On the Multi-User Diversity with Secrecy in Uplink Wiretap Networks

Hu Jin, *Member, IEEE*, Won-Yong Shin, *Member, IEEE*, and Bang Chul Jung, *Member, IEEE*

***Abstract*—In this letter, we consider the uplink wiretap network which consists of a base station, N legitimate users, and several eavesdroppers. We propose a novel user scheduling algorithm based on a threshold, which achieves the *optimal multi-user diversity gain*, i.e., $\log\log N$. To the best of our knowledge, there has been no such result in uplink wiretap networks. In order to obtain good throughput performance in the network, the threshold value needs to be carefully chosen. Through extensive simulations, we observe that the proposed user scheduling outperforms the conventional scheduling algorithms and it approaches the throughput performance of the optimal user scheduling algorithm in various scenarios.**

***Index Terms*—Physical-layer security, secrecy capacity, throughput scaling, multi-user diversity, user scheduling.**

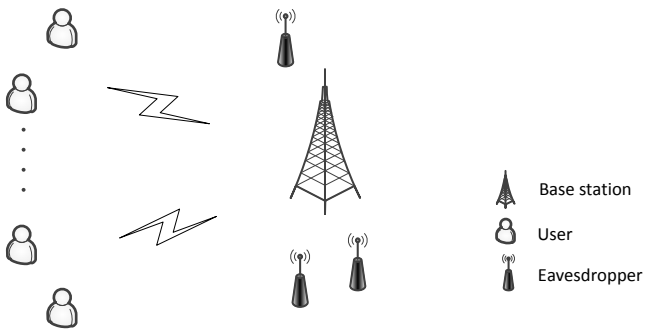

Fig. 1. An uplink wiretap network consisting of a base station, multiple users, and multiple eavesdroppers.

I. Introduction

In a pioneering paper [1], Shannon introduced the notion of information-theoretic secrecy, and established the achievability of perfectly secure communications in the presence of eavesdroppers. In [2], Wyner characterized a three-terminal wiretap channel, where the achievability of a positive secrecy rate was derived only over a physically degraded discrete memoryless channel. Subsequent work has shown that the analysis of multi-user channel models with secrecy constraints highlights the essential role of feedback and jamming as means to increase secrecy rates [3], [4]. Since it is difficult to obtain the exact secrecy capacity region in most multi-user scenarios, there has recently been a significant interest in analyzing the asymptotic performance of a variety of wireless wiretap networks at high signal-to-noise ratio (SNR) in terms of secure degrees-of-freedom [5], [6].

As an alternative approach, the asymptotic performance of multi-user networks can be characterized by showing a throughput scaling behavior when there exist infinitely many users. Several techniques that exploit the usefulness of fading in broadcast channels having many users have been proposed, thus resulting in the multi-user diversity (MUD) gain [7]–[9]. Various communication scenarios such as cooperative relaying and cognitive radio networks have been extensively studied by exploiting the MUD gain [10], [11]. For secure communications, we also need to consider the presence of (potential) multiple *eavesdroppers* in wiretap channels [12], [13] . In [12], it has been studied how to exploit the MUD gain by selecting a trusted-relay in a two-hop network. In addition, the problem of broadcasting secret information was examined in [13], where it was shown that the average secrecy rate is rather reduced as the number of users in a network increases, thus resulting in no MUD gain.

In this letter, we introduce an opportunistic user scheduling strategy which achieves the *optimal* MUD gain, i.e., $\log\log N$ in uplink wiretap networks. In the proposed user scheduling, instead of using complex coding schemes (e.g., superposed codes), the BS selects a certain user based on a pre-determined threshold (i.e., scheduling criteria) which is related to the maximum amount of information overheard by eavesdroppers.

II. System Model

The system model is illustrated in Fig. 1. N users communicate with a BS in the uplink where there exists K eavesdroppers which try to overhear the communications between the users and the BS. We assume that each node (user, BS, or eavesdropper) is equipped with a single antenna.

