Fair Rate Allocation for Broadcast Channel with Confidential Messages

Zhoujia Mao, C. Emre Koksal, Ness B. Shroff
E-mail: mao.29@osu.edu, koksal@ece.osu.edu, shroff@ece.osu.edu

***Abstract*—We consider a degraded block-fading broadcast channel, in which we treat each user as an "internal eavesdropper" for the information transmitted to another user. We addressed the problem of maximizing cumulative network utility, which is a function instantaneous rate of confidential data served for all users. Then, we propose a low complexity, provably optimal algorithm that jointly selects the amount of information to be transmitted to all users from the region of achievable open and secrecy rates in each block. In the described setup, there exists only one user with positive instantaneous secrecy rate, i.e., full equivocation from other users in a given block. Unlike existing scheduling approaches that serve only the user with the positive secrecy rate in each block, we propose a system that uses part of the secrecy rate for key generation, to be utilized at later times in the form of a one-time pad. To be able to serve a larger region of open-secrecy rates so that multiple users can simultaneously transmit data with full equivocation, we use superposition encoding and binning. Our system leads to a smoother service process, which increases the achieved long term utility, compared to the opportunistic scheduling approach.**

I. Introduction

With the recent studies (e.g., [1]–[6]), we have a better understanding on the basic limits and various schemes to achieve these limits for broadcast channels with confidential messages. In particular, [1], [2], [5], [6] considered a limited number of user types and studied capacity achieving schemes to encode information. In [3], the authors study a more general setting to evaluate the secrecy rate region for both common and independent messages to multiple users over the fading broadcast channel. There, the eavesdropper is external to the system, whereas [4] approaches a similar problem where the messages are to be kept confidential from other users in the system, i.e., internal eavesdroppers. Despite the significant progress in broadcast secrecy, most of the efforts have focused solely on the physical layer. Indeed, our understanding of how the physical layer secrecy techniques influence components of other layers remains limited.

In parallel, there has been some recent efforts [7]–[9] to build network mechanisms to engineer the service process for confidential data arriving at a data queue, with the motivation of achieving a low delay over the wiretap channel. The main mechanism to achieve this goal is motivated by [7], where the authors proposed the idea of using a key queue in the secrecy communication system. A key queue is maintained at both the transmitter and the receiver. Instead of using the entire instantaneous secrecy rate for information transmission, part of it is utilized to transmit random key bits that are stored at the receiver. These stored key bits are used later as a one-time pad to secure information bits. By a careful control of the amount of key generation, the secrecy rate can be smoothed out, leading to desirable delay properties. It is shown in [9] that, using this idea, a non-zero secrecy outage capacity can be achieved and that the ergodic secrecy capacity can be achieved in a delay-limited sense as long as certain conditions are satisfied. Low complexity cross layer algorithms are proposed in [8] to achieve the maximum achievable rate without any statistical knowledge on the state of the wiretap channel.

In this paper, we generalize the system introduced in [8] to the broadcast setting. We consider a degraded block-fading broadcast channel, in which we treat a user as an "internal eavesdropper" for the information transmitted to another user. In the fading broadcast channel, there exists only one user with positive instantaneous secrecy rate, i.e., full equivocation from other users in a given time slot. Consequently, existing solutions for network control (e.g., [10]) have mainly focused on pure scheduling, i.e., serve the user with the positive secrecy rate. While it maximizes the sum secrecy rate (as shown in [10]), this approach leads to a highly bursty service process over time and may lead to long droughts for a set of users. To that end, we specify the problem of secure transmission as that of network utility maximization. We exploit the aforementioned joint key and information transmission mechanism and expand it for the broadcast setting. We propose a simple and provably efficient algorithm which jointly selects secrecy and open rates in the given region for all users in each time slot. The main idea is to smooth out the service process for all users, which in turn increases the achieved utility.

Note that the broadcast secrecy model studied in our paper is the same as that in [4]. However, *our main objective is to allocate transmission rates fairly over users and over time*. Therefore, we are interested in a more general rate region in which all users can achieve positive open rates in each time slot. This leads to the essential difference of the encoding scheme in our paper and that in [4]. In [4], only one user is scheduled for transmission at a time but we use superposition encoding and successive decoding so that all users can achieve non-negative open rates. These open rates are exploited to transmit information, secured with the key bits, so that they remain confidential from other users.

