This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2645702, IEEE Transactions on Vehicular Technology

Minimizing Secrecy Outage Probability in Multiuser Wireless Systems with Stochastic Traffic

Xuan Wang, Yi Chen, *Student Member, IEEE*, Lin Cai, *Senior Member, IEEE* and Jianping Pan, *Senior Member, IEEE*

***Abstract*—We first extend the definition of the secrecy outage probability to wireless systems with adaptive transmission rates and secrecy rates. Then we consider a scheduling problem in the aforementioned system, jointly considering the reliability, security and stability, where the scheduler tries to allocate wireless resources to the legitimate users, stabilize the system and minimize the secrecy outage probability. Stochastic network optimization framework is used to decompose the problem and an online algorithm is proposed. We further consider a related problem, discuss the optimal solution and show that the proposed algorithm cannot lead to optimal solution in some scenarios. By comparing the offline algorithm with our first algorithm, we further propose a second refined online algorithm which is an optimal one. Extensive simulations are conducted to show the impact of the information arrival rate and the channel conditions on the system secrecy outage probability. 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 system, 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 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, physical-layer security became an attractive research area, since it can provide different kinds of security solutions in wireless systems, by exploring the physical-layer features such as channel conditions that are traditionally overlooked.

Physical-layer security in wireless systems has been widely discussed from different aspects [2]. 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 was discussed in [5]–[7]. The uniqueness feature can also be used as the link signature for authentication as discussed in [8]–[10]. The spread spectrum communication has been revisited as a physical-layer security approach in [11], [12]. Cooperative jamming and artificial noise were used to improve the secrecy capacity region as discussed in [13], [14].

Although these designed security schemes utilized the uniqueness of the physical-layer information, most of them were 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 multiuser wireless systems.

Specifically, the scheduling problem in a multi-user wireless system with one eavesdropper is studied. The traditional approach tries to maximize the ergodic achievable rate of the system (e.g., [15], [16]), 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. Different from the above, we consider minimizing the secrecy outage probability 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 to maximize the ergodic achievable rate [15], [16]. Therefore, the scheduling problem is formulated as an optimization problem minimizing the system secrecy outage probability (security issue) and subject to the constraints that the queues in the system should be stable (stability issue) and the transmission rate does not exceed the capacity region (reliability issue).

Little work that considering these three aspects jointly has been done. The research on this issue began with the assumption that the eavesdroppers' channel state information (CSI) at the symbol level (full instantaneous CSI) can be obtained by the BS, such as [21]–[25]. Considering the practical difficulty, [26] relaxed the assumption on the instantaneous CSI in a single legitimate receiver case. In [27], the authors further relaxed the instantaneous CSI assumption in a multiple legitimate receivers case. However, how to deal with multiple legitimate receivers still needs further investigation. 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.

The contributions of this work are four-fold. First we have extended the definition of the secrecy outage probability to wireless systems with channel-adaptive transmission. Second, we have proposed two online algorithms for the aforementioned scheduling problem, and showed that directly applying the stochastic network optimization framework cannot yield an optimal solution and some modifications should be done. Third, we have discussed a related offline problem, and proposed an optimal offline algorithm which motivates us to design the optimal online algorithm. Fourth, we have elaborated the impact of the information arrival rate and the channel conditions on the system secrecy outage probability

Part of the results has been presented at IEEE Infocom 2014 [1], Toronto, Canada.

X. Wang was with University of Victoria, Canada. Y. Chen, L. Cai and J. Pan are with University of Victoria, Canada (e-mail: {chenyi, cai, pan}@uvic.ca).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2645702, IEEE Transactions on Vehicular Technology

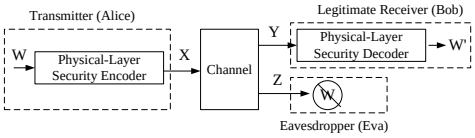


Fig. 1. Wire-tap Channel

through extensive simulations.

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. System models are introduced in Section III. Secrecy outage probability is revisited and the problem is formulated in Section IV. Online and offline algorithms are discussed in Section V. In Section VI, a case study of the proposed algorithms is presented, followed by the evaluation in Section VII. We conclude the paper in Section VIII.

