Transmission Policies for Improving Physical Layer Secrecy Throughput in Wireless Networks

Rung-Hung Gau, *Member, IEEE*

***Abstract*—In this letter, we analyze the physical layer secrecy throughput in wireless fading networks with independent eavesdroppers that do not collude. We study the impacts of the total number of eavesdroppers on the secrecy throughput. In addition, we propose two channel-adaptive transmission policies for improving the secrecy throughput. The proposed transmission policies have low computational complexity and therefore are feasible in practice. We use analytical results and simulation results to justify the usage of the proposed schemes.**

***Index Terms*—Physical layer security, wireless fading networks, probability models, performance analysis.**

I. Introduction

Recently, physical layer security in wireless networks draws a lot of attention. While cryptography-based security is mainly based on computational complexity theory, physical layer security is mainly based on information theory. In particular, cryptography-based privacy is based on the fact that some problems such as prime factorization and discrete logarithm are computationally intractable, although in principle they can be solved by brute-force search. In contrast, information-theoretic secrecy assures that an eavesdropper is unable to decode the private information irrespective of the computational capability of the eavesdropper. Technologies of physical layer security and technologies of cryptography-based security are complementary rather than competing.

In this letter, we study the physical layer secrecy throughput for wireless fading networks containing independent eavesdroppers that do not collude. Gopala, Lai, and El Gamal [1] derived the secrecy capacity when the transmitter knows the channel gains of both the legitimate receiver and the eavesdropper. In addition, they showed that the secrecy capacity can be achieved based on a water-filling algorithm for power control. However, the computational complexity of the water-filling algorithm is high, since it requires solving integral equations. For mobile devices, energy saving is very important. Typically, energy consumption is an increasing function of computational complexity. To strike a balance between computational complexity and secrecy throughput, we propose two channel-adaptive transmission policies and derive related analytical results. We use both analytical results and simulation results to justify the usage of the proposed channel-adaptive transmission policies.

II. Related Work

Wyner [2] introduced the so-called wiretap channel and the associated notion of secrecy capacity. In particular, an achievable secrecy rate is defined as a transmission rate at which the confidential message is secretly transmitted from the source node to the destination node, while keeping the eavesdropper from getting information of the confidential message. Leung-Yan-Cheong and Hellman [3] derived the secrecy capacity for Gaussian wiretap channels. Khisti, Tchamkerten, and Wornell [4] studied the problem of secure broadcasting over wireless fading channels. The secrecy capacity of the MIMO wiretap channel was characterized by Khisti and Wornell [5] [6]. Jeong, Kim, and Kim [7] proposed jointly optimizing the beamforming vector at the source node and the beamforming matrix at the relay node for amplify-and-forward MIMO relay networks. Bloch, Barros, Rodrigues, and McLaughlin [8] developed a secure communication protocol that uses a four-step procedure to ensure wireless information-theoretic security. Dong, Han, Petropulu, and Poor [9] proposed improving wireless physical layer security via cooperating relays. Zhou, Ganti, Andrews, and Hjorungnes [10] studied the throughput cost for achieving a certain level of security in random networks where the legitimate nodes and eavesdroppers are distributed according to independent two-dimensional Poisson point processes.

III. System Models

We consider a wireless fading network that contains a source node, a destination node, and independent eavesdroppers. Each node has a single (omnidirectional) antenna for transmission or reception. As in [10], it is assumed that the eavesdroppers do not collude and do not transmit data. Let N be the total number of eavesdroppers. The destination node is also called node 0, while the ith eavesdropper is called node i, $\forall 1 \leq i \leq N$. Let σ^2 be the power spectral density of the additive white Gaussian noise. Let W be the bandwidth used for data transmission. Without loss of essential generality, it is assumed that $W = 1$. Time is partitioned into time slots. Let T be the length of a time slot. Typically, the value of T is smaller than the coherence time of the wireless channel. Let $F_X(x) = P\{X \leq x\}$ be the cumulative distribution function of the random variable X. Let $G_{i,t}$ be a continuous random variable that represents the gain of the channel from the source node to node i in time slot t, $\forall 0 \leq i \leq N, t \geq 1$. By definition, $G_{i,t} \geq 0$ for sure. It is assumed that for each fixed i, $G_{i,t}$'s are independent and identically distributed (IID) random variables. In addition, it is assumed that G_{i,t_1} and G_{j,t_2} are statistically independent, $\forall (i, t_1) \neq (j, t_2)$. Similar to [7], it is assumed that the source node knows the value of $(G_{0,t}, G_{1,t}, .., G_{N,t})$

Manuscript received July 22, 2012. The associate editor coordinating the review of this letter and approving it for publication was M. Tao.

