Scheduling in a Secure Wireless Network

Xuan Wang, Yi Chen, Lin Cai, Jianping Pan
University of Victoria, Victoria, BC, Canada

***Abstract*—We consider a scheduling problem in a wireless network which consists of one base station, N legitimate users and one (or more) eavesdropper(s). The scheduling problem jointly considers the reliability, security and stability of the system, and is to allocate wireless resources to the legitimate users, stabilize the system and maximize the secure transmission rate. Based on the stochastic network optimization framework, the scheduling problem is decomposed to an online optimization problem. A scheduling algorithm and a low computational complexity algorithm that both do not consider power adaptation are proposed, along with a power adaptive one. Extensive simulations are conducted to show the impact of the information arrival rate and the eavesdropper's channel condition on the system performance. These observations provide important insights and guidelines for the design and resource management of future wireless networks using secure communication technologies.**

I. Introduction

In a wireless network, there are several aspects that affect the system performance, such as capacity, reliability and security. Traditionally, security is a high-layer issue, and is designed independently of the network protocol. But this approach may have some potential drawbacks. For instance, an application-layer solution may require a higher computational complexity that may not be desirable for energy-limited devices such as smart phones. Recently, the physical-layer security became an attractive research area, since it can provide different kinds of security solutions in a wireless network, by exploring the physical-layer features such as channel conditions that are traditionally overlooked.

Physical-layer security in a wireless network is widely discussed from different aspects [1]. For instance, due to the unique randomness of the channel, the channel information can be used to generate a secret key in a wireless network, which is discussed in [2]–[4]. The uniqueness feature can also be used as the link signature for authentication as discussed in [5]–[7]. The spread spectrum communication has been revisited as a physical-layer security approach in [8], [9]. Cooperative jamming and artificial noise are used to improve the secrecy capacity region as discussed in [10], [11].

Although these designed security schemes utilize the uniqueness of the physical-layer information, most of them are designed from a traditional security viewpoint. In this paper, we adopt a more fundamental treatment towards the security issue, i.e., from the information-theoretical security viewpoint towards the confidentiality issue in a multiuser wireless network.

We study the scheduling problem in a wireless broadcast network, where one or more eavesdroppers exist in the system. The traditional approach tries to maximize the ergodic achievable rate of the system (see, e.g., [12], [13]), which captures the fundamental capacity limits under perfect secrecy, but may exhibit a large delay due to the inherent requirement of the coding scheme for the perfect secrecy over a fading channel. Differently, we consider an outage-based characterization that measures the probabilistic performance of the system, which is a coding-delay-limited metric that is of practical interests. Besides, we further consider the queue stability issue which is often ignored in the work that maximizes the ergodic achievable rate. Therefore, the scheduling problem is formulated as an optimization problem maximizing the system secure transmission rate (security issue) which is defined based on the secrecy outage and subject to the constraints that the queues in the system should be stable (stability issue) and the transmission rate is not exceeding the capacity region (reliability issue).

Little work has been done jointly considering these three aspects. Some works assume that the eavesdroppers' channel state information at symbol level (full instantaneous CSI) can be obtained by the BS, such as [18]–[20], which may not be practical. Some works, such as [21], relax the assumption on the instantaneous CSI, however, the designed scheme is not scalable to a case with multiple legitimate receivers, which limits the usage of the proposed algorithm. In our work, we design a scalable scheduling algorithm with a weak assumption that only the distribution of the CSI of the eavesdropper is known by the BS, which is more practical.

Based on the stochastic network optimization framework, the scheduling problem is decomposed to an online optimization problem which may be non-convex. Motivated by the Lagrangian dual method, a simple but effective scheduling algorithm is proposed, along with a low computational complexity one and a power adaptive one. Simulation results show that these three algorithms can achieve a similar secure transmission rate, but different secrecy outage and delay performance. Furthermore, with the increase of the traffic load, it can be observed that the secure transmission rate first increases and then decreases, and this observation suggests that admission control should be used in order to achieve a high-level secrecy.

The rest of this paper is organized as follows. The preliminaries about the physical-layer security and the related work are presented in Section II. Then, the system models, including queueing model, encoder model and channel model, are introduced along with the problem formulation in Section III. In Section IV, the formulated problem is approximately solved and three scheduling algorithms, including a simple algorithm, a low computational complexity one and a power adaptive one, are proposed. A case study that the eavesdropper's channel is a non-fading additive white Gaussian noise

978-1-4799-3360-0/14/$31.00 © 2014 IEEE

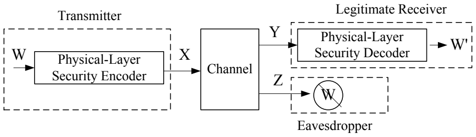
Transmitter
W
Physical-Layer Security Encoder
X
Channel
Y
Z
Legitimate Receiver
Physical-Layer Security Decoder
W'
W
Eavesdropper

Fig. 1. Wire-tap Channel

(AWGN) channel is also presented in Section IV, followed by the evaluation in Section V. We further consider how to extend the proposed algorithms to the multi-eavesdropper case in Section VI, followed by the conclusions and future work in Section VII.

II. Preliminaries and Related Work

A. Physical-Layer Security

Security is an important issue in communications, which typically include confidentiality, integrity, authentication, and nonrepudiation. The confidentiality guarantees the legitimate receivers can obtain the information, while eavesdroppers are unable to understand the information. Traditionally, confidentiality is achieved by cryptographic techniques, which are based on the computational complexity theory and key distribution technique. While for a wireless network, due to the broadcast nature of the wireless medium, the secret key distribution becomes a difficult problem [14]. The information-theoretical security, one branch of the physical-layer security, which aims to provide an alternative solution to the confidentiality, treats the secrecy communication from an information entropy point of view.

Typically, the eavesdropping in a wireless network can be captured by a wire-tap channel as shown in Fig. 1. The transmitter has a message W intended to transmit to a legitimate receiver, through a channel. The message W is mapped to the codeword X by a physical-layer security encoder, which jointly considers the security and reliability. Then X is transmitted to the receiver through a wireless channel. Due to the broadcast nature of the channel, both the legitimate receiver and the eavesdropper can observe the corrupted messages, Y and Z. The decoder in the legitimate receiver maps the received Y to an estimated message W'. The purpose of the encoder and decoder is to make sure the estimated message is the same as the original one, i.e., $W' = W$, and the corrupted message Z received by the eavesdropper contains no information about W.