The term $\alpha_i h_i \in \mathbb{C}$ denotes the channel coefficient between the i-th user and the BS, consisting of the large-scale path-loss component α_i and the small-scale complex fading component h_i, where $i \in \{1, \cdots, N\}$. The term $\beta_{ik} h_{ik} \in \mathbb{C}$ denotes the channel coefficient between the i-th user and the k-th eavesdropper, consisting of the large-scale path-loss component β_{ik} and the small-scale complex fading component h_{ik}, where $k \in \{1, \cdots, K\}$. For simplicity, we assume that the users experience the same degree of path-loss attenuation to the BS, i.e., the large-scale term α_i is assumed to be 1. The channel is assumed to be complex Gaussian, having zero-mean and unit variance, and independent across different i and k. We assume a block-fading model, i.e., the channels are constant during one block (e.g., frame) and change independently for every block. Suppose that only one legitimate user transmits its data packet through a certain scheduling algorithm of the

Manuscript received May 20, 2013. The associate editor coordinating the review of this letter and approving it for publication was M. Elkashlan.

This research was funded by the MSIP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013.

H. Jin is with the Department of Electrical and Computer Engineering, the University of British Columbia, Vancouver, BC, Canada V6T 1Z4 (e-mail: hjin@ece.ubc.ca).

W.-Y. Shin is with the Department of Computer Science and Engineering, Dankook University, Yongin 448-701, Republic of Korea (e-mail: wyshin@dankook.ac.kr).

B. C. Jung is with the Department of Information and Communication Engineering, Gyeongsang National University, Tongyeong 650-160, Republic of Korea (e-mail: bcjung@gnu.ac.kr). B. C. Jung is the corresponding author.

Digital Object Identifier 10.1109/LCOMM.2013.071813.131158

BS[1]. Then, the received signals $y \in \mathbb{C}$ at the BS and $y_k \in \mathbb{C}$ at the k-th eavesdropper when the i-th user is transmitting are given by

$$\begin{aligned} y &= h_i x_i + z, \\ y_k &= \beta_{ik} h_{ik} x_i + z_k, \end{aligned} \tag{1}$$

where x_i represents the transmit symbol of the i-th user and $z \in \mathbb{C}$ and $z_k \in \mathbb{C}$ denote the circularly symmetric complex additive white Gaussian noise (AWGN) at the BS and the k-th eavesdropper, respectively, having zero-mean and variance N_0. We assume that each user has an average transmit power constraint $\mathbb{E}[|x_i|^2] \leq P$. For a notational convenience we denote the transmitted SNR as $\rho = P/N_0$.

Suppose that the i-th user knows its channel gains to the BS and to the eavesdroppers, i.e., h_i and $\beta_{ik}h_{ik}$, respectively.[2] The secrecy data rate of the i-th user is then expressed as [14], [15]:

$$\begin{aligned} C_i &= \log\left(1+|h_i|^2\rho\right) - \\ &\quad \log\left(1+\max\{|\beta_{i1}h_{i1}|^2, \cdots, |\beta_{iK}h_{iK}|^2\}\rho\right) \\ &= \log\left(\frac{1+|h_i|^2\rho}{1+\max\{|\beta_{i1}h_{i1}|^2, \cdots, |\beta_{iK}h_{iK}|^2\}\rho}\right). \end{aligned} \tag{2}$$

The secrecy throughput of the uplink wiretap network is maximized when the BS selects the user yielding the best secrecy data rate among N users in each slot.

III. Opportunistic User Scheduling Based on a Threshold

When there is no eavesdropper in an uplink network, it is well known that the optimal throughput scales as $loglogN$ when the number of users in the network (N) tends to infinity [7]. However, the optimal throughput scaling with secrecy in the wiretap uplink network has not been shown. In this section, we introduce a threshold-based sub-optimal user scheduling algorithm which achieves the *optimal* throughput scaling for the uplink wiretap network. In the proposed user scheduling algorithm, one user is selected in the sense of having large channel gain to the BS as well as having small capacity loss due to the eavesdroppers. The basic idea of the proposed scheduling is to find a certain user out of N users satisfying the following criterion[3]:

$$|\beta_{ik}h_{ik}|^2\rho \leq \eta_I, \quad \text{for } k = 1, 2, \cdots, K, \tag{3}$$

where η_I denotes a pre-determined positive threshold. In particular, the value $\eta_I > 0$ is set to a small constant in order to assure that the capacity loss due to the eavesdroppers is small. Suitable values of η_I will be specified in the Section V. Under the proposed scheduling, the users satisfying (3) request transmission to the BS. Then, the BS selects a user who shows the maximum signal strength at the BS and the selected user starts to transmit its data packet.

