On the Secrecy Capacity of Multi-Cell Uplink Networks with Opportunistic Scheduling

Hu Jin, Bang Chul Jung†, and Won-Yong Shin*
Dept. Electronics and Communication Engineering, Hanyang University, Ansan, Korea
†Dept. Electronics Engineerring, Chungnam National University, Daejeon, Korea
*Division of Mobile Systems Engineering, Dankook University, Yongin, Korea
Email: hjin@hanyang.ac.kr, †bcjung@cnu.ac.kr, *wyshin@dankook.ac.kr

***Abstract*—In this paper, we propose a novel user scheduling that achieves the *optimal* multi-user diversity gain in multi-cell uplink networks with multiple eavesdroppers. In the proposed scheduling, each base station (BS) selects a certain user based on two pre-determined thresholds (i.e., scheduling criteria). The first threshold is related to the amount of generating interference of the users to other BSs and the second threshold is related to the maximum amount of information overheard by the eavesdroppers in the network. Simulation results show that the proposed scheduling significantly outperforms the other scheduling algorithms in terms of secrecy throughput. Note that the proposed scheduling can operate with a distributed manner when time division duplex is adopted, i.e., no coordination among different BSs is needed.**

***Index Terms*—Cellular networks, inter-cell interference, multi-user diversity, physical-layer security, secrecy capacity.**

I. Introduction

Since the seminal paper by Shannon [1], there has been a steady push to characterize the information-theoretic secrecy and to establish the achievability of secure communications in wiretap channels with eavesdroppers. Especially, to fundamentally analyze multi-user channel models with secrecy constraints, the essential role of secret-key generation [2], feedback [3], and cooperative jamming [4] has been highlighted as a means of increasing secrecy rates. Since in most multi-user scenarios, it is difficult to obtain the exact secrecy capacity region, there has recently been a significant interest in analyzing the asymptotic performance of a variety of multi-user wiretap networks assuming multiple sources/eavesdroppers in terms of secure degrees-of-freedom [5], [6].

On the other hand, there are some results on the usefulness of fading in single-cell broadcast channels, where one can exploit a multi-user diversity gain: opportunistic scheduling [7] and opportunistic beamforming [8]. Unlike the case of single-cell scenarios [7], [8], interference between wireless links existing in multi-cell networks is a critical problem. To solve the interference problem in cellular networks, a distributed opportunistic scheduling strategy was introduced in [9] while achieving full multi-user diversity gain under a certain user scaling condition. Moreover, scenarios obtaining the multi-user diversity have been studied in cooperative ad hoc networks [10] and in cognitive radio networks [11].

Besides the studies in [7]–[11], an important factor that we need to consider for secure communications is the presence of (potential) multiple eavesdroppers in wiretap channels. In [12], it has been studied how to exploit the multi-user diversity gain by using an opportunistic trusted-relay selection over two hops. The problem of broadcasting secret information was also examined in [13], where it was shown that the average secrecy rate is rather reduced as the number of receivers/users increases, thus resulting in no multi-user diversity gain. In ad hoc networks with multiple eavesdroppers [14], the achievable secure rate scaling was characterized by using a multihop transmission strategy, while the benefit of fading was not analyzed under the network model. Recently, in *single-cell* uplink wiretap networks having multiple eavesdroppers, it was shown that the optimal multi-user diversity gain can be obtained using a simple user scheduling method based on a pre-determined threshold [15]. It however remains open how to generalize the scheme in [15] to cellular network setups having multiple active transmitters since inter-cell interference issues also need to be carefully taken into account.

In this paper, we propose a novel opportunistic user scheduling which achieves the *optimal* multi-user diversity gain, i.e., $\log\log N$, by exploiting the usefulness of fading even in an uplink *multi-cell* wiretap network, which consists of M cells, N legitimate users in each cell, and K malicious eavesdroppers. In this network, we need to jointly take into account inter-cell interference of cellular networks and the presence of multiple eavesdroppers. To handle the above issues, in the proposed user scheduling, instead of using complex coding schemes (e.g., superposition coding), each base station (BS) selects a certain user based on two pre-determined thresholds (i.e., scheduling criteria). The first threshold is related to the amount of generating interference of the users to other BSs and the second threshold is related to the maximum amount of information overheard by K eavesdroppers in the network. To our knowledge, such a scheduling strategy, enabling both interference management and perfectly secure communication in a distributed fashion, for multi-cell uplink networks in the presence of multiple sources/eavesdroppers has never been proposed before in the literature. Numerical evaluation indicates that the proposed opportunistic user scheduling has a much higher secrecy throughput than that of the other scheduling methods.