In a more practical scenario, if the channel is an AWGN channel, i.e., X is corrupted by an additive white Gaussian noise, the secrecy capacity of such system is [15]

$$[C_{X\to Y} - C_{X\to Z}]^+,$$

where $C_{X\to Y}$ and $C_{X\to Z}$ are the capacity of the channel $X \to Y$ and $X \to Z$, respectively.

This result suggests that a perfect secrecy can be achieved if the entropy of the original message W is no larger than the secrecy capacity, i.e., $H(W) \leq [C_{X\to Y} - C_{X\to Z}]^+$. Otherwise, part of W can be decoded from Z, and the system experiences a secrecy outage event. Therefore, for each channel usage, the secrecy outage probability is defined as

$$P^{\text{out}} = Pr\{C_{X\to Z} > C_{X\to Y} - H(W)\},$$

since the capacity of the eavesdropper's channel $C_{X\to Z}$ is generally unknown, and can be modeled as a random variable. Further note that, $C_{X\to Z}$ is also related with $C_{X\to Y}$, since both channels have the same transmitter (therefore the same transmission power, frequency bandwidth and time portion of the resource). The secrecy outage probability is also determined by $H(W)$, which means P^{out} can be improved by adjusting how much information to be sent in each channel usage.

B. Related Work

The scheduling and resource allocation in a secure wireless communication system is widely discussed in the literature. However, most of the works are discussed from a traditional information-theoretical perspective, i.e., quantifying the capacity region under different network settings. All these works try to solve an optimization problem, implicitly or explicitly, based on the assumption that the system is saturated and each user in the system always has data to transmit. For instance, the secrecy capacity region of a wire-tap channel is discussed in [16]; that of a Gaussian wire-tap channel in [15]; that of a fading channel in [12]; that of a fading broadcast channel in [13]; that of a MIMO broadcast channel in [17]. All these works only consider the reliability and security issue in communications, and ignore the stability issue which is typically treated in the higher layer. However, the stability is of equal importance with reliability and security, since it further determines whether a practical system can work properly and desirably over a sufficiently long time period.

There is little work jointly considering these three aspects. In [18], authors studied how to transmit confidential messages to users in a fast-fading broadcast wireless network, subject to three constraints: reliability constraint that the message can be perfectly decoded, security constraint that the message is perfectly secured and stability constraint that the system is queue-length stable. An achievable secrecy rate region is obtained and a max-weight type of scheduling algorithm along with the optimal power control policy is designed so that to satisfy these three requirements. In [19], a secure communication system is designed to achieve a constant transmission rate. In this design, the developed scheme sends the key with the data when the system is perfectly secured, and uses the key to protect the data when the system is subject to a secrecy outage. A power control scheme is also designed to maximize the transmission rate. A work similar to [19] was reported in [20] where a different objective is used. All the above works share the same system assumption that the instantaneous CSI of the eavesdropper should be known by BS, which may not be practical.

In [21], the power allocation problem of a secure wireless communication system in the presence of statistical queueing constraints is studied. The effective secure throughput region

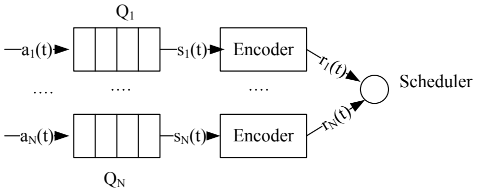

Fig. 2. System Block Diagram

is obtained through an effective capacity method, and a power allocation scheme that achieves such a region is obtained. The obtained scheme implicitly considers the stability issue of the system, since a queue constraint is employed. However, the authors only consider the single legitimate receiver, and the designed scheme is not scalable to a multi-legitimate-receiver case, which limits the usage of the proposed algorithm.

III. System Models and Problem Formulation

A. System Models

We first consider the downlink of a wireless network, with one base station (BS), N independent legitimate receivers and one eavesdropper. The multiple eavesdropper case will be discussed in Sec. VI. There are confidential data that arrive at the BS and need to be transmitted to the legitimate receivers through a shared wireless fading channel. In order to protect the data against the eavesdropper, the data have been encoded using the physical-layer security technology before transmission. We are interested in how to provide a best-effort security solution, since the secrecy outage may always happen. Therefore, the system is required to achieve reliability and stability first, and then security. The system is a time-slotted one, and w.l.o.g., we assume the slot length is 1 second. The system model is shown in Fig. 2.

1) Queueing Model: We assume that the data packets arrive at the end of each time slot and are queued up in an infinite virtual buffer reserved for each legitimate user. The amount of the data arriving in time slot t for user i is $a_i(t)$ and is a random variable with finite moments. Assuming the amount of the data of user i being transmitted to the physical-layer security encoder is $s_i(t)$, then, the queue dynamic is as follows

$$Q_i(t+1) = \max(Q_i(t) - s_i(t), 0) + a_i(t),$$

where $Q_i(t)$ is the amount of the data buffered in the queue i in time slot t.

2) Physical-Layer Security Encoder: The encoder uses Wyner's encoding scheme [16] to encode the input data $s_i(t)$, and the output data rate is $r_i(t)$, which should be equal to the channel rate that is allocated to user i in time slot t. The output rate should be no less than the input rate, i.e., $r_i(t) \geq s_i(t)$, and the difference $r_i(t) - s_i(t)$ quantifies the ability to secure against the eavesdropper.

3) Channel Model: The output data from the physical-layer security encoder have been directly sent through a wireless channel. For any time slot t, the received signals by legitimate receiver i, denoted by $y_i(t)$ and by eavesdropper, denoted by $y_e(t)$, are given by, respectively

$$y_i(t) = g_i(t)x_i(t) + w_i(t),$$
$$y_e(t) = g_e(t)x_i(t) + w_e(t),$$

where $g_i(t)$ and $g_e(i)$ are the complex fading coefficients from the BS to the legitimate receiver i and the eavesdropper, respectively. $w_i(t)$ and $w_e(t)$ represent the independent and identically distributed (i.i.d.) additive Gaussian noise with unit variance at the legitimate receiver i and the eavesdropper, respectively. Therefore, the channel gains from the BS to the legitimate receiver i and eavesdropper are $\gamma_i(t) = |g_i(t)|^2$ and $\gamma_e(t) = |g_e(t)|^2$, respectively.

Furthermore, we assume the channel of each user is independent and each channel experiences a block fading, i.e., the channel gain remains constant during each time slot and changes independently across time slots. The fading process is assumed to be ergodic and the distribution is bounded. The duration of each time slot is long enough and Wyner's encoding scheme can be performed within each time slot.

