Secure Communication via Sending Artificial Noise by the Receiver: Outage Secrecy Capacity/Region Analysis

Wei Li, Mounir Ghogho, *Senior Member, IEEE,* Bin Chen, Chunlin Xiong

***Abstract*—A novel approach for ensuring confidential wireless communication is proposed and analyzed from an information-theoretic standpoint. In this approach, the legitimate receiver generates artificial noise (AN) to impair the intruder's channel. This method is robust because it does not need the feedback of channel state information (CSI) to the transmitter and does not assume that the number of Eve's antennas should be smaller than that of Bob. Furthermore, we propose a new concept of outage secrecy region to evaluate the secrecy performance from a geometrical perspective. This should be useful if we need to know what zone should be protected (or militarized). Analysis and simulation results in practical environments show that the proposed method has a good performance.**

***Index Terms*—Artificial noise, privacy, outage secrecy region, secrecy capacity, physical layer security.**

I. Introduction

WIRELESS communication is inherently insecure owing to the broadcast nature of the wireless medium. A passive eavesdropper in an unknown location within "earshot" of a wireless transmission taps information about the transmitted signal without risk of detection. A natural framework for information security at the physical layer is the so-called wiretap channel introduced by Wyner [1] and associated notion of secrecy capacity. Secrecy problems involve three nodes: the transmitter (Alice), the legitimate receiver (Bob) and the eavesdropper (Eve). Alice wants to communicate with Bob while leaving Eve unable to decode the secret message. It is shown that perfect secrecy can be achieved without any key, provided that Bob has a better channel than Eve. The secrecy capacity is defined as the maximum achievable rate from Alice to Bob while keeping Eve completely ignorant of the transmitted message. Later, Wyner's work was extended to nondegraded discrete memoryless broadcast channels in [2], and then to the Gaussian channel in [3], recently to MIMO channels in [4] and to fading channels in [5].

In order to increase the secrecy capacity, artificial noise (AN) based method was suggested in [6]. In this method, AN is generated through multiple transmit antennas or the cooperating nodes, and is injected into the null-subspace of Bob's MIMO channel [7], [8]. AN is utilized to impair Eve's channel, while not affecting Bob's channel. The work in [9], [10] jointly optimizes the beamforming vector and the AN covariance matrix to achieve diverse signal to interference plus noise ratio (SINR) constraints for Bob and Eve. An outage probability-based approach to design the beamformers was proposed in [11]. However, these schemes have to face the following challenges: a) The channel state information (CSI) or at least partial CSI of Bob is needed at the transmitter; feeding back the CSI to the transmitter occupies some channel resource; b) If there is an uncertainty on the CSI at the transmitter, the AN may leak to Bob and thus reduces his SNR; this problem is even worse when Eve tries to personate Bob and feeds back her own CSI to Alice; considering the imperfect CSI, a robust Bayesian approach for multiuser MIMO wiretap channels was presented in [12]; c) if there are colluding Eves, or Eve has multiple antennas and the number of antennas exceeds the number of Alice's antennas, the AN can be calculated and eliminated if the CSI is perfectly known.

In this paper, we propose a novel AN based method to overcome the above problems. Different from the existing works where AN is added at the transmitter, the AN in our method is generated by the intended receiver, Bob, as shown in Fig. 1. The AN impairs the intruder's channel while it can be counteracted by Bob. This method has the following advantages: a) The CSI is not needed by Alice, so there is no feedback channel and thus the bandwidth resource is saved; uncertainty on the CSI is not an issue which implies robustness of the method; however, in order to use a wire-tap code, the channel capacity of Bob should be known at Alice. b) the AN can be generated by either multiple antennas or a single antenna, which is more practical than the existing AN methods which need multiple antennas at the transmitter; c) this method does not assume that the number of Eve's antennas should be smaller than that of Bob; indeed, even if there is a large number of antennas at Eve or there are colluding Eves, the AN is still hard to be totally eliminated because the CSI between Bob and Eve is not known to Eve; d) the proposed method can be combined with the masked beamforming scheme where an AN is generated at the transmitter to improve secrecy performance; e) it is particularly useful when the receiver has a stronger ability than the transmitter (e.g. the receiver is a base station); f) it is efficient if Eves are located around Bob; this is generally the case in several situations.