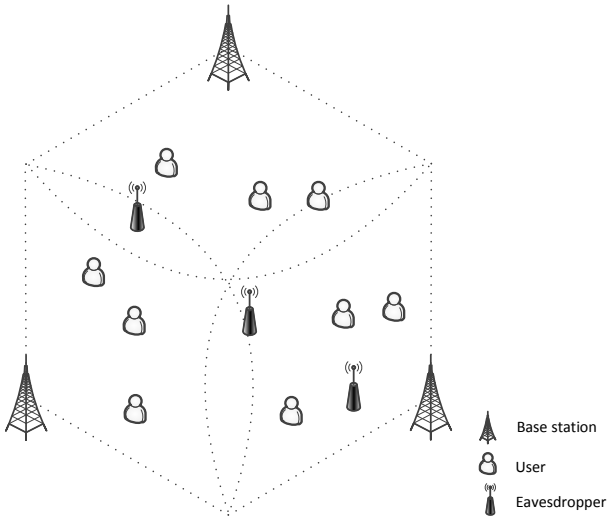

Fig. 1. A multi-cell uplink wiretap network consisting of multiple BSs, multiple users, and multiple eavesdroppers

The rest of the paper is organized as follows. Section II describes the system model. The opportunistic user scheduling based on thresholds is proposed in Section III. In Section IV, the achievable secrecy throughput scaling of the proposed scheduling is analyzed. Numerical results are shown in Section V. Finally, conclusion is drawn in Section VI.

II. System model

For the system model, M cells are considered. In each cell, N legitimate users communicate with a BS in the uplink. Within the area of M cells, there exist K eavesdroppers which try to overhear the communications from users to BSs. We assume that all nodes (user, BS, or eavesdropper) are equipped with a single antenna. Figure 1 shows an example of the system model when $M = 3$ and $K = 3$.

The term $\alpha_{iu_m} h_{iu_m} \in \mathbb{C}$ denotes the channel coefficient between user u_m in the m-th cell and the BS i, consisting of the large-scale path-loss component α_{iu_m} and the small-scale fading component h_{iu_m}, where $u_m \in \{1, \cdots, N\}$ and $i, m \in \{1, \cdots, M\}$. The term $\beta_{ku_m} g_{ku_m} \in \mathbb{C}$ denotes the channel coefficient between user u_m in the m-th cell and the k-th eavesdropper, consisting of the large-scale path-loss component β_{ku_m} and the small-scale fading component g_{ku_m}, where $k \in \{1, \cdots, K\}$. For simplicity, we assume that all legitimate users experience the same degree of path-loss attenuation to the BS, i.e., the large-scale term α_{iu_m} is assumed to be 1. [1] The small scale fading follows the complex Gaussian distribution, having zero mean and unit variance and being independent across different i, k and u_m. We also assume a block-fading model, i.e., the channels are fixed during one block (e.g., frame) and changes independently for every block. Suppose that only one legitimate user transmits its data packet through a certain scheduling algorithm in each cell.[2]

Then, when users $u_1, u_2, \cdots, u_M$, are transmitting, the received signals at the i-th BS, $y_i \in \mathbb{C}$, and at the k-th eavesdropper, $w_k \in \mathbb{C}$, are given by

$$\begin{aligned} y_i &= h_{iu_i} x_{u_i} + \sum_{\substack{m=1 \\ m \neq i}}^{M} h_{iu_m} x_{u_m} + z_{B,i}, \quad \text{for } i = 1, 2, \cdots, M, \\ w_k &= \sum_{m=1}^{M} \beta_{ku_m} g_{ku_m} x_{u_m} + z_{E,k}, \qquad \text{for } k = 1, 2, \cdots, K, \end{aligned} \tag{1}$$

where x_{u_m} represents the transmit symbol of user u_m. $z_{B,i} \in \mathbb{C}$ and $z_{E,k} \in \mathbb{C}$ denote circularly symmetric complex additive white Gaussian noise (AWGN) at the i-th 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 u_m-th user knows its channel gains to the BSs and the eavesdroppers, i.e., h_{iu_m} and $\beta_{ku_m} g_{ku_m}$. The secrecy throughput of the i-th cell is then expressed as [16], [17]:

$$C_i = C_{B,i} - C_{E,i}, \tag{2}$$

where

$$C_{B,i} = \log\left(1 + \frac{\rho |h_{iu_i}|^2}{1 + \rho \sum_{m=1, m\neq i}^{M} |h_{iu_m}|^2}\right), \tag{3}$$

$$C_{E,i} = \log\left(1 + \max_{k \in \{1,2,\cdots,K\}} \left\{ \frac{\rho |\beta_{ku_i} g_{ku_i}|^2}{1} + \rho \sum_{m=1, m\neq i}^{M} |\beta_{ku_m} g_{ku_m}|^2 \right\}\right). \tag{4}$$