The BS can obtain the instantaneous CSI of the legitimate receivers in each time slot, but can only know the distribution of the channel fading between the BS and the eavesdropper.

Assume the system uses an orthogonal MAC, i.e., the physical-layer resource can only be orthogonally allocated to each user, such as TDMA. We further assume that each time slot can be further divided and allocated to different users. Therefore, the rate allocated to user i in time slot t is represented as

$$r_i(t) = \tau_i(t) \log(1 + p(t)\gamma_i(t)),$$

where $\tau_i(t)$ is the time portion allocated to user i in time slot t, and $p(t)$ is the allocated power in time slot t. The system is either subject to a peak power constraint, i.e., $p(t) \leq P$, or subject to an average power constraint, i.e., $\lim_{T\to\infty} \frac{1}{T}\sum_{t=1}^{T} p(t) \leq P$.

B. Problem Formulation

In each time slot, the scheduler decides which user can transmit its data. More specifically, it determines how much data ($s_i(t)$) should been fetched from the queue, and sent to the encoder, and determines how to protect the data by choosing an appropriate output rate of the encoder ($r_i(t)$). Meanwhile, the system should be stabilized if possible, i.e., queues in the system should be stable and the average queue length over time is bounded.

The choice of $s_i(t)$ and $r_i(t)$ depends on the objective of the scheduler, and the physical-layer constraints. In order to achieve a reliable communication between legitimate users and BS, according to Shannon's Theorem, the rates allocated in each time slot ($\mathbf{r}(t)$) should not lie outside the capacity region, which is equivalent to $\sum_i \tau_i(t) \leq 1$.

In order to achieve a high level of secrecy, we need to maximize the average secure transmission rate of the system. The secure transmission rate of user i in time slot t is defined as: $R_i^s(t) = s_i(t)(1 - P_i^{\text{out}}(t)) = s_i(t)Pr\{C^e(t) \leq$

$r_i(t) - s_i(t)\}$. If user i uses time portion $\tau_i(t)$ and power $p(t)$, then $C^e(t) = \tau_i(t)\log(1 + p(t)\gamma_e(t))$, and we have

$$R_i^s(t) = s_i(t)F(\frac{(1 + p(t)\gamma_i(t))2^{-\frac{s_i(t)}{\tau_i(t)}} - 1}{p(t)}), \tag{1}$$

where F is the cumulative distribution function (CDF) of γ_e.

The average secure transmission rate of the system in slot t is defined as $R^s(t) = \sum_{i=1}^N R_i^s(t)$, which is used to quantify how many data can be received without secrecy outage in the system, and is a coding-delay-limited rate that is of practical interests.

Therefore, the scheduling problem can be formulated as:

$$\begin{aligned}
\max \quad & \lim_{T\to\infty} \tfrac{1}{T}\sum_{t=1}^T R^s(t) && \text{(2a)}\\
s.t. \quad & \forall i,\ Q_i \text{ is stable}, && \text{(2b)}\\
& \forall i,\ s_i(t) \le \min(\tau_i(t)\log(1 + p(t)\gamma_i(t)), Q_i(t)), && \text{(2c)}\\
& \textstyle\sum_i \tau_i(t) \le 1, && \text{(2d)}\\
& p(t) \le P, && \text{(2e)}
\end{aligned}$$

if the system is subject to a peak power constraint; and formulated as

$$\begin{aligned}
\max \quad & \lim_{T\to\infty} \tfrac{1}{T}\sum_{t=1}^T R^s(t)\\
s.t. \quad & \forall i,\ Q_i \text{ is stable},\\
& \forall i,\ s_i(t) \le \min(\tau_i(t)\log(1 + p(t)\gamma_i(t)), Q_i(t)),\\
& \textstyle\sum_i \tau_i(t) \le 1,\\
& \lim_{T\to\infty} \tfrac{1}{T}\sum_{t=1}^T p(t) \le P,
\end{aligned}$$

if the system is subject to an average power constraint.

IV. Scheduling Algorithm Design

A. Scheduling Under the Peak Power Constraint

First, we can observe that the optimum is obtained only if $p^* = P$. This is because the CDF function F is a monotonically increasing function, and

$$\begin{aligned}
& ((1 + p(t)\gamma_i(t))2^{-s_i(t)/\tau_i(t)} - 1)/p(t)\\
= \quad & (2^{-s_i(t)/\tau_i(t)} - 1)/p(t) + \gamma_i(t)2^{-s_i(t)/\tau_i(t)}
\end{aligned}$$

is a monotonically increasing function of $p(t)$ since $2^{-s_i(t)/\tau_i(t)} - 1$ is always negative. Therefore $R_i^s(t)$ is maximized when $p(t)$ is maximized.

According to the stochastic network optimization theory [22], in order to stabilize the system, we can minimize the Quadratic-Lyapunov-drift bound. If the drift bound satisfies certain conditions, then with the drift-bound-minimizing method, the system is stable.

Define the quadratic Lyapunov function of the system as

$$L(\mathbf{Q}(t)) = \frac{1}{2}\sum_i Q_i(t)^2,$$

then the one-slot conditional Lyapunov drift is

$$\Delta(\mathbf{Q}(t)) = \mathbb{E}[L(\mathbf{Q}(t + 1)) - L(\mathbf{Q}(t))|\mathbf{Q}(t)].$$

After calculation, we have

$$\begin{aligned}
\Delta(\mathbf{Q}(t)) \le \quad & \mathbb{E}[\textstyle\sum_i \frac{a_i(t)^2 + s_i(t)^2}{2} +\\
& Q_i(t)(a_i(t) - s_i(t))|\mathbf{Q}(t)].
\end{aligned}$$

If the RHS of the above inequation is minimized, we have

$$\Delta(\mathbf{Q}(t)) \le \quad B - \epsilon \textstyle\sum_i Q_i(t),$$

where $\epsilon \ge 0$ is a constant and B is a constant that satisfies

$$B > \mathbb{E}[\sum_i \frac{a_i(t)^2 + s_i(t)^2}{2}|Q_i(t)].$$

Then, based on Theorem 4.1 in [22], the system is stable.