[1]It is a feasible transmission scenario since under the model, it is sufficient to achieve full degrees-of-freedom gain with single user transmission.

[2]It does not seem easy for each user to acquire channel state information (CSI) to the eavesdroppers under the environment where the eavesdroppers listen to users' data packets (but not transmit their own signal). If the eavesdroppers transmit their own signals, then each user can obtain the CSI from the received signal from eavesdroppers. Even though assuming CSI to the eavesdroppers at each user may not be feasible, it will provide an upper bound on the performance given by any scheduling method. Note that such an assumption has commonly been made in the literature dealing with secrecy (refer to the previous studies [4], [6], [17] on the secrecy rate analysis).

[3]Although it is not the scope of this paper, it should be noted that the proposed scheme can reduce the feedback overhead of the system since only the users satisfying (3) need to feedback.

IV. Analysis of Secrecy Throughput Scaling Law

In the uplink, the transmission rate from each user to BS may be severely limited due to the existence of eavesdroppers for secure transmission at the physical layer. Now we show that the proposed user scheduling in Section III asymptotically achieves the optimal MUD gain, i.e., $\log\log N$, in terms of the secrecy throughput. The achievability is conditioned by the scaling behavior between the number of users, N, and the received SNR. We analyze how N scales with SNR so as to achieve the optimal MUD gain in uplink wiretap networks. We start from the following lemma.

Lemma 1: Let $f(x)$ denote a continuous function of $x \in [0, \infty)$, $0 < f(x) \leq 1$. Then, $\lim_{x\to\infty}(1-f(x))^x$ converges to zero if and only if $\lim_{x\to\infty} xf(x)$ tends to infinity.

Proof: See Appendix A. ∎

Since the channel coefficient is complex Gaussian with zero-mean, the term $|h_{ik}|^2$ is exponentially distributed, and its cumulative distribution function (CDF) is given by

$$\Pr\left\{|h_{ik}|^2 \leq x\right\} = 1 - e^{-x} \quad \text{for } x \geq 0. \tag{4}$$

Thus, the term $\max\{|h_{i1}|^2, \cdots, |h_{iK}|^2\}$, is distributed as

$$F(x) = (1-e^{-x})^K. \tag{5}$$

A lower bound on $F(x)$ is provided in the following lemma.

Lemma 2: For any $0 \leq x < 1$, $F(x)$ in (5) is lower-bounded by

$$F(x) \geq c_1 x^K, \tag{6}$$

where $c_1 = (1-e^{-1})^K$.

Proof: From the convexity of $1-e^{-x}$, we have

$$1 - e^{-x} \geq (1-e^{-1})x, \quad \text{for } 0 \leq x < 1, \tag{7}$$

which completes the proof. ∎

Now we are ready to establish the main result of this letter.

Theorem 1: For a given constant $\epsilon \in (0,1)$, the proposed user scheduling achieves $\log(\epsilon\rho\log N)$ secrecy throughput scaling with high probability (whp) in the high SNR regime if N scales as $\rho^{\frac{K}{1-\epsilon_0}}$ for a constant $\epsilon_0 \in (\epsilon, 1)$.

Proof: In order to prove this theorem, we first slightly modify the proposed scheduling algorithm to have the degraded performance, while still achieving the secrecy throughput scaling. Under this scheduling, the BS randomly selects one user among users satisfying (3) and the following criteria:

$$|h_i|^2 \geq \eta_{\text{tr}}, \quad i = 1, 2, \cdots, N. \tag{8}$$

Since the proposed scheduling selects the user showing the maximum signal strength at the BS while satisfying (3), the proposed scheduling always results in a better secrecy throughput performance than the scheduling modified in this section.