R.-H. Gau is with the Department of Electrical Engineering, National Chiao Tung University, Hsinchu, Taiwan (e-mail: runghung@mail.nctu.edu.tw).

This work was supported in part by the National Science Council, Taiwan, R.O.C., under grant number NSC 100-2628-E-009-017-MY2.

Digital Object Identifier 10.1109/LCOMM.2012.100812.121625

through channel estimation at the beginning of time slot t. Designing game-theoretic mechanisms for providing eavesdroppers incentives to cooperate in channel estimation is beyond the scope of the letter. Let P be an upper bound for the average transmission power of the source node. Let P_t be the transmission power of the source node in time slot t. Then, $\lim_{n\to\infty}\frac{1}{n}\sum_{t=1}^{n}P_t \le P$. Define $[x]^+ = \max(x,0)$. Define $C(x) = W\log_2(1+\frac{P\cdot x}{\sigma^2})$, $\forall x \ge 0$. According to [11], when $N=1$, the secrecy capacity in time slot t equals $[W\log_2(1+\frac{P_t\cdot G_{0,t}}{\sigma^2}) - W\log_2(1+\frac{P_t\cdot G_{1,t}}{\sigma^2})]^+ = [C(\frac{P_t\cdot G_{0,t}}{P}) - C(\frac{P_t\cdot G_{1,t}}{P})]^+$. In a time slot, if the eavesdropper with the best eavesdropping channel cannot decode the private information sent by the source node, none of the N eavesdroppers can decode the private information. Thus, the secrecy capacity in time slot t is $[C(\frac{P_t\cdot G_{0,t}}{P}) - C(\frac{P_t\cdot \max_{i:1\le i\le N} G_{i,t}}{P})]^+$, which is equal to $[C(\frac{P_t\cdot G_{0,t}}{P}) - \max_{i:1\le i\le N} C(\frac{P_t\cdot G_{i,t}}{P})]^+$. Let R_t be the data transmission rate of the source node in time slot t. A transmission policy determines the value of (P_t, R_t) at the beginning of time slot t. Let $\mathbf{1}\{condition\}$ be the indicator function with value one if the condition is true or with value zero otherwise. Denote the secrecy throughput when the transmission policy θ is used by $S(\theta)$. In time slot t, the least upper bound of the set of achievable secrete rates is $[C(\frac{P_t\cdot G_{0,t}}{P}) - \max_{i:1\le i\le N} C(\frac{P_t\cdot G_{i,t}}{P})]^+$. Thus, $S(\theta)$ is defined as follows.

$$\begin{aligned} S(\theta) &= \lim_{n\to\infty}\frac{1}{n}\sum_{t=1}^{n} R_t \times \\ &\qquad \mathbf{1}\{R_t \le [C(\frac{P_t\cdot G_{0,t}}{P}) - \max_{1\le i\le N} C(\frac{P_t\cdot G_{i,t}}{P})]^+\}. \end{aligned} \tag{1}$$

When secrecy is not a concern, one may set $R_t = C(\frac{P_t\cdot G_{0,t}}{P})$. In this letter, to optimize the secrecy throughput, the value of R_t is set according to the following equation.

$$R_t = [C(\frac{P_t\cdot G_{0,t}}{P}) - \max_{i:1\le i\le N} C(\frac{P_t\cdot G_{i,t}}{P})]^+. \tag{2}$$

We focus on wireless channels with Rayleigh fading. Let $\mu_1, \mu_2, .., \mu_N$ be positive real numbers. It is assumed that $G_{i,t}$ is an exponentially distributed random variable with mean equals $\frac{1}{\mu_i}$, $\forall i, t$. Let d_i be the distance between the source node and node i, $\forall 0 \le i \le N$. Typically, μ_i depends on d_i. Let θ_1 be the transmission policy in which $P_t = P$, $\forall t \ge 1$. Whenever appropriate, $G_{i,1}$ is abbreviated by G_i.

IV. Channel-Adaptive Transmission Policies

In this section, for improving the physical layer secrecy throughput, while keeping the computational complexity low, we propose two channel-adaptive transmission policies, denoted by θ_2 and θ_3. When θ_2 or θ_3 is used, the long-term average transmission power equals P.