By treating the refined problem as a multi-objective problem and using the penalty method, problem (2) is solved by solving the following online problem in each time slot

$$\begin{aligned}
\max \quad & \textstyle\sum_i Q_i s_i + V s_i F(\frac{(1+P\gamma_i)2^{-\frac{s_i}{\tau_i}} - 1}{P}) && \text{(3a)}\\
s.t. \quad & \forall i, s_i \le \min(\tau_i \log(1 + P\gamma_i), Q_i), && \text{(3b)}\\
& \textstyle\sum_i \tau_i \le 1, && \text{(3c)}
\end{aligned}$$

where V is a weight assigned to the secure transmission rate, which is used to show the importance of such an objective. For presentation simplicity, the time slot index t is omitted.

Based on Theorem 4.2 in [22], the performance of the penalty method can be guaranteed, and furthermore we have

$$\begin{aligned}
\lim_{T\to\infty} \frac{1}{T}\sum_{t=1}^T \mathbb{E}[R^s(t)] \quad & \le \quad \textbf{Opt} + \frac{B}{V},\\
\lim_{T\to\infty} \frac{1}{T}\sum_{t=1}^T \sum_i \mathbb{E}[Q_i(t)] \quad & \le \quad \frac{B + VR}{\epsilon},
\end{aligned}$$

where **Opt** is the optimum of problem (2) and $R = \mathbb{E}[\max_i \log(1 + P\gamma_i)]$ is bounded.

Generally the problem in (3) is difficult to solve, because the nice decomposable structure is destroyed by the constraint $s_i \le Q_i$. Without such a constraint, a primal decomposition can be used to simplify the problem. Therefore, we use a Lagrangian duality method to take account of the constraints $s_i \le Q_i$ by augmenting the original objective function with a weighted sum of the constraint functions $s_i \le Q_i$. The partial Lagrangian function of the problem is given by

$$\begin{aligned}
L(\mathbf{s}, \boldsymbol{\tau}; \boldsymbol{\lambda}) = \quad & \textstyle\sum_i Q_i s_i + V s_i F(\frac{(1+P\gamma_i)2^{-\frac{s_i}{\tau_i}} - 1}{P})\\
& +\lambda_i(Q_i - s_i),
\end{aligned}$$

the dual function is

$$g(\boldsymbol{\lambda}) = \max_{\mathbf{s},\boldsymbol{\tau}} L(\mathbf{s}, \boldsymbol{\tau}; \boldsymbol{\lambda}), \tag{4}$$

and the dual problem is

$$\begin{aligned}
\min \quad & g(\boldsymbol{\lambda}) && \text{(5a)}\\
s.t. \quad & \lambda_i \ge 0. && \text{(5b)}
\end{aligned}$$

If the primal problem (3) is convex, then the duality gap is zero. The maximum value of the primal problem (3) is identical to the minimum value of the dual problem (5). If the primal problem is nonconvex, then the dual problem provides an upper bound, which is not always tight, for the primal solution.

Note that the dual problem is always convex w.r.t. $\boldsymbol{\lambda}$ regardless of the primal problem. Therefore the dual problem can be directly solved by dual update methods, such as the gradient descent method. Hence, $\boldsymbol{\lambda}$ is updated based on

$$\lambda_i^{(l+1)} = \max(0, \lambda_i^{(l)} - s^{(l)}(Q_i - s_i^{(l)})),$$

where $s^{(l)}$ is a step sequence and square summable [23], and $s_i^{(l)}$ is the solution of step l, and is solved from (4).

For (4), it is equivalent to

$$\begin{aligned} g(\boldsymbol{\lambda}) = \max \quad & \textstyle\sum_i (Q_i - \lambda_i)s_i + \\ & V s_i F(\tfrac{(1+P\gamma_i)2^{-\frac{s_i}{\tau_i}}-1}{P}) + \lambda_i Q_i \\ s.t. \quad & \forall i, s_i \le \tau_i \log(1+P\gamma_i), \\ & \textstyle\sum_i \tau_i \le 1. \end{aligned}$$

Define $k_i = s_i/\tau_i$, then the problem can be reformulated as

$$\begin{aligned} g(\boldsymbol{\lambda}) = \max \quad & \textstyle\sum_i \tau_i U_i + \lambda_i Q_i \\ s.t. \quad & \textstyle\sum_i \tau_i \le 1, \end{aligned}$$

where

$$U_i = \max \quad (Q_i - \lambda_i)k_i + V k_i F(\tfrac{(1+P\gamma_i)2^{-k_i}-1}{P}) \quad \text{(6a)}$$
$$s.t. \quad k_i \le \log(1+P\gamma_i). \quad \text{(6b)}$$

The above problem, which is the dual problem, can be solved by allocating all the time portion to the user i^* who has the maximal U_i, i.e., $\tau_{i^*} = 1$, where $i^* = \arg\max_i U_i$. U_i is obtained by solving (6), which might not be a convex problem, since the convexity depends on function F and is generally unknown. But since (6) is a one-dimensional problem in a closed set, the optimum solution can be obtained straightforwardly by comparing the points with zero derivative and the boundary points, or solved by line search algorithms [23], therefore effectively solved.

Note that, for the dual problem, the solution is to allocate all the resource to only one user. Although the solution might not be optimal to the primal problem, the approach motivates us to design a simple algorithm that schedules only one user in each time slot. If only one user can be scheduled, then (3) is solved by finding the user with the maximal U_i^{app}, where

$$U_i^{\text{app}} = \max \quad Q_i k_i + V k_i F(\tfrac{(1+P\gamma_i)2^{-k_i}-1}{P}) \quad \text{(7a)}$$
$$s.t. \quad k_i \le \min(\log(1+P\gamma_i), Q_i). \quad \text{(7b)}$$

The above algorithm, which is called SIMPLE algorithm, is of low computational complexity comparing with the Lagrangian dual algorithm, since we do not need to update λ iteratively to find the user has the maximal utility in each iteration, which saves a lot of computation. If the computational complexity to solve (7) is $O(C)$, then the computational complexity of SIMPLE algorithm is $O(NC)$.

Low Computational Complexity Algorithm: For the SIMPLE algorithm, it requires solving N nonlinear and possible nonconvex optimization problems in each time slot, which is a burden for the scheduler. In order to further reduce the computational complexity, we can separate the user selection and resource allocation.

If we replace the objective of (2) by a constant value, then the resultant algorithm is a feasible solution and all the requirements of (2) can be satisfied. More specifically, an online feasible algorithm can be obtained by replacing V to 0 in the SIMPLE algorithm, and is stated as follows

$$i^* = \arg\max_i Q_i \min(\log(1+P\gamma_i), Q_i).$$

The above algorithm essentially is a user selection algorithm. In order to maximize the secure transmission rate of the system, we need to fetch a proper amount of the data from the queue of the selected user i^*, based on (7).