Suppose that $\eta_{\text{tr}} = \epsilon \log N$. Let β be the maximum value among $\beta_{i,k}$ where $i \in \{1, \cdots, N\}$ and $k \in \{1, \cdots, K\}$. Then, the event that the i-th user satisfies the two criteria (3) and (8) occurs with the probability larger than or equal to

$F(\eta_I\rho^{-1}\beta^{-2})e^{-\eta_{\rm tr}}$. Thus, the probability that such an event occurs for at least one user is lower-bounded by

$$1-\left[1-F(\eta_I\rho^{-1}\beta^{-2})e^{-\eta_{\rm tr}}\right]^N. \tag{9}$$

By *Lemma 1*, (9) converges to 1 as N tends to infinity, if and only if

$$\lim_{N\to\infty} NF(\eta_I\rho^{-1}\beta^{-2})e^{-\eta_{\rm tr}}\to\infty. \tag{10}$$

From *Lemma 2*, the term in (10) can be lower-bounded by

$$\begin{aligned}&\lim_{N\to\infty} c_1 N\left(\eta_I\rho^{-1}\beta^{-2}\right)^K e^{-\eta_{\rm tr}}\\ &= c_1\eta_I^K\beta^{-2K}\cdot\lim_{N\to\infty}\frac{N}{\rho^K}e^{-\epsilon\log N}\\ &= c_1\eta_I^K\beta^{-2K}\cdot\lim_{N\to\infty}\frac{N^{1-\epsilon}}{\rho^K},\end{aligned}$$

which increases with N (or equivalently ρ) as N scales as $\rho^{\frac{K}{1-\epsilon_0}}$ for $\epsilon_0\in(\epsilon,1)$. Hence, there exists at least one user satisfying (3) and (8) whp. From (2), a lower bound on the achievable secrecy throughput is finally given by

$$\begin{aligned}C &\geq \log\left(\frac{1+\rho\eta_{\rm tr}}{1+\eta_I}\right)\\ &= \log\left(\frac{1}{1+\eta_I}+\frac{\epsilon}{1+\eta_I}\cdot\rho\log N\right)\\ &= \log\left(c_2+c_2\epsilon\rho\log N\right),\end{aligned} \tag{11}$$

which scales as $\log(\epsilon\rho\log N)$, under the condition that N scales as $\rho^{\frac{K}{1-\epsilon_0}}$, where $c_2=\frac{1}{1+\eta_I}>0$ is a constant value. This completes the proof of the theorem. ■

Remark 1: It is also proved that the optimal throughput scaling of the uplink wiretap networks is $\log\log N$ by *Theorem 1* while the proposed user scheduling yields a lower bound on the secrecy throughput performance, compared with the optimal user scheduling which directly maximizes the secrecy data rate in (2).

Remark 2: There exists an optimal η_I resulting in the maximum secrecy capacity in practical communication scenarios with finite N even though (11) indicates that η_I should be as low as possible to achieve large secrecy throughput when N tends to infinity. A smaller η_I reduces the secrecy capacity loss, but it corresponds to a smaller MUD gain because the number of users satisfying the strict condition on the secrecy capacity loss becomes small. On the other hand, if a larger η_I is set, then a more MUD gain can be achieved because the number of users satisfying (3) becomes large, but it also induces a larger secrecy capacity loss. Hence, η_I needs to be carefully chosen in order to achieve a better secrecy throughput performance for given parameters N, ρ and K.

V. Numerical Results

In this section, we perform empirical simulations to evaluate the secrecy throughput with the proposed user scheduling in the uplink wiretap network and investigate the effects of N, ρ and K on the secrecy throughput.

Fig. 2 shows the optimal η_I for varying N. The optimal η_I tends to be smaller as the number of users increases, which means more strict condition on the capacity loss due to the eavesdroppers is favorable when a large number of users exist.

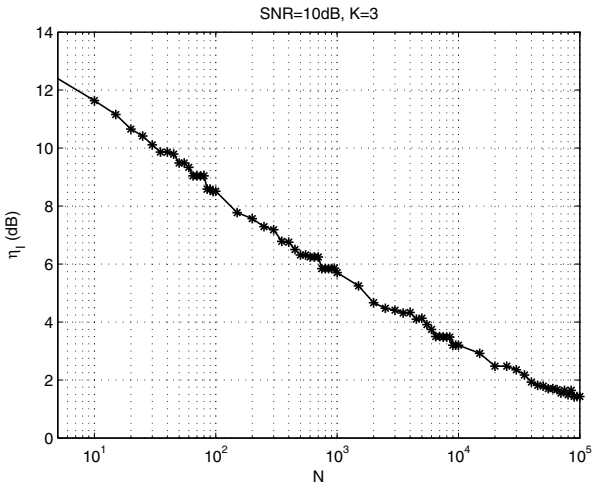

Fig. 2. The optimal η_I for the maximum secrecy throughput of the proposed user scheduling according to the number of users in a network (N).