Another contribution of this paper is the introduction of the concepts of *outage secrecy region* (OSR) using a geometrical perspective. In practical communication systems, when the eavesdroppers are passive, it is impossible to calculate the secrecy capacity or Eve's bit error rate. In [8] a probabilistic framework using stochastic geometry is presented to quantify

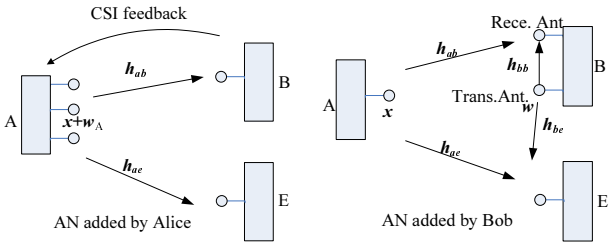
Manuscript received June 19, 2012. The associate editor coordinating the review of this letter and approving it for publication was M. Tao.

This work was supported in part by the NSFC under Grants 61101096 and 61101098, and the NSF of Hunan Province under Grant 11jj4055.

W. Li, B. Chen, and C. Xiong are with the School of Electronic Science and Engineering, National University of Defense Technology, Changsha, 410073 P. R. China (e-mail: liwei.nudt.cn@gmail.com; lierbency@126.com; xchlzju@nudt.edu.cn).

M. Ghogho is with the University of Leeds, Leeds LS2 9JT, U.K., and also with the International University of Rabat, 11100, Morocco (e-mail: m.ghogho@leeds.ac.uk).

Digital Object Identifier 10.1109/LCOMM.2012.081612.121344



(a) add AN at transmitter (b) add AN at receiver

Fig. 1: Secret communication using artificial noise.

the probability of secrecy versus the spatial density of the eavesdroppers, the power of the AN, the range of communication and antenna configurations. In this paper, by taking into account both path loss and small scale fading, we adopt the outage capacity approach to determine the OSR which is defined as follows. For a given rate R and maximum outage probability ε, the OSR consists of the coordinates of Eve for which the probability that the secrecy capacity is lower than R is lower than or equal to ε, i.e. if Eve is the (R, ε)-OSR region, the probability that she can decode the transmitted signal (of rate R) can reach ε. The minimum noise power from Bob required to achieve a given outage security region can also be derived. The analysis allows us to identify the zone that needs to be protected (or militarized) to guarantee some physical layer security specifications. This is particularly useful for military applications.

The rest of this paper is organized as follows. In Section II, we describe the system model and present the secure communication mechanism. Section III defines the outage security region and analyzes the secrecy performance of our scheme. Numerical results are shown in Section V, and conclusions are drawn in Section VI.

II. System Model

We assume that Alice has a single antenna, Bob has one receiving antenna and one transmitting antenna, and Eve has a single receiving antenna. In the security technique, Eve's location and channel are not known to Alice. However, in the security region analysis, we assume that Eve's noise variance is known, although we also consider the worst case scenario where this noise power is zero. As shown in Fig. 1 (b), Bob sends the AN while receiving the desired signal from Alice. The discrete-time system model is constructed as follows,

$$z(k) = h_{ab}x(k) + h_{bb}w(k) + n(k), \tag{1}$$

$$y(k) = h_{ae}x(k) + h_{be}w(k) + e(k), \tag{2}$$

for $k = 1, 2, ...$, where $x(k)$ is the transmitted signal with variance $\sigma_x^2 = P_A$, $w(k)$ is the AN sent by Bob whose power is equal to P_B, $z(k)$ and $y(k)$ are the received signals at Bob and Eve respectively, h_{ab}, h_{ae} and h_{be} are respectively the channels between Alice and Bob, Alice and Eve, and Bob and Eve, h_{bb} is the channel between the transmit and receive antennas of Bob, $n(k)$ and $e(k)$ are complex white Gaussian noises with powers equal to σ_b^2 and σ_e^2 respectively.

The crucial problem is how to design the AN signal $w(k)$ and counteract the effect of the AN on Bob. Because the CSI of Eve is unknown to Bob, the best $w(k)$ is a complex white Gaussian noise with the same bandwidth as that of $x(k)$. To cancel the effect of the AN on Bob, we can use the technology of full duplex wireless [13], [14]. Through antenna cancellation, RF interference cancellation and digital cancellation, the AN can be counteracted to an acceptable degree. Authors in [13] proposed a two-antenna full duplex radio design that uses a balun. The transmit antenna transmits the positive signal, and to cancel self-interference, the radio combines the negative signal with its received signal after adjusting the delay and attenuation of the negative signal to match the self-interference.