The above low computational complexity algorithm, which is called LOW hereinafter, can also guarantee the stability of the system, although after the user selection it reallocates the resource in order to maximize the secure transmission rate. This is because the term $V k_i F(\frac{(1+P\gamma_i)2^{-k_i}-1}{P})$ is upper-bounded and negligible when Q_i is sufficiently large. Therefore, when the system is about to be unstable (Q_i becomes unbounded), the scheduling algorithm degrades to the max-weight algorithm, which is throughput-optimal and can prevent the system from becoming unstable.

Since the selected user may not be the one with the maximal utility, the performance of LOW should be worse than SIMPLE, which is the cost of the low computational complexity feature, as the computational complexity of LOW is $O(C)$, which is N times smaller than that of SIMPLE.

Eavesdropper with AWGN channel: If the channel of eavesdropper is an AWGN channel without fading, the secure transmission rate of user i in time slot t becomes

$$\begin{aligned} R_i^s(t) &= s_i(t)\delta(r_i(t) - s_i(t) - C^e(t)), \\ &= s_i(t)\delta(\log(\frac{1+p(t)\gamma_i(t)}{1+p(t)\gamma_e(t)}) - \frac{s_i(t)}{\tau_i(t)}) \end{aligned}$$

where $\delta(x)$ is an indicator function. $\delta(x) = 1$ if $x \ge 0$ and $\delta(x) = 0$ if otherwise.

By replacing the F function in (1) with $\delta(x)$, we can have the scheduling algorithm for the AWGN channel case. Due to the simplicity of $\delta(x)$, the solution for such a special case can be obtained easily, and the problem can be solved more efficiently. The resultant scheduling algorithm is similar to the classic max-weight scheduling.

We need to solve the following problem in each time slot,

$$\begin{aligned} U_i = \max \quad & Q_i k_i + V k_i \delta(\log(\tfrac{1+P\gamma_i}{1+P\gamma_e}) - k_i) \\ s.t. \quad & k_i \le \min(\log(1+P\gamma_i), Q_i). \end{aligned}$$

and find the user with maximal U_i. After some manipulations, we have

$$\begin{aligned} U_i = \max(&(Q_i + V)\min(\log(\frac{1+P\gamma_i}{1+P\gamma_e}), Q_i), \\ & Q_i \min(\log(1+P\gamma_i), Q_i)), \end{aligned}$$

and for the selected user i^*,

$$k_{i^*}^* = \begin{cases} \min(\log(\frac{1+P\gamma_{i^*}}{1+P\gamma_e}), Q_{i^*}) & \gamma_{i^*} > \frac{(1+P\gamma_e)^{1+\frac{Q_{i^*}}{V}}-1}{P} \\ \min(\log(1+P\gamma_{i^*}), Q_{i^*}) & \text{otherwise.} \end{cases}$$

Note that if $k_{i^*}^* = \log(1+P\gamma_{i^*})$, the data are not protected by the physical-layer security encoder, and a user with a channel better than the eavesdropper's one may also not be fully protected. This is because the secure transmission rate can be achieved by such a user is too marginal, and the resource should be used by other users that can achieve a higher secure transmission rate.

B. Scheduling Under the Average Power Constraint

Since $p(t)$ is controllable in each time slot, we can define a virtual queue $Z(t)$ to capture the dynamic feature of $p(t)$, i.e., $Z(t+1) = \max(Z(t) + p(t) - P, 0)$. Therefore, we have

$$Z(T) - Z(0) \geq -PT + \sum_{t=0}^{T-1} p(t),$$

which is equivalent to

$$\lim_{T\to\infty} \frac{\mathbb{E}[Z(T)]}{T} - \frac{\mathbb{E}[Z(0)]}{T} \geq -P + \lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} p(t).$$

Then the sufficient condition of the average power constraint is that the virtual queue $Z(t)$ is stable [22].

Now there are $N+1$ queues in the system that need to be stabilized: one is the virtual queue $Z(t)$, and the others are the real queue $Q_i(t)$. By defining a Lyapunov function as a quadratic-sum function, i.e., $\frac{1}{2}(\sum Q_i(t)^2 + Z(t)^2)$, we can find that minimizing the one-slot Lyapunov drift is equivalent to maximizing $-p^2/2 - Zp + \sum_i Q_i s_i$. Then, based on the penalty method, in each time slot, we need to solve

$$\begin{aligned} \max \quad & -p^2/2 - Zp + \textstyle\sum_i Q_i s_i + VR_i^s \\ s.t. \quad & \forall i, s_i \leq \min(\tau_i \log(1+p\gamma_i), Q_i), \\ & \textstyle\sum_i \tau_i \leq 1. \end{aligned}$$

According to the same argument as the peak power constraint case, we find the above problem can be approximately solved by allocating all the time portion to the user with the maximal $U_i^{'}$ ($\tau_i = 1$), where

$$\begin{aligned} U_i^{'} = \max \quad & -p^2/2 - Zp + Q_i k_i + Vk_i F(\tfrac{(1+p\gamma_i)2^{-k_i}-1}{p}) \\ s.t. \quad & k_i \leq \min(\log(1+p\gamma_i), Q_i), \end{aligned}$$

whose convexity also depends on F.

Although the above problem may be non-convex, since it is a two-dimensional problem, the interior-point method can be used to solve it in an efficient way. The above algorithm will be refer to as SIMPLE-P hereinafter. Note that, comparing to the SIMPLE algorithm, the computational complexity of SIMPLE-P is higher, as a two-dimensional possible non-convex problem should be solved, which is the cost of power adaptation.

Eavesdropper with AWGN channel: Similar to the peak power constraint case, we need to solve the following problem for each i

$$\begin{aligned} U_i^{'} = \max \quad & -p^2/2 - Zp + Q_i k_i + Vk_i\delta(\log(\tfrac{1+p\gamma_i}{1+p\gamma_e}) - k_i) \\ s.t. \quad & k_i \leq \min(\log(1+p\gamma_i), Q_i). \end{aligned}$$

and find the user with the maximal $U_i^{'}$.