II. Problem Description

We consider a downlink cellular network with one base station and K users. The base station communicates with

K users over a block fading broadcast channel, composed of K independent point-to-point channels. We assume that these channels have a constant gain within a block (coherence interval) of n channel uses, and vary from block to block. The length of a time block is assumed to be large enough to invoke random coding techniques. Let $\pi_1(t), \pi_2(t), \ldots, \pi_K(t)$ denote the user indices that are ranked from the smallest to the largest according to their instantaneous channel states (achievable rates) in each block t. Let $X(t)$ denote the signal, broadcast from the base station and $Y_{[\pi_1(t),\pi_K(t)]}(t)$ denote the received signal (channel outputs) by K users. We assume that the broadcast channel is degraded, i.e., $X(t) \rightarrow Y_{\pi_K(t)}(t) \rightarrow Y_{\pi_{K-1}(t)}(t) \rightarrow \ldots \rightarrow Y_{\pi_2(t)}(t) \rightarrow Y_{\pi_1(t)}(t)$ forms a Markov chain in each block t. In each block, a sequence of independent messages $M_i(t),\ i = 1, 2, \ldots, K$ from messages sets $\mathcal{M}_i(t) = \{1, 2, \ldots, 2^{nR_{m,i}(t)}\},\ i = 1, 2, \ldots, K$ is available at the base station to be transmitted to the users at that block. We assume that the messages transmitted at the beginning of each block must be decoded by the end of block (delay-limited transmission). Within block t, the base station uses a $(2^{nR_{m,1}(t)}, 2^{nR_{m,2}(t)}, \ldots, 2^{nR_{m,K}(t)}, n)$ code $\mathcal{C}_n(t)$ to map these K messages into a signal $X^n(t)$. We assume the transmission power is fixed power across blocks. Each decoder $i \in \{1, 2, \ldots, K\}$ maps the received signal $Y_i^n(t)$ to a message $\tilde{M}_i(t) \in \mathcal{M}_i(t)$.

We consider the problem of maximizing long term utility of secrecy rates subject to reliable and secrecy constraints.

$$(A) \quad \max_{\vec{\mu}} \qquad \liminf_{T\rightarrow\infty} \frac{1}{T}\sum_{t=0}^{T-1}\sum_{i=1}^{K} U_i\big(\mu_i(t)\big)$$

$$P_e(\mathcal{C}_n(t)) \triangleq Prob(M_{[1,K]}(t) \neq \tilde{M}_{[1,K]}(t)|\mathcal{C}_n(t)) \leq \epsilon, \quad (1)$$

$$\lim_{T\rightarrow\infty} \frac{1}{n} H(M_i(t)|Y^{nT}_{[1,K]\backslash i}\mathcal{C}_n(t)) \geq \mu_i(t) - \epsilon,\ i = 1, 2, \ldots, K, \quad (2)$$

for all t, where $\epsilon > 0$ is an arbitrarily small value, $\mu_i(t)$ is the secrecy transmission rate of user i in block t, and the utility functions $U_i(\cdot),\ i = 1, 2, \ldots, K$ are assumed to be monotonically increasing, reversible and differentiable on the half real line $\Re^+ \bigcup \{0\}$. Furthermore, $H(M_i(t)|Y^{nT}_{[1,K]\backslash i}, \mathcal{C}_n(t))$ is the conditional entropy of user i's message given all other users' received information over T blocks, and $\frac{1}{n}H(M_i(t)|Y^{nT}_{[1,K]\backslash i}\mathcal{C}_n(t))$ is then the equivocation rate [11] of user i given the information of other users over T blocks. Note that, when $U_i(\cdot),\ i = 1, 2, \ldots, K$ are concave functions, the objective of Problem (A) will tend to increase as the allocated rates are less variable across time (a la Jensen's). This leads to a solution with a smooth secure transmission rate over time. Furthermore, with a carefully chosen concave function, a fair (e.g., by the use of log utility) allocation across users can also be achieved. Constraint (1) states that there exists a code $\mathcal{C}_n(t)$ in each block t with sufficiently large n symbols such that the decoding error probability is arbitrarily small. Constraint (2) means that the instantaneous secrecy transmission rate is bounded by the equivocation rate over sufficiently large T blocks, which ensures that the decoded message achieves weak secrecy from other users [11].