Therefore, because the AN and channel h_{bb} are known to Bob, the residual noise can be rebuilt and eliminated by digital interference cancellation as follows:

$$z'(k) = z(k) - h_{bb}w(k) = h_{ab}x(k) + n(k). \tag{3}$$

III. Outage Secrecy Region

We start by recalling the results of [3] for the Gaussian wiretap channel, where it is assumed that Alice and Bob communicate over a standard additive white Gaussian noise (AWGN) channel with noise power σ_b^2, and Eve's observation is also corrupted by Gaussian noise with power $\sigma_e^2 + P_B |h_{be}|^2$. The secrecy capacity in this case is

$$C = \left(\log_2(1+\gamma_B) - \log_2(1+\gamma_E)\right)^+ \tag{4}$$

where $\gamma_B = \frac{|h_{ab}|^2 P_A}{\sigma_b^2}$ and $\gamma_E = \frac{|h_{ae}|^2 P_A}{\sigma_e^2 + P_B|h_{be}|^2}$; $x^+ = max(x, 0)$.

Since we do not know Eve's CSI, we cannot calculate the secrecy capacity. In this situation, we could adopt a probabilistic approach which quantifies the probability that the secrecy capacity is larger than a certain rate. Here, we introduce the concept of OSR, which is related to the outage secrecy capacity. Assuming that Bob's location is known to Alice, we define the OSR as follows.

Definition (Outage Secrecy Region): For a given transmission rate R, and an outage probability ε, the (R, ε)-OSR is defined as a region over which the probability that the secrecy capacity is lower than R is lower than or equal to ε, and is mathematically formulated as

$$R_s = \{\boldsymbol{\theta}_e | p_{out}(R) \leq \varepsilon\}. \tag{5}$$

where $p_{out}(R) := \Pr(C_s < R)$ and $\boldsymbol{\theta}_e$ is the geographical coordinate vector of Eve, with respect to the position of Alice, which is chosen to be the origin of the coordinate system.

Taking into account the path-loss component, we have that $|h_{ab}|^2 = \lambda d_{ab}^{-\kappa} t_{ab}$, $|h_{ae}|^2 = \lambda d_{ae}^{-\kappa} t_{ae}$ and $|h_{be}|^2 = \lambda d_{be}^{-\kappa} t_{be}$, where t_{ab}, t_{ae} and t_{be} are independent exponentially distributed random variables with unit power, and λ is a constant which depends on signal and system parameters. Since R is positive, using (4) and (5) , $p_{out}(R)$ can be rewritten as

$$p_{out}(R) = 1 - \Pr\left\{\log_2\left(\frac{1+\alpha_{ab}t_{ab}}{1+\frac{\alpha_{ae}t_{ae}}{1+\alpha_{be}t_{be}}}\right) \geq R\right\} \tag{6}$$

where $\alpha_{ab} = \lambda P_A d_{ab}^{-\kappa}/\sigma_b^2$, $\alpha_{ae} = \lambda P_A d_{ae}^{-\kappa}/\sigma_e^2$ and $\alpha_{be} = \lambda P_B d_{be}^{-\kappa}/\sigma_e^2$. Since t_{ab}, t_{ae} and t_{be} are independent, their joint probability density function is $\exp(-t_{ae} - t_{be} - t_{ab})$.

Thus we have

$$p_{out}(R) = 1 - \iiint_D \exp(-t_{ae} - t_{be} - t_{ab}) dt_{ae} dt_{be} dt_{ab} \quad (7)$$

where $D = \{(t_{ae}, t_{be}, t_{ab}) \,|t_{ae} \geq 0, t_{be} \geq 0, t_{ab} \geq T\}$, where $T = \frac{2^R}{\alpha_{ab}} \left(1 + \frac{\alpha_{ae} t_{ae}}{1+\alpha_{be} t_{be}}\right) - \frac{1}{\alpha_{ab}} \geq 0$.