A. Probability-based power allocation

The transmission policy θ_2 exploits the probability that the source node could secretly transmit information to the destination node in a time slot. Define $q = P\{C(G_0) > \max_{i:1\le i\le N} C(G_i)\}$. Namely, q is the probability that eavesdroppers cannot decode in a time slot. When the transmission policy θ_2 is used, the value of (P_t, R_t) is set according to the following rules. If $G_{0,t} > \max_{i:1\le i\le N} G_{i,t}$, $P_t = \frac{P}{q}$. Otherwise, $P_t = 0$.

Wang, Yu, and Zhang [12] derived a close-form expression for q when $\mu_i = \mu$, $\forall i$. We derive the value of q when $(\mu_1, \mu_2, .., \mu_N)$ is arbitrary. For each i, where $i \in \{1,2,3,..,N\}$, define an event $A_i = \{G_0 \le G_i\}$. Then, $P\{A_i\} = P\{G_0 \le G_i\} = \frac{\mu_0}{\mu_0+\mu_i}$ [13]. In addition, $\forall S \subset \{1,2,3,..,N\}$, since $\min_{i:i\in S} G_i$ is exponentially distributed with mean equals $(\sum_{i:i\in S}\mu_i)^{-1}$,

$$\begin{aligned} P\{\cap_{i:i\in S} A_i\} &= P\{G_0 \le \min_{i:i\in S} G_i\} \\ &= \frac{\mu_0}{\mu_0 + \sum_{i:i\in S}\mu_i}. \end{aligned} \tag{3}$$

Furthermore,

$$\begin{aligned} q &= \{G_0 > \max_{i:1\le i\le N} G_i\} \\ &= 1 - P\{G_0 \le \max_{i:1\le i\le N} G_i\} \\ &= 1 - P\{\cup_{i=1}^{N} A_i\} \\ &= 1 - \sum_{i=1}^{N} P\{A_i\} + \sum\sum_{i<j} P\{A_i \cap A_j\} + .. + \\ &\quad (-1)^N P\{A_1 \cap A_2 \cap .. \cap A_N\}. \end{aligned} \tag{4}$$

The last equality is based on the de Morgan laws in probability theory [13].

B. Dynamic power allocation

We now introduce the transmission policy θ_3 that allows the transmitter to use more transmission power when the quality of the legitimate channel is much better than the quality of the eavesdropping channel. Let λ be a positive real number. Let P^* be a real number that satisfies the following equation.

$$\begin{aligned} &P^* \times E[[1 - e^{-\lambda(G_{0,t} - \max_{i:1\le i\le N} G_{i,t})}] \times \\ &\mathbf{1}\{G_{0,t} - \max_{i:1\le i\le N} G_{i,t}\}] = P. \end{aligned} \tag{5}$$

When θ_3 is used, the value of P_t is set according to the following equation.

$$\begin{aligned} P_t &= P^* \times (1 - e^{-\lambda(G_{0,t} - \max_{i:1\le i\le N} G_{i,t})}) \times \\ &\qquad \mathbf{1}\{G_{0,t} - \max_{i:1\le i\le N} G_{i,t}\}. \end{aligned} \tag{6}$$

Note that when $0 < \lambda < \infty$, P_t is an increasing function of $G_{0,t} - \max_{i:1\le i\le N} G_{i,t}$, as long as $G_{0,t} - \max_{i:1\le i\le N} G_{i,t} > 0$. When $\lambda = \infty$, power allocation becomes independent of channel states.

V. Analytical Results

A. Secrecy throughput analysis

We derive the value of $S(\theta_1)$ as follows. Abbreviate $G_{i,1}$ by G_i. Then,

$$\begin{aligned} S(\theta_1) &= \lim_{n\to\infty}\frac{1}{n}\sum_{t=1}^{n}[C(G_{0,t}) - \max_{i:1\le i\le N} C(G_{i,t})]^+ \times 1 \\ &= E[[C(G_0) - \max_{i:1\le i\le N} C(G_i)]^+]. \end{aligned} \tag{7}$$

The first equality is based on Equation (1), Equation (2), and $P_t = P$. Recall that for each fixed i, $G_{i,t}$'s are IID random variables. Based on the law of large numbers [13], we have the second equality.