Equivalently, we need to solve the following two problems to determine $U_i^{'}$,

$$\begin{aligned} U_i^{'} = \max \quad & -p^2/2 - Zp + Q_i k_i \\ s.t. \quad & k_i \leq \min(\log(1+p\gamma_i), Q_i), \\ & k_i > \log(1+p\gamma_i) - \log(1+p\gamma_e), \end{aligned}$$

and

$$\begin{aligned} U_i^{'} = \max \quad & -p^2/2 - Zp + Q_i k_i + Vk_i \\ s.t. \quad & k_i \leq \min(\log(1+p\gamma_i), Q_i), \\ & k_i \leq \log(1+p\gamma_i) - \log(1+p\gamma_e). \end{aligned}$$

The above two problems are convex optimization problems, and therefore they can be effectively solved.

V. Evaluation and Discussion

A. Simulation Setting

In the simulation, we consider a system that contains two legitimate receivers and one eavesdropper. Although the number of legitimate receivers is limited to two, it is sufficient to quantify the performance of the proposed algorithms and investigate the relationship between the system performance and different network configurations. The channel gains of the receivers and the eavesdropper are modeled as Nakagami fadings. So, γ_i and γ_e are Gamma distributed random variables. The probability density function of γ_i is

$$f(x) = (\frac{m_i}{P_i^r})^{m_i} \frac{x^{m_i-1}}{\Gamma(m_i)} \exp(-\frac{m_i x}{P_i^r}), \quad (m_i \geq 0.5),$$

and the CDF of γ_i is

$$F(x) = \frac{\int_0^{m_i x/P_i^r} t^{m_i-1} e^{-t} dt}{\Gamma(m_i)}, \quad (m_i \geq 0.5),$$

where m_i is the fading parameter of user i, P_i^r is the average received power in the Nakagami fading of user i, which is used to model the large-scale path loss and shadowing effect. Since we assume the noise power is one, P_i^r is the average Signal-to-Noise-Ratio (SNR) of user i. Note that, m_i is used to control the variability of γ_i, and a small m_i results in a large variation of γ_i. When $m_i = 1$, the Nakagami fading becomes a Rayleigh fading. When $m_i \to \infty, \gamma_i = P_i^r$, the channel becomes an AWGN channel.

The amount of traffic arrival in each time slot $a_i(t)$ is exponentially distributed (the distribution has no essential impact on the system performance), the power constraint is $P = 1$, and the system frequency bandwidth is normalized to 1. So the units of the secure transmission rate and the arrival rate are both bps/Hz and are omitted hereinafter. We choose the parameter V as 100. During the simulation, we find that 3,000 time slots are long enough for the system to converge to its steady state. Therefore, we run 5,000 time slots, and collect the results from the last 2,000 ones. For each simulation setting, we repeat ten times and take the average. Other parameters used for different network configurations are listed in the caption of each figure.

B. The Impact of the Arrival Rate

We fix the arrival rate of user 1 ($\lambda_1 = 0.5$), increase the arrival rate of user 2 (λ_2) from 0.1 to 1.5, and the results are shown in Fig. 3, Fig. 4 and Fig. 5.

In Fig. 3, when $\lambda_2 < 1$, with the increase of λ_2, the secure transmission rate also increases, approximately in a linear function w.r.t. λ_2. It means when the traffic load of the system is small, there is enough room for the physical-layer encoder to protect the data from the eavesdropping. This can be seen from Fig. 4. When $\lambda_2 < 1$, the secrecy outage probability only has a small change w.r.t. λ_2. With the further increase of λ_2, the secure transmission rate starts to decrease, which means in the large traffic load case, the system has a severe secrecy outage, which can be observed in Fig. 4, where the secrecy outage probability increases linearly w.r.t. λ_2. Further note that the secrecy outage probability first decreases and then increases along with the increase of λ_2. This is because when λ_2 is small, the traffic in the system is dominated by user 1's, which suggests user 1 has more impact on the secrecy outage probability. With the increase of λ_2, the secrecy outage of user 2 dominants the system secrecy outage. Since user 2 has a better channel, the secrecy outage probability decreases. With the further increase of λ_2, more and more data cannot be protected due to the resource shortage, and therefore the secrecy outage probability increases.

Considering the secure transmission rate, different algorithms result in a similar performance. This is because all the proposed algorithms try to maximize the secure transmission rate, despite the simplification and approximation. SIMPLE-P is slightly better than SIMPLE, since it can adapt the power to the channel efficiently to improve the system performance; SIMPLE is slightly better than LOW, since in each time slot, the decision made by SIMPLE is no worse than LOW. While for the secrecy outage probability, although when $\lambda_2 > 1$ all three algorithms have an almost identical performance, the performance of LOW is significantly worse than the others when λ_2 is small.

The average queue length in the system is investigated in Fig. 5. The queue length is an indicator to show the delay performance and a large queue length means a large delay. With the increase of λ_2, the queue length increases exponentially in all three algorithms, which is consistent with queueing theory. When λ_2 is small, the LOW algorithm exhibits the lowest queue length, i.e., the best delay performance. This is because, comparing with the other two algorithms, LOW behaves more like a traditional max-weight scheduling algorithm that does not need to make a tradeoff between the delay performance and the secure transmission rate. The delay performance of SIMPLE is worse than SIMPLE-P, since it cannot utilize the power-adaptation to improve the delay performance. While when λ_2 is large, all the three algorithms have an almost identical delay performance, which is because the scheduling algorithms are more emphasizing on the stability requirement, and all behave as the traditional max-weight scheduling algorithm.

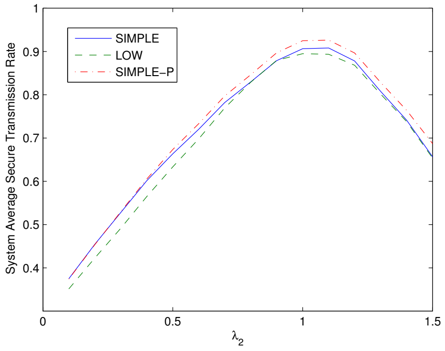

Fig. 3. The impact of the arrival rate: secure transmission rate. $P_e^r = 1, P_1^r = 2, P_2^r = 5, \lambda_1 = 0.5, m_1 = m_2 = m_e = 1$.