III. Characterization of the Instantaneous Achievable Rates

In each block t, an *open-secrecy rate vector* $(R_{m,[1,K]}(t), R_{s,[1,K]}(t))$ is achievable if there exists a code $\mathcal{C}_n(t)$ such that for any $\epsilon > 0$, the following are satisfied:

$$P_e(\mathcal{C}_n(t)) \triangleq Prob(M_{[1,K]}(t) \neq \tilde{M}_{[1,K]}(t)|\mathcal{C}_n(t)) \leq \epsilon, \quad (3)$$

$$\frac{1}{n} H(M_i(t)|Y^n_{[1,K]\backslash i}(t), \mathcal{C}_n(t)) \geq R_{s,i}(t) - \epsilon,\ i = 1, 2, \ldots, K. \quad (4)$$

Note that Constraint (4) gives the "instantaneous" equivocation rate, which is different from the equivocation rate over T blocks as in Equation (2). In (4), we condition on the instantaneous observation vector of each user in the current block, whereas in (2), the observations across the entire session of T blocks are considered. Thus, satisfying (4) does not automatically guarantee (2). We define $\Lambda(t)$ to be the instantaneous region of open-secrecy rates. The following theorem characterizes $\Lambda(t)$. The theorem holds for any t and we drop the time index t for ease of notation.

Theorem 1: Suppose the broadcast channel is degraded and the received signals at K users $Y_K \rightarrow Y_{K-1} \rightarrow \ldots \rightarrow Y_2 \rightarrow Y_1$ form a Markov chain. The open-secrecy rates region Λ is achievable if and only if

$$0 \leq R_{s,i} \leq R_{m,i} \leq \begin{cases} I(X_1; Y_1),\ i = 1 \\ I(X_i; Y_i|X_{i-1}),\ i = 2, \ldots, K \end{cases}$$

$$0 \leq R_{s,i} \leq \begin{cases} I(X_K; Y_K|X_{K-1}) - I(X_K; Y_{K-1}|X_{K-1}), \\ \quad i = K \\ 0,\ i = 1, \ldots, K-1 \end{cases}. \quad (5)$$

Furthermore, Λ is convex in $(R_{m,[1,K]}, R_{s,[1,K]})$.
The proof can be found in [12].

Next, we claim that, if for all t, we choose $(R_{m,[1,K]}(t), R_{s,[1,K]}(t)) \in \Lambda(t)$, there exists a sequence of codebooks $\mathcal{C}_n(t)$ for which Equation (1) and (2) are satisfied for all t. One such strategy involves the use of secret key queues, as motivated by [7]. We elaborate on this strategy in what follows. From Theorem 1, we can see that in any block t, only the user with the best channel state (all others are degraded versions) has nonzero secrecy rate. It has been shown in [7] that the user with a zero instantaneous secrecy rate can still transmit information with full equivocation from other users in that block by introducing key queues at both transmitter and receiver sides. The basic idea is to exploit the time when the user has the best channel state to transmit some random private key bits along with the data. When a user has a 0 instantaneous secrecy rate, but a non-zero open rate, it can still use the previously shared secret key bits as a one-time pad (simply using bit-by-bit XOR operation) and transmit information bits with full equivocation [13]. The

important point here is to utilize the instantaneous secrecy rate $R_{s,i}(t)$ in region $\Lambda(t)$ of user i fully in each block t. The important thing to note about this mechanism is that, it has been shown in Theorem 2 of [7] that, if the key bits transmitted at block t satisfy the instantaneous equivocation constraint, as given in (4), and utilized later in the form of one-time pad as described above, then Constraint (2) is satisfied for the entire session. Hence, with this system, it suffices to guarantee (4) for the desired secrecy.

A separate secret key queue is kept at the base station for each user and the the mirror key queue is at the associated receiver. Let the state of the key queues for user i be $q_{k,i}(t)$. We assume that all these key buffers have infinite sizes. As illustrated in Fig. 1, the amount of secure data transmitted at time t to user i is $\mu_i(t)$. A part ($\mu_{k,i}(t)$ bits) of this data is secured using $\mu_{k,i}(t)$ key bits. The remaining $\mu_i(t) - \mu_{k,i}(t)$ bits is secured using the available secrecy rate $R_{s,i}(t)$. Since the secrecy rate is fully utilized, the portion of the secrecy rate, not used to secure data is used to generate $R_{k,i}(t)$ key bits into the ith key queue.