Based on the above equation, we have

$$\begin{aligned} & S(\theta_1) \\ = \ & E[[C(G_0) - \max_{i:1\leq i\leq N} C(G_i)]^+] \\ = \ & E[E[[C(G_0) - \max_{i:1\leq i\leq N} C(G_i)]^+ | G_0]] \\ = \ & \int_0^\infty E[[C(G_0) - \max_{i:1\leq i\leq N} C(G_i)]^+ | G_0 = x] \, dF_{G_0}(x) \\ = \ & \int_0^\infty E[[C(x) - \max_{i:1\leq i\leq N} C(G_i)]^+] \, dF_{G_0}(x). \end{aligned} \tag{8}$$

The second equality is based on $E[X] = E[E[X|Y]]$. Note that the Riemann-Stieltjes integral is used in the right-hand side of the third equality.

Since $F_{\max_{i:1\leq i\leq N} G_i}(y) = \prod_{i=1}^N P\{G_i \leq y\} = \prod_{i=1}^N (1 - e^{-\mu_i y})$, we have

$$\begin{aligned} & \frac{dF_{\max_{i:1\leq i\leq N} G_i}(y)}{dy} \\ = \ & \sum_{i=1}^N \mu_i e^{-\mu_i y} \prod_{j:j\neq i} (1 - e^{-\mu_j y}). \end{aligned} \tag{9}$$

Then, based on Equation (8), we have

$$\begin{aligned} & S(\theta_1) \\ = \ & \int_0^\infty \int_0^x [C(x) - C(y)] \times [\sum_{i=1}^N \mu_i e^{-\mu_i y} \prod_{j:j\neq i} 1 - e^{-\mu_j y}] \\ & \times \mu_0 e^{-\mu_0 \cdot x} \, dy \, dx. \end{aligned} \tag{10}$$

Similarly,

$$\begin{aligned} S(\theta_2) &= \lim_{n\to\infty} \frac{1}{n} \sum_{t=1}^n [C(\frac{G_{0,t}}{q}) - \max_{1\leq i\leq N} C(\frac{G_{i,t}}{q})]^+ \\ &= E[[C(\frac{G_0}{q}) - C(\frac{\max_{i:1\leq i\leq N} G_i}{q})]^+] \\ &= \int_0^\infty \int_0^x [C(\frac{x}{q}) - C(\frac{y}{q})] \times [\sum_{i=1}^N \mu_i e^{-\mu_i y} \times \\ & \quad \prod_{j:j\neq i} (1 - e^{-\mu_j y})] \times \mu_0 e^{-\mu_0 x} \, dy \, dx. \end{aligned} \tag{11}$$

Proposition 1: $S(\theta_2) > S(\theta_1)$.

Proof:

1. For each fixed (x, y), where $0 \leq y \leq x$, define $h_{x,y}(z) = C(\frac{x}{z}) - C(\frac{y}{z})$, $\forall z \in (0, 1]$. By direct computation, $\frac{dh_{x,y}(z)}{dz} = (\frac{W}{\ln(2)}) \times (\frac{\sigma^2 z + Py}{\sigma^2 z + Px}) \times (\frac{\sigma^2 P(y-x)}{(\sigma^2 z + Py)^2})$.

2. Then, $h^{'}_{x,y}(z) < 0$, $\forall 0 \leq y < x, z \in (0, 1]$. In addition, $h^{'}_{x,y}(z) = 0$, $\forall 0 \leq y = x, z \in (0, 1]$. Thus, since $q \in (0, 1)$, $C(\frac{x}{q}) - C(\frac{y}{q}) \geq C(\frac{x}{1}) - C(\frac{y}{1})$, $\forall 0 \leq y \leq x$, and the equality holds only when $y = x$.

3. Therefore, based on Equation (10) and Equation (11), $S(\theta_2) > S(\theta_1)$.

QED.