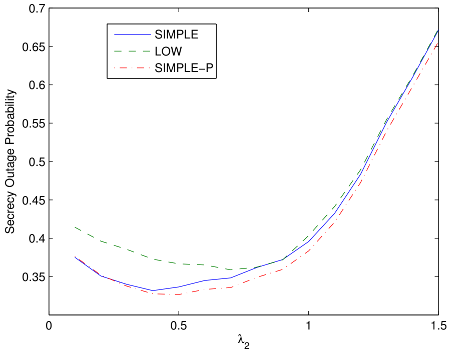

Fig. 4. The impact of the arrival rate: secrecy outage probability. $P_e^r = 1, P_1^r = 2, P_2^r = 5, \lambda_1 = 0.5, m_1 = m_2 = m_e = 1$.

In summary, when the traffic load of the system is high, the performance of SIMPLE and LOW are almost identical, while LOW has a low computational complexity. When the traffic load of the system is small, LOW exhibits a small queueing delay but with a large secrecy outage. As SIMPLE-P can adapt the power to the variation of the channel, the performance is always no worse than that of SIMPLE, however with a higher computational complexity.

C. The Impact of the Eavesdropper's Channel

We change the eavesdropper's channel to investigate the impact on the system performance, and the results are shown in Fig. 6, Fig. 7 and Fig. 8.

From Fig. 6, with the increase of the average SNR of the eavesdropper's channel (P_e^r), the secure transmission rate decreases. This is because the system experiences a frequent secrecy outage as the eavesdropper's channel becomes better, which can be seen from Fig. 7.

Comparing different arrival rates (λ_2), the increase of P_e^r has a severe impact on the secure transmission rate when λ_2 is

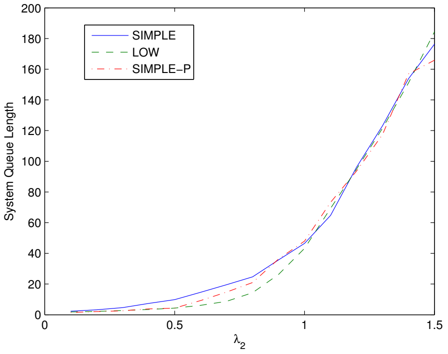

Fig. 5. The impact of the arrival rate: queue length. $P_e^r = 1, P_1^r = 2, P_2^r = 5, \lambda_1 = 0.5, m_1 = m_2 = m_e = 1$.

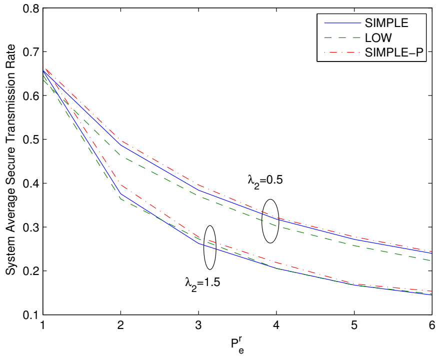

Fig. 6. Secure transmission rate, eavesdropper with fading channel. $P_1^r = 2, P_2^r = 5, \lambda_1 = 0.5, m_1 = m_2 = m_e = 1$.

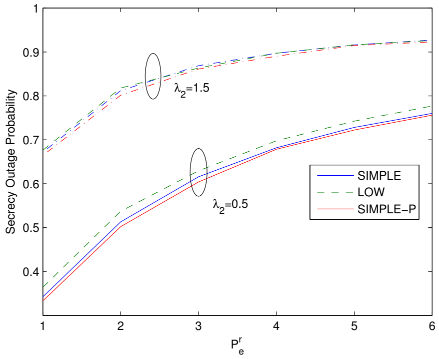

Fig. 7. Secrecy outage probability, eavesdropper with fading channel. $P_1^r = 2, P_2^r = 5, \lambda_1 = 0.5, m_1 = m_2 = m_e = 1$.

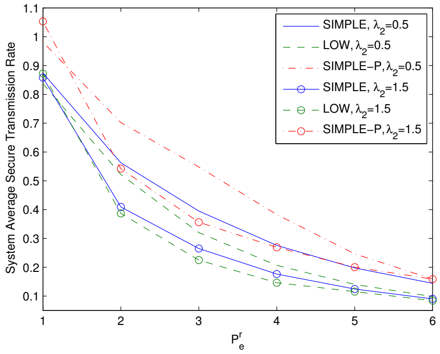

Fig. 8. Secure transmission rate, eavesdropper with AWGN channel. $P_1^r = 2, P_2^r = 5, \lambda_1 = 0.5, m_1 = m_2 = 1$.

large. A large λ_2 means the available resource that can be used to protect the data from eavesdropping is small, since more resources are used to achieve the reliable communication. While with the increase of P_e^r, the ability of the eavesdropper to decode the message becomes stronger, i.e., the secrecy outage happens more frequently. Therefore a system with a large arrival rate is more sensitive to P_e^r.

With different P_e^r, different algorithms can achieve a comparable secure transmission rate, and the performance gap is almost less than 2%. Similar observations can be found in the secrecy outage probability from Fig. 7. The change of P_e^r has almost no impact on the performance gap for both secure transmission rate and secrecy outage probability.

When the eavesdropper experiences an AGWN channel, the secure transmission rate is illustrated in Fig. 8. All the trends observed in Fig. 6 can be seen in Fig. 8, which suggests the observations in Fig. 6 are not related to the fading variability. However, different algorithms perform differently. The performance of the two algorithms that do not consider power adaptation are similar, and both are worse than the power adaptive one, SIMPLE-P, in spite of λ_2. This is because with the AWGN channel, the secrecy outage probability is a step function, and the power allocation has a great impact on the secrecy outage probability, which is illustrated in Fig. 9, and therefore has a further impact on the secure transmission rate.

Comparing Fig. 8 with Fig. 6, when P_e^r is small, a small fading variability results in a better performance; when P_e^r is large, a large fading variability results in a better performance; This is because when P_e^r is small, a large fading variability increases the chance of secrecy outage, since the ability of the eavesdropper to decode the message is weak. When P_e^r is large, the ability of the eavesdropper to decode the message becomes strong and therefore a large fading variability benefits the secure transmission. By comparing Fig. 7 with Fig. 9, the above reasoning can be confirmed from the secrecy outage point of view.

VI. Further Discussion: Multiple Eavesdroppers

Considering a system with multiple eavesdroppers, the message is secured if and only if none of the eavesdroppers can decode the message. Therefore, the secure transmission rate of user i in time slot t is

$$R_i^s(t) = s_i(t) \prod_j Pr\{C_j^e(t) \leq r_i(t) - s_i(t)\} = s_i(t)G, \quad (8)$$

where

$$G = \prod_j F_j\left(\frac{(1 + p(t)\gamma_i(t)2^{-\frac{s_i(t)}{r_i(t)}} - 1}{p(t)}\right),$$

and F_j is the CDF of the channel gain of eavesdropper j.