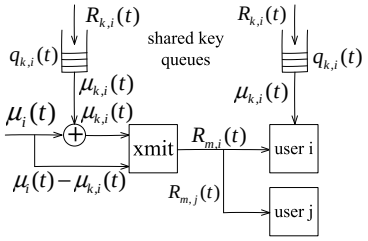

Fig. 1. Key Queue Model

The evolution of the secret-key queue can be characterized simply, as given in the following lemma we proved in [8]:

Lemma 1: [8] The key queue $q_{k,i}$ evolution can be characterized by $q_{k,i}(t+1) = q_{k,i}(t) + R_{s,i}(t) - \mu_i(t)$, subject to constraints $0 \le \mu_i(t) \le \min[q_{k,i}(t) + R_{s,i}(t), R_{m,i}(t)]$.

With the transmission rate $\mu_i(t)$, the key generation and usage rates can be calculated as follows: If the required transmission rate is larger than the secrecy encoding rate, i.e., $\mu_i(t) > R_{s,i}(t)$, then then we do not generate new key bits $R_{k,i}(t) = 0$ and use $\mu_{k,i}(t) = \mu_i(t) - R_{s,i}(t)$ amount of key bits in the key queue to secure the transmission that the secrecy rate can not support. If the required transmission rate is less than the secrecy encoding rate, i.e., $\mu_i(t) \le R_{s,i}(t)$, then then there is no need to use the stored key bits in the key queue $\mu_{k,i}(t) = 0$ and the remaining $R_{k,i}(t) = R_{s,i}(t) - \mu_i(t)$ amount of secrecy rate can be used to generate new key bits into the key queue. Note that, either key generation or key usage is zero, i.e., $\mu_{k,i}(t)R_{k,i}(t) = 0$ for all t, since any solution with $\mu_{k,i}(t) > 0$ and $R_{k,i}(t) > 0$, can be equivalently replicated by using the secrecy rate to transmit data rather than generating and using key bits at the same time.

IV. The Rate Allocation Algorithm

With the above observations, the original problem reduces to one involving the joint control of data rate and the key queues. Thus, we transform Problem (A) into the following problem:

$$(B) \quad \max_{\vec{\mu},\vec{R}_s,\vec{R}_m} \quad \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1}\sum_{i=1}^{K} U_i\big(\mu_i(t)\big)$$

$$q_{k,i}(t+1) = q_{k,i}(t) - \mu_i(t) + R_{s,i}(t), \tag{6}$$

$$0 \le \mu_i(t) \le \min[q_{k,i}(t) + R_{s,i}(t), R_{m,i}(t)], \tag{7}$$

$$(R_{m,[1,K]}(t), R_{s,[1,K]}(t)) \in \Lambda(t) \tag{8}$$

where $(\cdot)^+ = \max[\cdot, 0]$. Constraints (6) and (7) are directly from Lemma 1 and Constraint (8) characterizes the region of the open-secrecy rates $\Lambda(t)$ in each block t. Next, we provide the rate allocation algorithm to achieve smooth rates for users by using key queues.

In the case of our algorithm makes use of *virtual queues* to keep track of the instances of complete key queue outage. Let us denote the state of the virtual queues with $\tilde{q}_{k,i},\ i = 1, 2, \ldots, K$. Our virtual queues evolve according to the following equation:

$$\tilde{q}_{k,i}(t+1) = \big((\tilde{q}_{k,i}(t) - \epsilon')^+ + \mu_i(t) - R_{s,i}(t) + 1_{o,i}(t)\big)^+ \tag{9}$$

where

$$1_{o,i}(t) = \begin{cases} 0, & \text{if } \mu_i(t) = 0 \text{ or } \mu_i(t) < q_{k,i}(t) + R_{s,i}(t) \\ 1, & \text{otherwise} \end{cases} \tag{10}$$

is the indicator that the key queue $q_{k,i}$ is drained in block t and $\epsilon' > 0$ is the parameter to be chosen as follows: Identical to Lemma 7 of [8] for the single user system, keeping all virtual queues strongly stable guarantees the key outage rate to remain below ϵ'. Thus, we choose ϵ' sufficiently small so that the decoding errors due to complete drainage of the key queue remains small enough to meet (1).