Here $C_{B,i}$ denotes the achievable data rate of the i-th cell when there are no eavesdroppers, while $C_{E,i}$ denotes the data rate loss due to the eavesdroppers. As observed from (2), the secrecy throughput of each cell is affected by other cell interference from users as well as the eavesdroppers. Hence, user scheduling should be carefully designed in order to exploit the multi-user diversity.

III. Opportunistic User Scheduling with Thresholds

When there are no eavesdroppers and no inter-cell interference in an uplink network, it is well known that the optimal throughput scales as $\log \log N$ when the number of users in a network (N) tends to infinity [7]. However, the optimal secrecy throughput scaling in the multi-cell uplink has not been shown. In this section, we propose a threshold-based scheduling algorithm which achieves the same throughput scaling even though there exist both inter-cell interference and eavesdroppers. In the proposed user scheduling algorithm, in each cell one user is selected in the sense of having large channel gain to the serving BS as well as reducing the

[1] In practical wireless systems, the path-loss component of users is different from each other. However, as explained in Section 4, the path-loss does not affect the throughput scaling which is the main theoretical result of this paper.

[2] It is sufficient to achieve full degrees-of-freedom gain in this model.

capacity loss due to the eavesdroppers and reducing generating interference to other BSs. The i-th BS finds a certain user that has the largest channel gain among the users satisfying the following two criteria:

$$\rho|h_{mu_i}|^2 \leq \eta_B, \quad \text{for } m = 1, \cdots, i-1, i+1, \cdots, M, \quad (5)$$

$$\rho|\beta_{ku_i} g_{ku_i}|^2 \leq \eta_E, \quad \text{for } k = 1, 2, \cdots, K, \quad (6)$$

where η_B and η_E denote two pre-determined positive thresholds. In particular, the value η_B and η_E are set to small values in order to assure that the capacity loss due to inter-cell interference and the eavesdroppers is small. Suitable values of η_B and η_E will be specified in the next section. The users satisfying (5) and (6) send scheduling requests to their corresponding BSs. Note that each user can determine the feedback of the scheduling request in the case of time division duplex (TDD) because it can estimate the channels via pilot signals from BSs, and thus the proposed scheduling can operate with a distributed manner in each cell.

IV. Secrecy Throughput Analysis

In this section, we show that the user scheduling proposed in Section III asymptotically achieves the optimal multi-user diversity gain, i.e., $\log\log N$, in each cell. 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 multi-user diversity gain in the multi-cell uplink networks with eavesdroppers. We start from the following lemma.

Lemma 1: Let $f(x)$ denote the value of the function f at position x, where the function f is given by f: $[0, \infty) \to R$ with $x \mapsto f(x)$. If $0 < f(x) \leq 1$, $\lim_{x\to\infty} (1 - f(x))^x$ converges to zero if and only if $\lim_{x\to\infty} x f(x)$ tends to infinity.

Proof: See Appendix A. ∎

Since the channel coefficient is assumed to follow complex Gaussian distribution, the term $|h|^2$ ($= |h_{iu_m}|^2$ or $|g_{ku_m}|^2$) is exponentially distributed, and its cumulative distribution function (CDF) is given by

$$\Pr\left\{|h|^2 \leq x\right\} = 1 - e^{-x} \quad \text{for } x \geq 0. \quad (7)$$

Thus, the CDF of the largest value among L exponential random variables is given as

$$F_L(x) = (1 - e^{-x})^L. \quad (8)$$

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

Lemma 2: For any $0 \leq x < 1$, $F_L(x)$ in (8) is lower-bounded by

$$F_L(x) \geq c_L x^L, \quad (9)$$

where $c_L = (1 - e^{-1})^L$.