B. A closed-form expression for P^*

We now derive a closed-form expression for P^*. Define $\theta(y) = \int_y^\infty (1 - e^{-\lambda(x-y)}) \mu_0 e^{-\mu_0 x} \, dx$. Then,

$$\begin{aligned} \theta(y) &= \int_y^\infty (1 - e^{-\lambda(x-y)}) \mu_0 e^{-\mu_0 x} \, dx \\ &= \int_y^\infty \mu_0 e^{-\mu_0 x} \, dx - \int_y^\infty \mu_0 e^{-(\lambda+\mu_0)x} e^{\lambda y} \, dx \\ &= e^{-\mu_0 y} - (\frac{\mu_0}{\lambda + \mu_0}) \cdot e^{-\mu_0 y} \\ &= (\frac{\lambda}{\lambda + \mu_0}) \cdot e^{-\mu_0 y}. \end{aligned} \tag{12}$$

For each pair (i, α), where $i \in \{1, 2, .., N\}$ and $\alpha \in \{1, 2, .., N-1\}$, define the set $B_{N,i,\alpha}$ as follows.

$$\begin{aligned} & B_{N,i,\alpha} \\ = \ & \{(k_1, k_2, .., k_\alpha) | k_1, k_2, .., k_\alpha \in \{1, 2, 3, .., i-1, i+1, \\ & i+2, .., N\}, k_1 < k_2 < .. < k_\alpha\}. \end{aligned} \tag{13}$$

Then,

$$\begin{aligned} & E[[1 - e^{-\lambda(G_{0,t} - \max_{i:1\leq i\leq N} G_{i,t})}] \times \\ & \mathbf{1}\{G_{0,t} - \max_{i:1\leq i\leq N} G_{i,t}\}] \\ = \ & \int_0^\infty [\int_y^\infty (1 - e^{-\lambda(x-y)}) \mu_0 e^{-\mu_0 x} \, dx] \times \\ & \sum_{i=1}^N \mu_i e^{-\mu_i y} \prod_{j:j\neq i} (1 - e^{-\mu_j y}) \, dy \\ = \ & (\frac{\lambda}{\lambda + \mu_0}) \int_0^\infty e^{-\mu_0 y} \sum_{i=1}^N \mu_i e^{-\mu_i y} \prod_{j:j\neq i} (1 - e^{-\mu_j y}) \, dy \\ = \ & (\frac{\lambda}{\lambda + \mu_0}) \sum_{i=1}^N \mu_i \int_0^\infty e^{-(\mu_0+\mu_i)y} \prod_{j:j\neq i} (1 - e^{-\mu_j y}) \, dy \\ = \ & (\frac{\lambda}{\lambda + \mu_0}) \sum_{i=1}^N \mu_i \cdot [\frac{1}{\mu_0 + \mu_i} + \sum_{\alpha=1}^{N-1} (-1)^\alpha \times \\ & \sum_{(k_1,k_2,..,k_\alpha)\in B_{N,i,\alpha}} (\mu_0 + \mu_i + \sum_{\beta=1}^{\alpha} \mu_{k_\beta})^{-1}]. \end{aligned} \tag{14}$$

Based on Equation (9), the probability density function for $\max_{i:1\leq i\leq N} G_{i,t}$ is $\sum_{i=1}^N \mu_i e^{-\mu_i y} \prod_{j:j\neq i} (1 - e^{-\mu_j y})$. Thus, we have the first equality. The second equality is based on Equation (12). The last equality is based on the fact that $\int_0^\infty e^{-sy} \, dy = \frac{1}{s}$, $\forall s > 0$.

Therefore, based on Equation (5),

$$\begin{aligned} P^* = \ & P \times \{(\frac{\lambda}{\lambda + \mu_0}) \sum_{i=1}^N \mu_i \cdot [\frac{1}{\mu_0 + \mu_i} + \sum_{\alpha=1}^{N-1} (-1)^\alpha \times \\ & \sum_{(k_1,k_2,..,k_\alpha)\in B_{N,i,\alpha}} (\mu_0 + \mu_i + \sum_{\beta=1}^{\alpha} \mu_{k_\beta})^{-1}]\}^{-1}. \end{aligned} \tag{15}$$

VI. Simulation and Numerical Results

We wrote a C program to obtain the value of the secrecy throughput based on discrete event-driven simulations. Each simulation instance contains one million time slots. Let θ_4

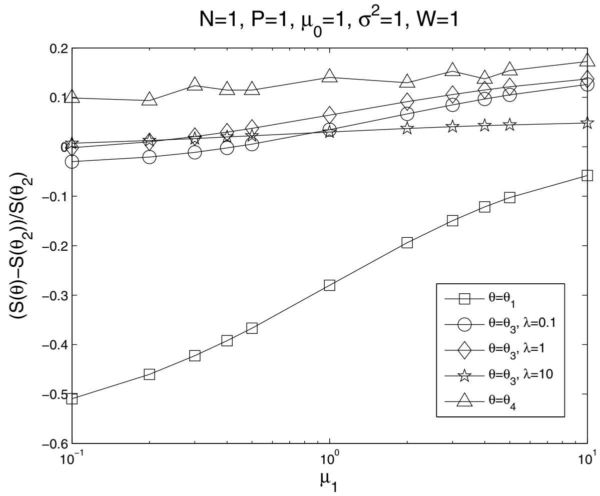

Fig. 1. The impacts of μ_1 on the secrecy throughput.

