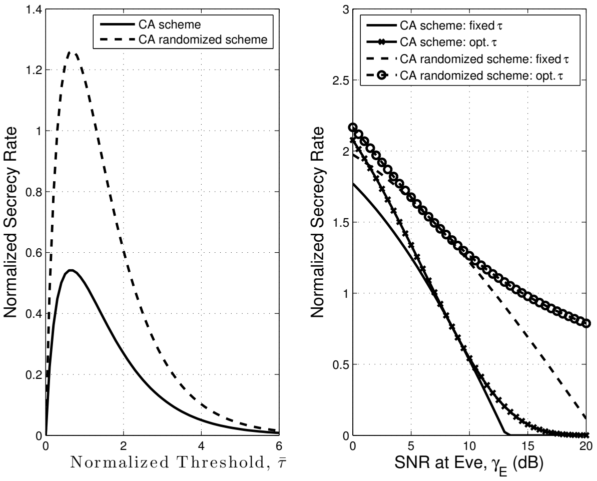


Fig. 2. Normalized secrecy rates of the three schemes for various values of γ_{E} when $L = 128$, $\gamma_{\mathrm{B}} = 10$ dB, and $\bar{\tau} = 0.5$.



(a) (b)

Fig. 3. Normalized secrecy rates of the CA schemes when $L = 128$ and $\gamma_{\mathrm{B}} = \gamma_{\mathrm{E}} = 10$ dB: (a) normalized secrecy rate versus $\bar{\tau}$; (b) normalized secrecy rates with fixed $\bar{\tau} = 0.5$ and optimized $\bar{\tau}$.

V. Concluding Remarks

In this paper, we studied CA randomization for a multi-carrier system. In order to see the performance gain of CA randomization, we derived the secrecy rates of three different schemes including the CA randomized scheme. It was shown that the secrecy rate can be positive even if Bob's channel is more degraded than Eve's channel in the CA scheme and can be further improved by CA randomization. In particular, the CA randomization can provide additional performance gain that increases with the number of subcarriers.

[2] For convenience, we omit the lower-bound in this section.

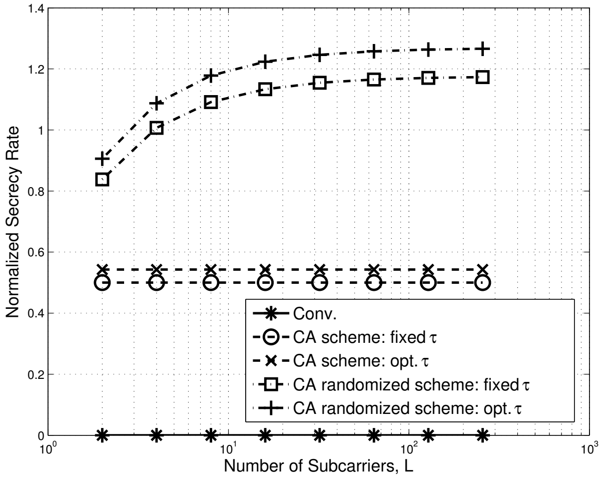


Fig. 4. Normalized secrecy rates versus L when $\gamma_\mathrm{B} = \gamma_\mathrm{E} = 10$ dB.

Appendix A
Proof of Lemma 1

Let $f_\alpha(x)$ denote the probability density function (pdf) of $x = \alpha_l$. Then, we can show that

$$\mathbb{E}\left[D_l \log_2\left(1+\frac{P\alpha_l}{N_0}\right)\right] = \int_\tau^\infty \log_2\left(1+\frac{Px}{N_0}\right) f_H(x)dx$$
$$= e^{-\bar{\tau}} \int_0^\infty \log_2\left(u+\gamma_\mathrm{B} t\right) e^{-t} dt,$$

where $u = 1 + \bar{\tau}\gamma_\mathrm{B} = 1 + \gamma_\tau$. Using (6), we can show that

$$\int_0^\infty \log_2\left(u+\gamma_\mathrm{B} t\right) e^{-t} dt = \log_2 u + \Pi\left(\frac{\gamma_\mathrm{B}}{u}\right)$$
$$= \log_2 u + \Pi\left(\frac{\gamma_\mathrm{B}}{1+\gamma_\tau}\right). \quad (18)$$

From this, we have $\mathbb{E}\left[D_l \log_2\left(1+\frac{\alpha_l}{N_0}\right)\right] = e^{-\bar{\tau}}\left(\log_2 u + \Pi\left(\frac{\gamma_\mathrm{B}}{1+\gamma_\tau}\right)\right)$, which results in (11).

Since D_l and G_l are independent and $\mathbb{E}[D_l] = \Pr(\alpha_l \ge \tau) = e^{-\bar{\tau}}$, it can be shown that

$$\mathbb{E}\left[D_l \log_2\left(1+\frac{\beta_l P}{N_0}\right)\right] = \mathbb{E}[D_l]\mathbb{E}\left[\log_2\left(1+\frac{\beta_l P}{N_0}\right)\right]$$
$$= e^{-\bar{\tau}}\Pi(\gamma_\mathrm{E}),$$

which leads to (12).