Our algorithm for Problem (B) involves only rate selection. We define $V \in \Re^+$ to be the control parameter of our rate selection algorithm. In block t, the controller at the base station solves the following optimization problem and allocate the calculated rate:

$$\max_{\substack{\mu_{[1,K]}(t) \\ R_{m,[1,K]}(t) \\ R_{s,[1,K]}(t)}} \sum_{i=1}^{K} \Big[\frac{V}{2} U_i\big(\mu_i(t)\big) - \tilde{q}_{k,i}(t)\mu_i(t) + \tilde{q}_{k,i}(t)R_{s,i}(t)\Big]$$

$$s.t. \qquad (\mu_{[1,K]}(t), R_{m,[1,K]}(t), R_{s,[1,K]}(t)) \in \Pi(t) \tag{11}$$

where $\Pi(t) = \{(\mu_{[1,K]}(t), R_{m,[1,K]}(t), R_{s,[1,K]}(t)) : 0 \le \mu_i(t) \le \min[q_{k,i}(t) + R_{s,i}(t), R_{m,i}(t)],\ i = 1, 2, \ldots, K;\ (R_{m,[1,K]}(t), R_{s,[1,K]}(t)) \in \Lambda(t)\}$ is a nonempty convex set by Theorem 1. We chose Set $\Pi(t)$ to guarantee Constraints (7) and (8) in Problem (B). When $U_i(\cdot)$ is a concave function for all i, Equation (11) is a standard convex programming problem. The term $\frac{V}{2}U_i\big(\mu_i(t)\big) + \tilde{q}_{k,i}(t)R_{s,i}(t)$ can be viewed as the utility of user i by allocating transmission rate $\mu_i(t)$ and secrecy rate $R_{s,i}(t)$ and the term $\tilde{q}_{k,i}(t)\mu_i(t)$ can be viewed as its cost. When the virtual key queue $\tilde{q}_{k,i}(t)$

is small, the algorithm tries to allocate a high amount of transmitted data $\mu_i(t)$ to increase the utility; and when $\tilde{q}_{k,i}(t)$ is large, the controller allocates a small amount of transmitted data $\mu_i(t)$ and large value of secrecy rate $R_{s,i}(t)$ for user i to reduce its cost. This pushes the served data rate to be smoother over users and over time.

The following theorem evaluates the performance of our algorithm in achieving the objective of Problem (B) and hence Problem (A).

Theorem 2: If the broadcast channel is degraded and
1) $U_i(\cdot),\ \forall i$ are strictly concave on $\Re^+ \bigcup \{0\}$, and its slope at 0 satisfies $0 \leq \beta = U_i^{'}(0) < \infty,\ \forall i$,
2) $0 \leq R_{m,i}(t) \leq R_{\max,i} < \infty$ and $0 \leq \mu_i(t) \leq \mu_{\max,i} < \infty,\ \forall t \geq 0$,
then our algorithm achieves:

$$\liminf_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} \sum_{i=1}^{K} U_i\big(\mu_i(t)\big) \geq \liminf_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} \sum_{i=1}^{K} U_i\big(\mu_i^*(t)\big) - O\left(\frac{1}{V}\right), \tag{12}$$

where $y = O(x)$ implies y goes to 0 as x goes to 0, and $\mu_i^*(t)$ is the optimal transmission rate of Problem (B) for user i at time t for all i and $t \geq 0$.

From Theorem 2, we can see that the average sum utility of the transmission rates of our algorithm approaches the optimal value of Problem (B) as V increases. The proof is in [12].