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

$$1 - e^{-x} \geq (1 - e^{-1})x, \quad \text{for } 0 \leq x < 1, \quad (10)$$

which completes the proof. ∎

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

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 $\rho^{\frac{K+M-1}{1-\epsilon_0}}$ 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 the modified scheduling, the BS in the i-th cell randomly selects one user among users satisfying (5), (6) and the following criterion:

$$|h_{iu_i}|^2 \geq \eta_{\text{tr}}, \quad u_i = 1, 2, \cdots, N. \quad (11)$$

Since the proposed scheduling selects the user showing the maximum signal strength at each BS while satisfying (5) and (6), the proposed scheduling always result in a better secrecy throughput performance than the modified scheduling in this section. Therefore, the throughput of the modified scheduling can be regarded as the lower bound of the throughput of the proposed scheduling in Section III.

Suppose that $\eta_{\text{tr}} = \epsilon \log N$. Let β be the maximum value among β_{ku_m} where $k \in \{1, \cdots, K\}$, $m \in \{1, \cdots, M\}$ and $u_m \in \{1, \cdots, N\}$. Then, in the i-th cell, the event that user u_i satisfies the three conditions (5), (6) and (11) occurs with a probability larger than or equal to $F_{M-1}(\eta_B)F_K(\eta_E\rho^{-1}\beta^{-2})e^{-\eta_{\text{tr}}}$. The probability that at least one user satisfies the three conditions in each cell is lower-bounded by

$$1 - \left[1 - F_{M-1}(\eta_B\rho^{-1})F_K(\eta_E\rho^{-1}\beta^{-2})e^{-\eta_{\text{tr}}}\right]^N. \quad (12)$$

By *Lemma 1*, (12) converges to 1 as N tends to infinity, if and only if

$$\lim_{N\to\infty} N F_{M-1}(\eta_B\rho^{-1})F_K(\eta_E\rho^{-1}\beta^{-2})e^{-\eta_{\text{tr}}} \to \infty. \quad (13)$$

From *Lemma 2*, the term in (13) can be lower-bounded by

$$\begin{aligned}
&\lim_{N\to\infty} N c_{M-1}(\eta_B\rho^{-1})^{M-1} c_K \left(\eta_E\rho^{-1}\beta^{-2}\right)^K e^{-\eta_{\text{tr}}} \\
&= c_{M-1}c_K\eta_B^{M-1}\eta_E^K\beta^{-2K} \cdot \lim_{N\to\infty} \frac{N}{\rho^{K+M-1}} e^{-\epsilon\log N} \\
&= c_{M-1}c_K\eta_B^{M-1}\eta_E^K\beta^{-2K} \cdot \lim_{N\to\infty} \frac{N^{1-\epsilon}}{\rho^{K+M-1}},
\end{aligned}$$

which increases with N (or equivalently ρ) as N scales as $\rho^{\frac{K+M-1}{1-\epsilon_0}}$ for $\epsilon_0 \in (\epsilon, 1)$. Hence, there exists at least one user satisfying (5), (6) and (11) whp. From (5), (6) and (11), we can calculate the following bounds for $C_{B,i}$ and $C_{E,i}$ as

$$\begin{aligned}
C_{B,i} &\geq \log\left(1 + \frac{\rho\eta_{\text{tr}}}{1 + (M-1)\eta_B}\right), \\
C_{E,i} &\leq \log\left(1 + \max_{k\in\{1,2,\cdots,K\}} \rho|g_{ku_i}|^2\right) \\
&\leq \log\left(1 + \eta_E\right).
\end{aligned} \quad (14)$$

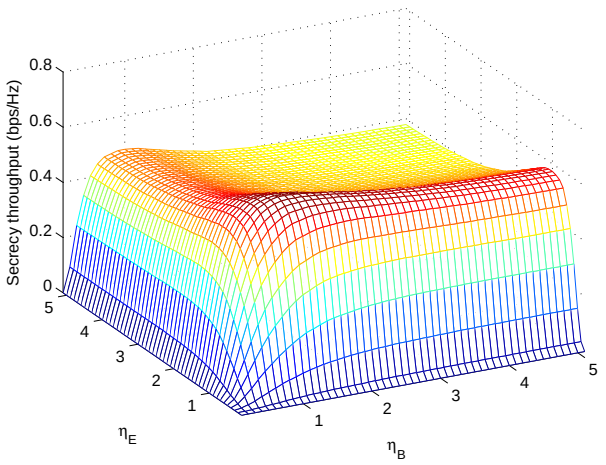

Fig. 2. Secrecy throughput for varying η_B and η_E when $K = 3$, $M = 3$, $N = 100$ and $\rho = 0$dB.