Appendix B
Proof of Lemma 2

From [29], we have the following inequalities:

$$\frac{1}{2}\ln\left(1+\frac{2}{x}\right) \le e^x E_1(x) \le \ln\left(1+\frac{1}{x}\right),$$

which lead to the following bounds on $\Pi(x)$:

$$\frac{1}{2}\log_2(1+2x) \le \Pi(x) \le \log_2(1+x).$$

Using this, from (11) and (12), we can have the following result:

$$\frac{R_{\mathrm{B;CA}}(\tau)}{R_{\mathrm{E;CA}}(\tau)} \ge \frac{R_{\mathrm{B;CA}}(\tau)}{Le^{-\bar{\tau}}\log_2(1+\gamma_\mathrm{E})}$$
$$\ge \frac{\log_2\sqrt{(1+\gamma_\tau)(1+\gamma_\tau+2\gamma_\mathrm{B})}}{\log_2(1+\gamma_\mathrm{E})}. \quad (19)$$

Thus, a sufficient condition that $\underline{R}_{\mathrm{S;CA}}(\tau)$ is positive is

$$\sqrt{(1+\gamma_\tau)(1+\gamma_\tau+2\gamma_\mathrm{B})} > 1+\gamma_\mathrm{E},$$

which is equivalent to

$$(\gamma_\tau+1)^2 + 2\gamma_\mathrm{B}(\gamma_\tau+1) - (\gamma_\mathrm{E}+1)^2 > 0. \quad (20)$$

Since $\gamma_\tau = \bar{\tau}\gamma_\mathrm{B}$, we can readily verify that (14) satisfies (20) through the quadratic formula, which completes the proof.

Appendix C
Proof of Lemma 3

Eve can perform decoding for all possible combinations of M subcarriers out of L subcarriers. Since she will have a different codeword from decoding for each combination, without any side information, Eve would not have any preference and would choose one of them as a correct one. This is equivalent to a random selection of M subcarriers. Thus, according to Property 2 in [30], we can show that

$$R_{\mathrm{E;CAR}}(\tau) = (1+(L-1)e^{-\bar{\tau}})e^{-\bar{\tau}}\Pi(\gamma_\mathrm{E}). \quad (21)$$

From (12) and (21), we can have (15).

References

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[2] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[3] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, October 1975.

[4] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, May 1978.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inform. Theory*, vol. 54, pp. 2515–2534, June 2008.

[6] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, “Coding for secrecy: An overview of error-control coding techniques for physical-layer security,” *IEEE Signal Processing Magazine*, vol. 30, pp. 41–50, September 2013.

[7] M. Bloch, M. Hayashi, and A. Thangaraj, “Error-control coding for physical-layer secrecy,” *Proceedings of the IEEE*, vol. 103, pp. 1725–1746, October 2015.

[8] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, “Applications of LDPC codes to the wiretap channel,” *IEEE Trans. Inform. Theory*, vol. 53, pp. 2933–2945, August 2007.

[9] H. Mahdavifar and A. Vardy, “Achieving the secrecy capacity of wiretap channels using polar codes,” *IEEE Trans. Inform. Theory*, vol. 57, pp. 6428–6443, October 2011.

[10] R. L. Rivest and A. T. Sherman, “Randomized encryption techniques,” in *Advances in Cryptology: Proceedings of Crypto 82* (D. Chaum, R. L. Rivest, and A. T. Sherman, eds.), pp. 145–163, Boston, MA: Springer US, 1983.

[11] S. Goldwasser and S. Micali, “Probabilistic encryption,” *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270 – 299, 1984.

[12] F. Oggier and M. J. Mihaljevic, “An information-theoretic security evaluation of a class of randomized encryption schemes,” *IEEE Trans. Inform. Forensics Security*, vol. 9, pp. 158–168, Feb 2014.

[13] L. Ozarow and A. Wyner, "Wire-tap channel II," *AT&T Bell Laboratories Technical Journal*, vol. 63, pp. 2135–2157, December 1984.

[14] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inform. Forensics Security*, vol. 6, pp. 532–540, September 2011.

[15] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," *IEEE Trans. Inform. Forensics Security*, vol. 8, pp. 619–625, April 2013.

[16] J. Choi, J. Ha, and H. Jeon, "Physical layer security for wireless sensor networks," in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–6, Sept 2013.

[17] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, June 2008.

[18] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inform. Theory*, vol. 7, pp. 1354–1367, Aug 2012.

[19] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *INFOCOM, 2011 Proceedings IEEE*, pp. 1125–1133, April 2011.

[20] J. Choi and J. Ha, "Secret key transmission based on channel reciprocity for secure iot," in *EuCNC2016-EmergConc*, pp. 1–5, June 2016.

[21] H. Li, X. Wang, and J. Y. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," *IEEE Trans. Wireless Commun.*, vol. 14, pp. 1155–1165, Feb 2015.

[22] J. Choi, "Secure transmissions via compressive sensing in multicarrier systems," *IEEE Signal Processing Letters*, vol. 23, pp. 1315–1319, Oct 2016.

[23] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. L. Goff, "Robust outage secrecy rate optimizations for a MIMO secrecy channel," *IEEE Wireless Communications Letters*, vol. 4, pp. 86–89, Feb 2015.

[24] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, pp. 1747–1761, Oct 2015.

[25] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451–456, Jul 1978.

[26] M.-S. Alouini and A. J. Goldsmith, "Capacity of Rayleigh fading channels under different adaptive transmission and diversity-combining techniques," *IEEE Trans. Vehicular Technology*, vol. 48, pp. 1165–1181, July 1999.

[27] P. H. Lin, S. H. Lai, S. C. Lin, and H. J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Selected Areas of Commun.*, vol. 31, pp. 1728–1740, September 2013.

[28] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, pp. 134–145, January 2013.

[29] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. New York: Dover Publications, 1972.

[30] J. Choi, "On channel-aware secure HARQ-IR," *IEEE Trans. Inform. Forensics Security*, vol. 12, pp. 351–362, Feb 2017.