Further, we have that

$$\begin{aligned} p_{out}(R) &= 1 - \int_0^\infty e^{-t_{ae}} \int_0^\infty e^{-t_{be}} \int_T^\infty e^{-t_{ab}} dt_{ab} dt_{be} dt_{ae} \\ &= 1 - \exp\left(-\frac{2^R}{\alpha_{ab}} + \frac{1}{\alpha_{ab}}\right) \int_0^\infty \frac{e^{-t_{be}}}{\frac{2^R}{\alpha_{ab}} \frac{\alpha_{ae}}{(1+\alpha_{be} t_{be})} + 1} dt_{be} \end{aligned} \quad (8)$$

Now using the result (obtained after some algebra)

$$\int_0^\infty \frac{e^{-t}}{\frac{a}{1+bt}+1} dt = 1 + e^{\frac{a+1}{b}} Ei\left(-\frac{a+1}{b}\right) \frac{a}{b}$$

where $Ei(x)$ is the exponential integral $\int_{-\infty}^{x} (e^t/t) dt$, for $a = 2^R \frac{\alpha_{ae}}{\alpha_{ab}}$ and $b = \alpha_{be}$, we obtain the final expression

$$\begin{aligned} p_{out}(R) &= 1 - \exp\left(-\frac{2^R}{\alpha_{ab}} + \frac{1}{\alpha_{ab}}\right) \\ &\times \left(1 + \exp\left(\frac{2^R \frac{\alpha_{ae}}{\alpha_{ab}} + 1}{\alpha_{be}}\right) Ei\left(-\frac{2^R \frac{\alpha_{ae}}{\alpha_{ab}} + 1}{\alpha_{be}}\right) \frac{2^R \alpha_{ae}}{\alpha_{ab} \alpha_{be}}\right) \end{aligned} \quad (9)$$

Using the above expression, the (R, ε)-OSR is obtained by finding the coordinates of Eve for which (5) is satisfied.

Since Eve's power may not be known, we now consider the worst case scenario where Eve is noise-free, i.e. $\sigma_{e^2} = 0$; this also addresses the case where Eve's antenna gain, which may be unknown, is (much) higher than that of Bob; in fact, setting $\sigma_{e^2} = 0$ is equivalent to setting Eve's antenna gain to infinity. In this case, we have that

$$\begin{aligned} \lim_{\sigma_e^2 \to 0} p_{out}(R) =& 1 - \exp\left(-\frac{(2^R + 1)\sigma_b^2}{\lambda P_A d_{ab}^{-\kappa}}\right) \\ &\times \left(1 + \exp(\Psi) E_i(-\Psi) \Psi\right) \end{aligned} \quad (10)$$

where $\Psi = \frac{2^R \sigma_b^2 d_{ae}^{-\kappa}}{\lambda P_B d_{be}^{-\kappa} d_{ab}^{-\kappa}}$. Again, eq. (5) can be used to determine the (R, ε)-OSR in this case.

IV. Discussions and Extensions

Combining with the masked Beamforming scheme

If Alice has more than one antenna, we can combine our method with the masked beamforming scheme, which consists of Alice transmitting the sum of the information bearing signal and an AN signal [8]:

$$\mathbf{x}(k) = \mathbf{p} s(k) + \mathbf{w}_A(k) \quad (11)$$

where $\mathbf{p}$ is the normalized beamforming vector which is set to $\mathbf{p} = \mathbf{h}_{ab}^H / \|\mathbf{h}_{ab}\|$, $s(k)$ is the scalar complex information signal with power equal to P_A, $\mathbf{w}_A(k)$ is a complex Gaussian vector with covariance $K_{\mathbf{w_A}}$, and chosen to be a linear combination of the vectors that span the null space of $\mathbf{h}_{ab}$, i.e. $\mathbf{h}_{ab}^H \mathbf{w}_A(k) = 0$. The secrecy capacity in this case is

$$C = \left(\log_2(1 + \gamma_B) - \log_2(1 + \gamma_E)\right)^+ \quad (12)$$

where $\gamma_B = \frac{\|\mathbf{h}_{ab}\|^2 P_A}{\sigma_b^2}$ and $\gamma_E = \frac{\|\mathbf{h}_{ae}\|^2 P_A}{\sigma_e^2 + P_B \|\mathbf{h}_{be}\|^2 + \mathbf{h}_{ae} K_{\mathbf{w_A}} \mathbf{h}_{ae}^H}$.