Interestingly, the optimal η_I (in dB) becomes linearly reduced as N increases in logarithmic scale. The optimal η_I becomes large as ρ and K increase, but we omit the figures because of page limitation in this letter. In the next figures, it is assumed that the proposed scheduling operates with the optimal η_I.

Fig. 3 shows the secrecy throughput for varying the number of users in the network when $\rho=10$dB and $K=3$. In this figure, two user scheduling algorithms are considered as references: *MaxSNR* and *MinSNR*. The term of MaxSNR indicates the user scheduling algorithm that selects the user having the maximum SNR at the BS regardless of the channel gain to eavesdroppers, while the term of MinSNR indicates the user scheduling algorithm that selects the user having the minimum SNR at the eavesdroppers regardless of the channel gain to the BS. The optimal scheduling algorithm is also shown, where the scheduler selects one user in the sense of maximizing the secrecy throughput. We can observe that the secrecy throughputs of both the optimal scheduling and the proposed scheduling increase with nearly the same scale as N increases. However, the secrecy throughputs of both *MaxSNR* and *MinSNR* are much smaller than those of the optimal scheduling and the proposed scheduling. In this simulation, we assume that $\beta_{ik}=1$ for $i,k\in\{1,\cdots,K\}$.

Fig. 4 shows the secrecy throughput over varying the transmitted SNR ρ. We can observe the proposed scheduling always outperforms the conventional *MaxSNR* and *MinSNR* strategies. All algorithms are saturated in terms of secrecy throughput as ρ increases and there exists a *constant gap* between the throughput of the optimal scheduling and that of the proposed scheduling.

Fig. 5 shows the secrecy throughput of various scheduling algorithms for varying the number of eavesdroppers, K. It is shown that the secrecy throughput decreases as the number of eavesdroppers increases as expected. However, the proposed user scheduling yields almost the same throughput as that of the optimal scheduling regardless of K.

VI. Conclusion

We have proposed a sub-optimal user scheduling which operates with a threshold related to the channel gain to the

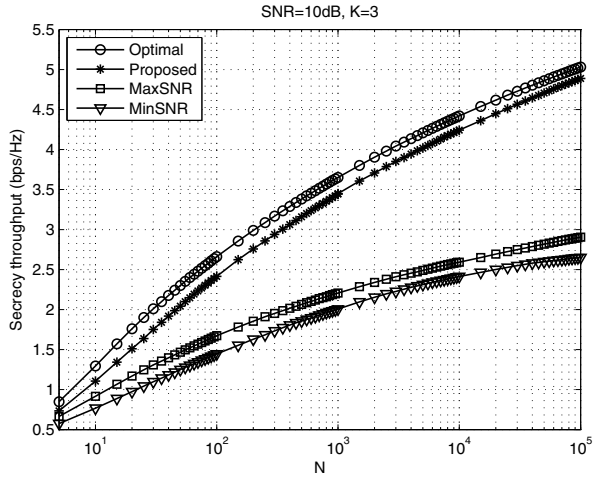

Fig. 3. Secrecy throughput of various user scheduling algorithms for varying N when $K = 3$ and $\rho = 10$dB.

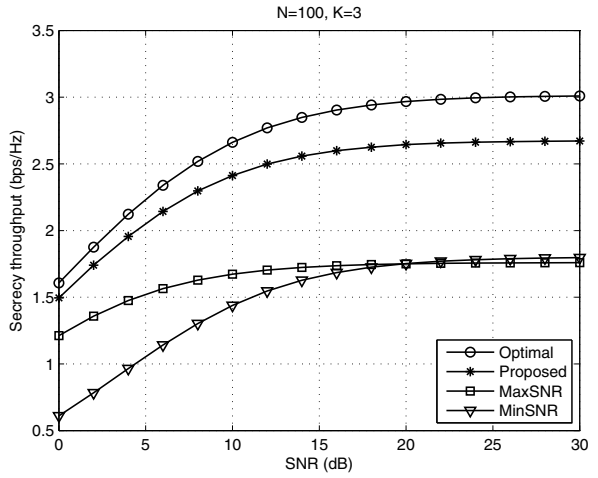

Fig. 4. Secrecy throughput for varying SNR (ρ) when $K = 3$ and $N = 100$.

eavesdroppers. It was proved that the secrecy throughput of the proposed user scheduling is optimal in that its throughput scaling is the same as that of the uplink network without eavesdroppers. As a by-product, it was proved that the optimal throughput scaling can be achieved in uplink wiretap networks.