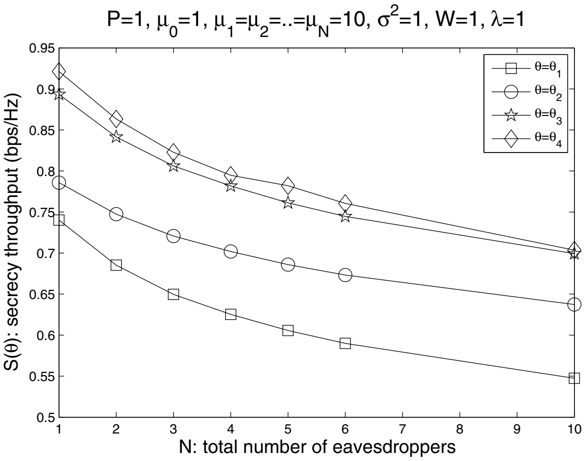

Fig. 2. The impacts of the total number of eavesdroppers on the secrecy throughput.

be the transmission policy that is used in [1] for the case in which the transmitter knows the channel gains of the legitimate receiver and the eavesdroppers. In Figure 1, we show simulation results for $\frac{S(\theta)-S(\theta_2)}{S(\theta_2)}$, when $N = 1$. We find that $\frac{S(\theta_1)-S(\theta_2)}{S(\theta_2)}$ is always negative, which is consistent with Proposition 1. In contrast, $\frac{S(\theta_3)-S(\theta_2)}{S(\theta_2)} \geq 0$, regardless of the values of μ_1 and P. However, though not shown in the letter due to the limit of space, when $\frac{P}{\sigma^2} \geq 10$, the difference between $S(\theta_3)$ and $S(\theta_2)$ becomes negligible. In Figure 2, we show the impacts of the total number of eavesdroppers on the secrecy throughput. In particular, regardless of the adopted transmission policy, as the total number of eavesdroppers increases, the value of the secrecy throughput decreases. In comparison with θ_1, θ_3 could increase the secrecy throughput by more than 20%. In addition, $\frac{S(\theta_3)}{S(\theta_4)} \geq 0.96$. This means that θ_3 is near-optimal and it is unnecessary to find an optimal value for λ by the exhaustive search. Unlike θ_4, θ_3 is based on a close-form expression and does not require numerically solving an integral equation in order to find the proper water level. We also used Maple to obtain equation-based numerical results. The numerical results are consistent with simulation results. For example, when $N = 2$, $P = 1.0$, $\sigma^2 = 1.0$, $\mu_0 = 1.0$, and $\mu_1 = \mu_2 = 0.1$, for $S(\theta_1)$, the numerical result is 0.006905, while the simulation result is 0.006852. When $N = 2$, $P = 1.0$, $\sigma^2 = 1.0$, $\mu_0 = 1.0$, and $\mu_1 = \mu_2 = 0.1$, for $S(\theta_2)$, the numerical result is 0.011019, while the simulation result is 0.011736.

VII. Conclusion

In this letter, we have studied the physical layer secrecy throughput in wireless fading networks with independent eavesdroppers that do not collude. We have analyzed the impacts of the total number of eavesdroppers on the secrecy throughput. In addition, to improve the secrecy throughput, we have proposed two channel-adaptive transmission policies. We have derived closed-form expressions for the proposed transmission policies. Furthermore, we have used analytical results and simulation results to show that the proposed channel-adaptive transmission policies could improve the physical layer secrecy throughput. Future work includes studying the case in which the gains of the eavesdropping channels are unknown. Another direction of future research is extending the analysis in the letter to cooperative communications systems.

References

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

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

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

[4] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas–part I: the MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas–part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[7] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

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

[9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[10] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[11] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[12] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. 2007 IEEE International Symposium on Information Theory*, pp. 1301–1305.

[13] S. M. Ross, *Introduction to Probability Models*, 10th edition. Academic Press, 2009.