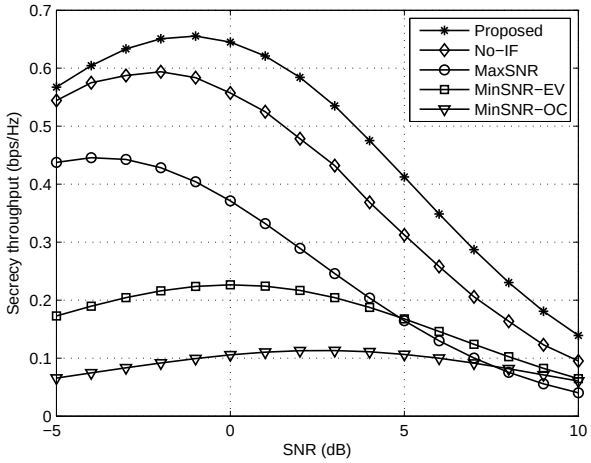

Fig. 3. Secrecy throughput for varying SNR (ρ) when $K = 3$, $M = 3$ and $N = 100$.

From (2), a lower bound on the achievable secrecy throughput of the i-th cell is finally given by

$$\begin{aligned} C_i &\geq \log\left(1+\frac{\rho\eta_{\mathrm{tr}}}{1+(M-1)\eta_B}\right)-\log\left(1+\eta_E\right) \\ &= \log\left(\frac{1}{1+\eta_E}+\frac{\epsilon\cdot\rho\log N}{(1+\eta_E)(1+(M-1)\eta_B)}\right) \\ &= \log\left(d_1+d_2\epsilon\rho\log N\right), \end{aligned} \tag{15}$$

which scales as $\log(\rho\log N)$, under the condition that N scales as $\rho^{\frac{K+M-1}{1-\epsilon_0}}$, where $d_1, d_2 > 0$ are constant values. This completes the proof of the theorem. ■

V. Numerical Results

In this section, we perform extensive computer simulations in order to evaluate the secrecy throughput of the proposed scheduling in the multi-cell uplink networks and investigate the effect of the parameters N, ρ and K on the secrecy throughput. Figure 2 shows the secrecy throughput for varying η_B and η_E when $K = 3$, $M = 3$, $N = 100$ and $\rho = 0$dB. We can observe that the maximum secrecy throughput, 0.64 (bps/Hz), is obtained when $\eta_B = 1.33$ and $\eta_E = 1.01$. We need to carefully choose the scheduling criteria to maximize the secrecy throughput in various environments. In the following figures, we obtain the secrecy throughput of the proposed scheduling with the optimal criteria (η_B and η_E) which are obtained through two dimensional exhaustive search.

Figure 3 shows the secrecy throughput for varying SNR (ρ) when $K = 3$, $M = 3$ and $N = 100$. In this figure, four other scheduling algorithms are also considered: *No-IF*, *MaxSNR*, *MinSNR-EV* and *MinSNR-OC*. The term No-IF indicates the user scheduling algorithm that only considers the threshold related to eavesdroppers as in [15]. For No-IF, the optimal threshold within each single cell is also numerically obtained. The term of MaxSNR indicates the user scheduling algorithm that selects the user having the maximum SNR at the BS and the term of MinSNR-EV represents the user scheduling algorithm that selects the user having the minimum SNR at the eavesdroppers. The term of MinSNR-OC represents the user scheduling algorithm that selects the user generating minimum interference to the other cells. The proposed scheduling outperforms other scheduling algorithms over all SNR values in terms of secrecy throughput. Note that there exists the optimal point such that the maximum throughput is achieved for all scheduling algorithms according to SNR values, which means that the increase of power at users does not lead to the better secrecy throughput in the multi-cell uplink networks.

Figure 4 shows the secrecy throughput for varying the number of legitimate users in a cell when $K = 3$, $M = 3$ and $\rho = 0$dB. By help of the multi-user diversity gain, all scheduling algorithms yield better throughput as N increases and the proposed algorithm significantly outperforms other scheduling algorithms. The performance gap between the proposed algorithm and the other algorithms increases as N increases.

Fig. 5 shows the secrecy throughput of various scheduling algorithms for varying the number of eavesdroppers, K. The proposed scheduling yields the best performance. However, the throughput gain of the proposed algorithm over the No-IF scheme becomes smaller as the number of eavesdroppers increases. This is mainly because the throughput loss due to the eavesdroppers becomes more dominant than loss from the other cell interference as the number of eavesdroppers increases.