APPENDIX

A. Proof of Lemma 1

If $\lim_{x\to\infty} xf(x) \to \infty$, then it follows that $f(x) = \omega\left(\frac{1}{x}\right)$ [16], thus resulting in

$$\lim_{x\to\infty} (1 - f(x))^x = o\left(\lim_{x\to\infty} \left(1 - \frac{1}{x}\right)^x\right) = o(1)$$

for $0 < f(x) \leq 1$. It is hence seen that $\lim_{x\to\infty} (1 - f(x))^x$ converges to zero. If $\lim_{x\to\infty} xf(x)$ is finite, then there exists a constant $c_3 > 0$ such that $xf(x) < c_3$ for any $x \geq 0$. We then have

$$\lim_{x\to\infty} (1 - f(x))^x > \lim_{x\to\infty} \left(1 - \frac{c_3}{x}\right)^x = e^{-c_3} > 0,$$

which completes the proof.

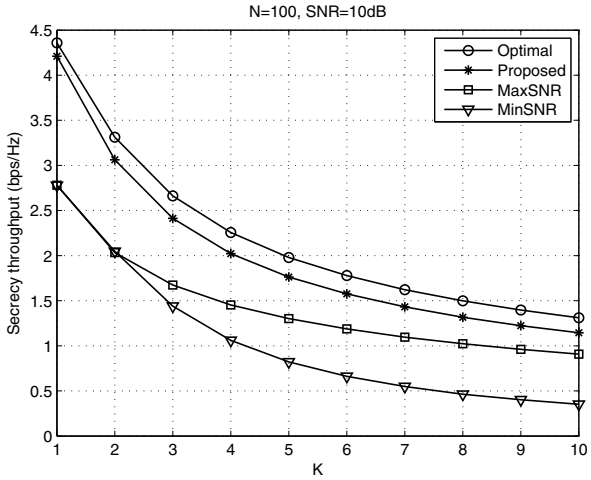

Fig. 5. Secrecy throughput according to the number of eavesdroppers (K) when $N = 100$ and $\rho = 10$dB.

REFERENCES

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

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

[3] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: encryption over the channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5059–5067, Nov. 2008.

[4] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[5] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[6] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers," in *Proc. 2012 Allerton Conf. Commun., Control and Comput.*, pp. 193–200.

[7] R. Knopp and P. A. Humblet, "Information capacity and power control in single cell multiuser communications," in *Proc. 1995 IEEE International Conference on Communications*, pp. 331–335, Jun. 1995.

[8] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1277–1294, Jun. 2002.

[9] M. Sharif and B. Hassibi, "On the capacity of MIMO broadcast channels with partial side information," *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 506–522, Feb. 2005.

[10] W.-Y. Shin, S.-Y. Chung, and Y. H. Lee, "Parallel opportunistic routing in wireless networks," *IEEE Trans. Inf. Theory*, to appear.

[11] T. W. Ban, W. Choi, B. C. Jung, and D. K. Sung, "Multi-user diversity in a spectrum sharing system," *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 102–106, Jan. 2009.

[12] S. Vasudevan, S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. Leung, "Multi-user diversity for secrecy in wireless networks," in *Proc. 2010 Inf. Theory Applications Workshop*, pp. 1–9.

[13] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "On multiuser secrecy rate in flat fading channel," in *Proc. 2009 IEEE Military Commun. Conf.*, pp. 1–7.

[14] S. K. Leung-Van-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[15] P. K. 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.

[16] D. E. Knuth, "Big Omicron and big Omega and big Theta," *ACM SIGACT News*, vol. 8, pp. 18–24, Apr.-Jun. 1976.

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