From (12) we can see that the combined strategy has the advantage that the eavesdroppers around Alice as well as those around Bob suffer strong interference. Therefore, the secrecy performance is improved. Due to space limitation, the OSR in this scenario is not investigated here. Further, power allocation is also an interesting issue to investigate.

The case of multi-antenna Eve

In our system model, the CSI from Alice to Eve, $\mathbf{h}_{ae}$, is assumed known to Eve, but not the CSI between Bob and Eve, $\mathbf{h}_{be}$. Indeed, since Bob only transmits white noise, Eve cannot estimate $\mathbf{h}_{be}$. So it is almost impossible for Eve to counteract the AN totally. Thus, it is reasonable to assume that Eve treats the AN as white noise. So our method is still useful even if Eve has multiple antennas.

V. Simulation Results

In order to evaluate the secrecy performance of the proposed method, the following scenario is considered in the simulations. We locate Alice at (0, 0), and Bob at (1, 0). The channel bandwidth is set to 5MHz. The transmit power at Alice is 1W. The maximum transmit power at Bob is 10W. The noise power density is -180dBm/Hz, and the path-loss propagation model (in dB) is $128.1 + 37.6 \log_{10}(d)$ (where d is the distance in km) [15]. In the simulations, Eve has a single antenna, and Bob has two antennas (one for receiving and one for transmitting). All channels experience Rayleigh fading.

Fig.2 illustrates the OSR for the transmission rate $R = 1.5 \times 10^3$ bit/s and different values of outage probability ε. The result shows that the OSR corresponding to high probability of outage is around Alice, and thus the area around Alice is not likely to be secure; the figure shows that the area around Bob is however very likely to be secure, i.e. it is associated with a very low probability of outage ε. This means that Eve has to be very close to Alice for successful eavesdropping.

Fig.3 illustrates the outage probability for different AN power P_B versus the x-coordinate of Eve when she moves on the line $y = 0.5$. We see that the outage probability decreases as P_B increases. It also increases when Eve gets closer to Alice, and decreases when Eve gets closer to Bob.

Fig.4 depicts the simulated averaged (ergodic) secrecy capacity for different strategies. Eve moves along the line $y = 0.5$ from (-3,0.5) to (3,0.5). We compare the performance of five strategies: a) AN sent by Bob with $P_B = 1W$ and $P_A = 1W$; Alice has a single antenna and Bob has one receive antenna and one transmit antenna; b) AN sent by Alice with equal powers for the information signal and the AN; $P_A = 0.5W$, $tr(K_{\mathbf{w_A}}) = 0.5W$; Alice has 2 antennas and Bob has single antenna; c) combined strategy: AN sent by both Alice and Bob with $P_B = 1W$ and $P_A = 0.5W$, $tr(K_{\mathbf{w_A}}) = 0.5W$; Alice has 2 antennas, Bob has one transmit antenna and one receive antenna; d) Alice has single antenna, Bob has 2 receive antennas, $P_A = 1W$; e) Alice has 2 antennas, Bob has 2 receive antennas; AN is added by Alice with $P_A = 0.5W$, $tr(K_{\mathbf{w_A}}) = 0.5W$.

It is shown that strategy (a) achieves better performance when Eve is located close to Bob whereas strategy (b) achieves better performance when Eve is located close to Alice. Strategy (c) captures the advantages of strategies (a) and (b); it is useful when both the transmitter and receiver have extra power and antenna to send AN. Strategy (d) achieves the worst performance when Eve is close to Alice. Strategy (e) achieves

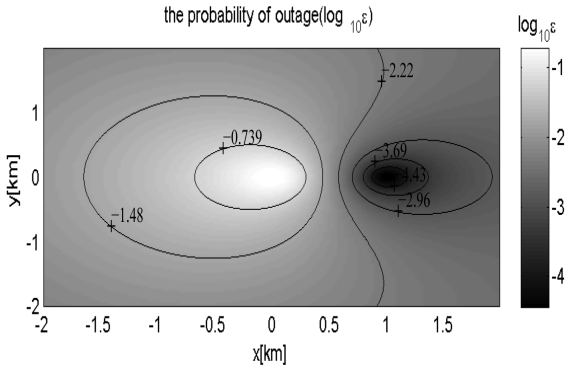


Fig. 2: Outage secrecy region for different values of ε, P_A=1 W, P_B=10 W, R=1.5e3 bit/s.