V. Numerical Example

Consider a 2-user system. In block t, user $\pi_1(t)$ has a channel that is degraded from $\pi_2(t)$. We generate the region of achievable open and secrecy rates as follows. First, we generate i.i.d. processes $C_1(t)$ and $C_2(t)$ at random, uniformly distributed within $[5, 20]$ in each block t. The region is encapsulated by $0 \leq R_{m,\pi_1(t)}(t) \leq \min[C_1(t), C_2(t)]$, $0 \leq R_{m,\pi_2(t)}(t) \leq \max[C_1(t), C_2(t)]$, $R_{m,\pi_1(t)}(t) \leq R_{m,\pi_2(t)}(t)$, $R_{m,\pi_1(t)}(t) + R_{m,\pi_2(t)}(t) \leq \max[C_1(t), C_2(t)]$ for the open rates, and $R_{s,\pi_1(t)}(t) \equiv 0$, $0 \leq R_{s,\pi_2(t)}(t) \leq R_{m,\pi_2(t)}(t) - R_{m,\pi_1(t)}(t)$ for the secrecy rates in block t. Our algorithm solves for $\mu_{[1,2]}(t)$, $R_{m,[1,2]}(t)$ and $R_{s,\pi_1(t)}(t)$ as per Equation (11). For opportunistic scheduling, the user, $\pi_2(t)$, with the better channel in block t always has open and secrecy rates $\max[C_1(t), C_2(t)]$ and the other one, $\pi_1(t)$, has 0 open and secrecy rates. We simulate $T = 10^6$ blocks, run the rate control algorithm for different values of control parameters V and compare the performance of our algorithm with the opportunistic scheduling. From Fig. 2, one can see that, for appropriately chosen value of V, our algorithm outperforms opportunistic scheduling. Note that, opportunistic scheduling algorithm does not make use of any key queue, since the worse user always has zero open rate even its key queue has keys.

VI. Conclusion

We considered a degraded block-fading broadcast channel, in which we treat each user as an "internal eavesdropper" for the information transmitted to another user. We addressed the problem of maximizing the network utility, which is a function instantaneous rate of confidential information served for all users subject to decoding error and equivocation constraints. Toward solving the problem, we first specified the region of open and secrecy rates, achievable at each time slot. Then, we transformed the problem into a that of a joint rate allocation and secret key control. Then, we proposed a low-complexity and provably optimal algorithm that jointly selects the amount of information to be transmitted to all users from the region of achievable open and secrecy rates in each block. Unlike existing scheduling approaches that serve only the user with the positive secrecy rate in each block, our system uses part of the secrecy rate for key generation, to be utilized at later times in the form of a one-time pad. Our system leads to a smoother service process, which in turn increases the achieved long term utility, compared to the opportunistic scheduling approach.

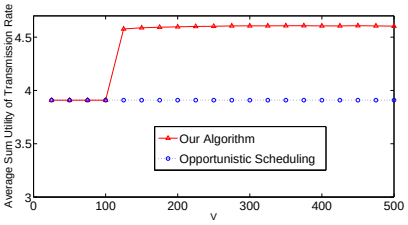

Fig. 2. Performance comparison of rate control algorithms of our algorithm and opportunistic scheduling

References

[1] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[2] A. Khisti and T. Liu, "Private Broadcasting over Independent Parallel Channels," 2012. [Online]. Available: http://arxiv.org/abs/1212.6930
[3] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure Broadcasting," 2007. [Online]. Available: http://arxiv.org/pdf/cs/0702093
[4] Y. Liang, H. V. Poor, and L. Ying, "Secure Communications over Wireless Broadcast Networks: Stability and Utility Maximization," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 682–692, September 2011.
[5] J. Xu, Y. Cao, and B. Chen, "Capacity Bounds for Broadcast Channels With Confidential Messages," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4529–4542, October 2009.
[6] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, June 2008.
[7] K. Khalil, M. Youssef, O. O. Koyluoglu, and H. El Gamal, "On the delay limited secrecy capacity of fading channels," in *ISIT*, Seoul, Korea, June - July 2009.
[8] Z. Mao, C. E. Koksal, and N. B. Shroff, "Achieving full secrecy rate with low packet delays: An optimal control approach," *IEEE Journal on Selected Areas of Communication*, vol. 31, no. 9, September 2013.
[9] O. Gungor, J. Tan, C. E. Koksal, H. El Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," 2013, to appear.
[10] C. E. Koksal, O. Ercetin, and Y. Sarikaya, "Control of Wireless Networks with Secrecy," *IEEE/ACM Transactions on Networking*, vol. 21, no. 1, pp. 324–337, February 2013.
[11] A. D. Wyner, "The Wire-Tap Channel," *The Bell System Technical Hournal*, vol. 54, no. 8, pp. 1355–1387, October 1975.
[12] Z. Mao, C. E. Koksal, and N. B. Shroff, "Fair rate allocation for broadcast channel with confidential messages," Tech. Rep., 2013. [Online]. Available: http://www.ece.osu.edu/˜maoz/CSPreport2013.pdf
[13] C. E. Shannon, "Communication Theory of Secrecy Systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, October 1949.