Comparing (8) to (1), the only difference between the multi-eavesdropper case and the single-eavesdropper case is the slight different objective function. Therefore by replacing

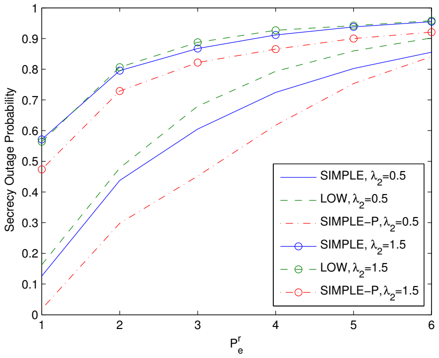

Fig. 9. Secrecy outage probability, eavesdropper with AWGN channel. $P_1^r = 2, P_2^r = 5, \lambda_1 = 0.5, m_1 = m_2 = 1$.

function F in the single eavesdropper case with function G, we can obtain the solution for the multi-eavesdropper case.

By observing (8) we can conclude that the secure transmission rate of a system with multiple eavesdroppers is no larger than that with a single eavesdropper, and generally with the increase of the number of eavesdroppers in the system, the secure transmission rate decreases.

VII. Conclusions and Future Work

In this paper, we investigated the scheduling problem in a secure wireless network. The reliability, security and stability are jointly considered. The reliability and security issues are considered through a probabilistic secure transmission rate whose long-term average is maximized, and the stability issue is considered through the queue length stability. By using stochastic network optimization, the offline problem is decomposed to an online problem, which may not be convex. Motivated by the Lagrangian dual of the online problem, we proposed an approximate but simple algorithm to solve the problem. Along with that, a low computational complexity scheduling algorithm and an algorithm that considers the adaptive power allocation were proposed. Simulation results showed that, all three algorithms can achieve a similar performance in terms of the secure transmission rate, while the secrecy outage probability of the low complexity one is quite different from the other two when the system is subject to a low traffic load. Furthermore, several observations were obtained on the relationship between the secure transmission rate of the system and traffic load, channel conditions, etc. These observations provide important insights and guidelines for the design and resource management of future wireless networks using secure communication technologies.

There are several open research issues beckon for further research. First, although a low complexity scheduling algorithm is developed, the computational complexity may need to be further reduced, since a nonconvex problem needs to be solved. Second, in a more practical scenario, it is possible that only part of the eavesdropper's channel information can be obtained, so how to use the partial information to schedule the user against the eavesdropper is still open. In an even more common scenario that the eavesdropper is invisible to the scheduler, how to design a scheduling algorithm that can do a best-effort secure transmission needs to be further investigated.

Nevertheless, the proposed work serves as a first-step towards the scheduling problem in a multi-user secure wireless network under the coding-delay-limited scenario.

References

[1] Y-S Shiu, S-Y Chang, H-C Wu, S. C-H Huang, H-H Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66-74, April 2011.

[2] S. Gollakota, D. Katabi, "Physical layer wireless security made fast and channel independent," in *IEEE INFOCOM 2011*, pp. 1125-1133, 10-15 April 2011.

[3] Q. Wang, H. Su, K. Ren, K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *IEEE INFOCOM 2011*, pp. 1422-1430, 10-15 April 2011.

[4] H. Liu, J. Yang, Y. Wang, Y. Chen, "Collaborative secret key extraction leveraging Received Signal Strength in mobile wireless networks," in *IEEE INFOCOM 2012*, pp. 927-935, 25-30 March 2012.

[5] N. Patwari, S. K. Kasera, "Robust location distinction using temporal link signatures," in *ACM MobiCom'07*, 2007.

[6] J. Zhang, M. H. Firooz, N. Patwari, S. K. Kasera, "Advancing wireless link signatures for location distinction," in *ACM MobiCom'08*, 2008.

[7] Y. Liu, P. Ning, "Enhanced wireless channel authentication using time-synched link signature," in *IEEE INFOCOM 2012*, pp. 2636-2640, 25-30 March 2012.

[8] T. Li, J. Ren, Q. Ling, A. Jain, "Physical layer built-in security analysis and enhancement of CDMA systems," in *IEEE Military Communications Conference 2005*, Oct. 2005.

[9] Y. Hwang, H. C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: analysis and design," *IEEE Transactions on Signal Processing*, vol. 52, no. 9, pp. 2637-2649, Sept. 2004.

[10] S. Goel, R. Negi, "Secret communication in presence of colluding eavesdroppers", in *IEEE MILCOM'05*, 2005.

[11] A. Sheikholeslami, D. Goeckel, H. P.-Nik, D. Towsley, "Physical layer security from inter-session interference in large wireless networks," in *IEEE INFOCOM 2012*, pp. 1179-1187, 25-30 March 2012.

[12] P. K. Gopala, L. Lai, H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[13] A. Khisti, A. Tchamkerten, G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2453-2469, June 2008.

[14] Y. Liang, H. V. Poor, S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory,* vol. 5, no. 4-5, pp. 355–580, Jun. 2009.

[15] S. K. L.-Y.-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, pp. 451456, July 1978.

[16] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[17] F. Oggier, B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961-4972, Aug. 2011.

[18] Y. Liang, H. V. Poor, L. Ying, "Wireless broadcast networks: Reliability, security, and stability," in *Information Theory and Applications Workshop 2008*, pp. 249-255, Jan. 27 2008 - Feb. 1 2008.

[19] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, N. B. Shroff, "Joint power and secret key queue management for delay limited secure communication," in *IEEE INFOCOM 2010*, 14-19 March 2010.

[20] Z. Mao, C. E. Koksal, N. B. Shroff, "Towards achieving full secrecy rate in wireless networks: A control theoretic approach," in *Information Theory and Applications Workshop (ITA) 2011*, 6-11 Feb. 2011.

[21] D. Qiao, M. C. Gursoy, S. Velipasalar, "Secure wireless communication and optimal power control under statistical queueing constraints," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 628-639, Sept. 2011.

[22] M. J. Neely, "Stochastic network optimization with application to communication and queueing systems," *Synthesis Lectures on Communication Networks*, 2010.

[23] S. P. Boyd and L. Vandenberghe. *Convex optimization*. Cambridge University Press, 2004.