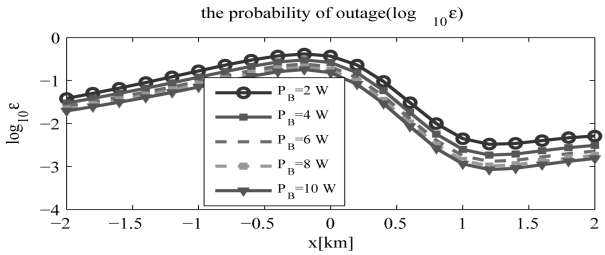


Fig. 3: Outage probability versus Eve's x-coordinate when she moves on line y=0.5.

the largest secrecy capacity, because the 2X2 MIMO system increases the capacity of Bob significantly. From the result, we conclude that in the presence of Eve, if the number of Bob's antennas is less than Alice's antennas, it is better to use all of Bob's antennas to receive Alice's signal; otherwise it is better to use some of Bob's antenna to transmit AN to disturb Eve.

VI. Conclusion

In this paper, we have introduced a novel method to provide secure communication via sending an artificial noise by the transmit antenna of the legitimate receiver. We also consider the far-field path loss component and introduce the concept of outage secrecy region which may be helpful in guiding the design of physical layer security solutions. Simulation results show that the proposed method can achieve high security in practical settings, especially when the intruder's location is near the intended receiver. Finally, the proposed method can be combined with the existing mask beamforming method to further improve secrecy performance.

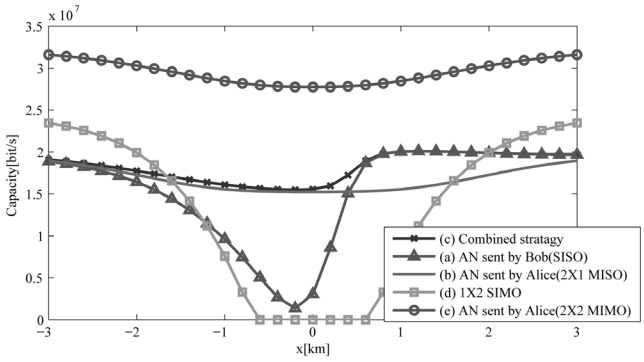


Fig. 4: Average secrecy capacity of 5 methods versus Eve's x-coordinate when Eve moves on line y=0.5.

References

[1] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J,* vol. 54, pp. 1355–1387, 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory,* vol. IT-24, no. 3, pp. 339–348, May 1978.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory,* vol. 24, pp. 451–456, July 1978.

[4] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. 2008 IEEE Int. Symp. Information Theory*, pp. 524–528.

[5] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory,* vol. 54, no. 6, pp. 2470–2492, June 2008.

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

[7] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.,* vol. 59, pp. 351–361, 2011.

[8] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers," presented at the IEEE ICC Workshop on Physical Layer Security, 2011.

[9] W. C. Liao, T. H. Chang, W. K. Ma, *et al.*, "Joint transmit beamforming and artificial noise design for QoS discrimination in wireless downlink," presented at IEEE ICASSP, 2010.

[10] Q. Haohao, C. Xiang, S. Yin, *et al.*, "Optimal power allocation for joint beamforming and artificial noise design in secure wireless communications," in *Proc. 2011 IEEE International Conference on Communications*, pp. 1–5.

[11] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability-based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. PP, no. 99, 2011.

[12] M. Pei, J. Wei, K. K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[13] M. Jainy, J. I. Choiy, T. M. Kim, *et al.*, "Practical, real-time, full duplex wireless," presented at the MobiCom, Las Vegas, Nevada, USA, 2011.

[14] S. W. Kim, Y. J. Chun, and S. Kim, "Co-channel interference cancellation using single radio frequency and baseband chain," *IEEE Trans. Commun.,* vol. 58, no. 7, pp. 2169–2175, 2010.

[15] 3GPP and T. 25.814V7.0.0, "Technical Specification Group Radio Access Network: Physical-Layer Aspects for Evolved UTRA (Rel. 7)," in editing, 2007.