VI. Conclusion

We proposed a user scheduling that achieves the *optimal* multi-user diversity gain in multi-cell uplink networks with multiple eavesdroppers, in which each BS selects a certain user by considering both the amount of generating interference from users to other BSs and the amount of information overheard by eavesdroppers. In the proposed scheduling, the thresholds should be carefully determined for better perfor-

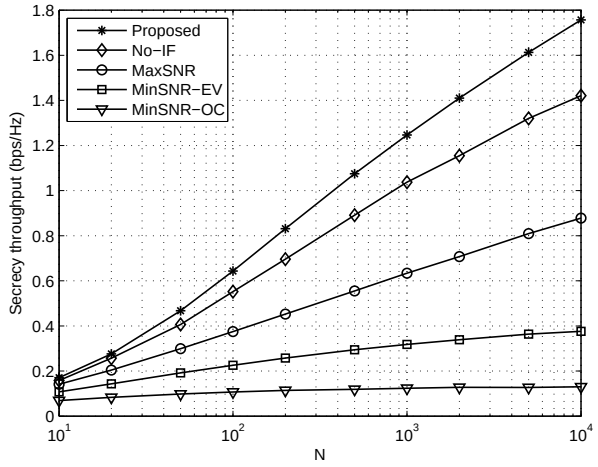

Fig. 4. Secrecy throughput for varying N when $K = 3$, $M = 3$ and $\rho = 0$dB.

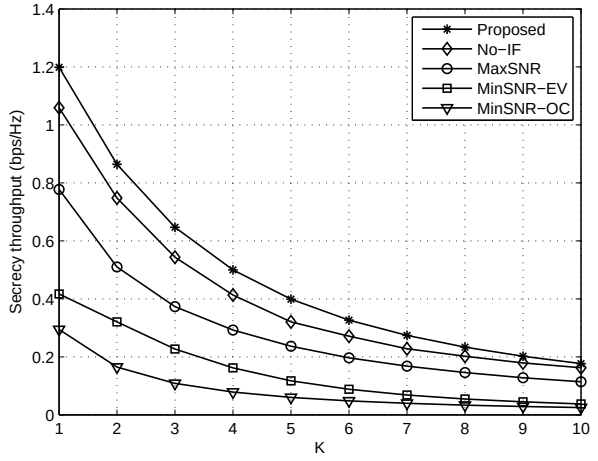

Fig. 5. Secrecy throughput for varying the number of eavesdroppers (K) when $N = 100$, $M = 3$ and $\rho = 0$dB.

mance. Extensive simulation results verify that the proposed scheduling significantly outperforms the other scheduling algorithms in terms of secrecy throughput.

APPENDIX

If $\lim_{x\to\infty} xf(x) \to \infty$, then it follows that $f(x) = \omega\left(\frac{1}{x}\right)$ [18], 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 $d_3 > 0$ such that $xf(x) < d_3$ for any $x \geq 0$. We then have

$$\lim_{x\to\infty} (1 - f(x))^x > \lim_{x\to\infty} \left(1 - \frac{d_3}{x}\right)^x = e^{-d_3} > 0,$$

which completes the proof.

ACKNOWLEDGEMENT

This work was supported partly by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (2015R1C1A1A01053857), IITP grant funded by the Korea government (MSIP) (No. B0126-15-1064, Research on Near-Zero Latency Network for 5G Immersive Service), and the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (MSIP) (2015R1A2A1A15054248).

REFERENCES

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

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, May 1993.

[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, June 2011.

[6] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers," in *Proc. Annual Allerton Conf. Commun., Control and Comput.*, Monticello, IL, Oct. 2012.

[7] R. Knopp and P. A. Humblet, "Information capacity and power control in single cell multiuser communications," in Proc. *IEEE International Conference on Communications (ICC)*, 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] W.-Y. Shin, D. Park, and B. C. Jung, "Can one achieve multiuser diversity in uplink multi-cell networks?," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3535–3540, Dec. 2012.

[10] W.-Y. Shin, S.-Y. Chung, and Y. H. Lee, "Parallel opportunistic routing in wireless networks," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6290–6300, Oct. 2013.

[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. Inf. Theory Applications Workshop (ITA)*, San Diego, CA, Jan./Feb. 2010.

[13] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "On multiuser secrecy rate in flat fading channel," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Boston, MA, Oct. 2009.

[14] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[15] H. Jin, W.-Y. Shin, and B. C. Jung, "On the multi-user diversity gain with secrecy in uplink wiretap networks," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1778–1781, Sep. 2013.

[16] 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.

[17] 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.

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