II. Preliminaries and Related Work

A. Physical-Layer Security

Security is an important issue in communications, which typically includes confidentiality, integrity, authentication, and nonrepudiation. The confidentiality guarantees that 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 techniques. While for a wireless network, due to the broadcast nature of the wireless medium, the secret key distribution becomes a difficult problem [17]. The information-theoretical security, one branch of the physical-layer security, aims to provide an alternative solution to the confidentiality, and 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. Alice has a message W intended to transmit to a legitimate receiver Bob. 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 Bob through a wireless channel. Due to the broadcast nature of the channel, both Bob and the eavesdropper Eva can observe the corrupted messages, Y and Z. The decoder in Bob maps the received Y to an estimated message W'. The purpose of the encoder and decoder is to ensure that the estimated message is the same as the original one, i.e., $W' = W$, and the corrupted message Z received by Eva 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 a system is [18]

$$C_s = [C_Y - C_Z]^+,$$

where C_Y and C_Z are the capacity of the Bob's channel $X \to Y$ and Eva's channel $X \to Z$, respectively.

This result suggests that a perfect secrecy can be achieved if the entropy of the original message W is no greater than the secrecy capacity, *i.e.*, $H(W) \leq C_s$. Otherwise, part of W can be decoded from Z.

B. Related Work

Scheduling and resource allocation in a secure wireless communication system has been widely discussed in the literature. However, most of the works took a traditional information-theoretical perspective, i.e., quantifying the capacity region under different network settings. These works tried 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 [19]; that of a Gaussian wire-tap channel in [18]; that of a fading channel in [15]; that of a fading broadcast channel in [16]; that of a MIMO broadcast channel in [20]. All these works considered the reliability and security issue in communications, and ignored the stability issue which is typically treated in the higher layers. 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 considering these three aspects jointly. In [32], the authors investigated the opportunistic scheduling in a mixed radio frequency/free space optical network where the objective is the trade-off between security and reliability. In [22], the authors studied how to transmit confidential messages to users in a fast-fading broadcast wireless network, subject to three constraints: the reliability constraint that the message can be perfectly decoded, the security constraint that the message is perfectly secured and the stability constraint that the system is queue-length stable. An achievable secrecy rate region was obtained and a max-weight type of scheduling algorithm along with the optimal power control policy was designed so to satisfy these three requirements. A similar work was reported in [23], where the achievable secret rate region was obtained by using opportunistic scheduling. In [21] the authors studied the queue length stability through the effective bandwidth method and proposed a power allocation algorithm to achieve the effective secure throughput region. In [24], a secure communication system was 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 has also been designed to maximize the transmission rate. A work similar to [24] was reported in [25] where a different objective is used. All the above works assumed that the instantaneous CSI of the eavesdropper should be known by BS.

Considering the practical difficulty of the above assumption, in [26], the power allocation problem of a secure wireless communication system in the presence of statistical queueing constraints was studied. The effective secure throughput region was obtained through an effective capacity method, and a power allocation scheme that achieves such a region has been obtained. The obtained scheme implicitly considers the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2645702, IEEE Transactions on Vehicular Technology

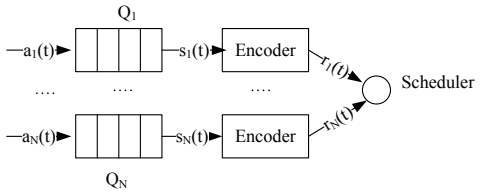


Fig. 2. System Block Diagram

stability issue of the system, since a queue constraint is employed. However, considering a single legitimate receiver, the scheme is not scalable to a multi-legitimate-receiver case, which motivates this work. In [27], a scheduling algorithm was proposed to maximize the weighted-sum-rate with constraints that the queue should be stable and the secrecy outage probability proposed in [4] should meet certain constraints. However, the secrecy outage probability in [27] is actually the upper bound, as it also includes the secrecy outage probability for users that are not scheduled to transmit.

III. System Models

We consider the downlink of a wireless network, with one base station (BS), N independent legitimate receivers and one eavesdropper. The multiple eavesdropper case can be easily extended as discussed in [1]. 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. The system is a time-slotted one. Without loss of generality, we further assume that the slot length is 1 second. The system model is shown in Fig. 2.

A. Queueing Model

We assume that the data packets arrive at the end of each time slot and are queued in an infinite-size virtual buffer reserved for each legitimate user. The amount of the data arriving in time slot t for user i, $a_i(t)$, is a random variable with finite moments and cannot be transmitted until slot $t+1$. The average arrival rate is λ_i. Assume that the amount of the data of user i being transmitted in the same time slot to the physical-layer security encoder is $s_i(t)$. The queue dynamic is as follows

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

where $Q_i(t)$ is the amount of the data buffered in queue i in time slot t, and $s_i(t) \leq Q_i(t)$ since the transmitted data size cannot be larger than the buffered data size.

B. Physical-Layer Security Encoder

The encoder uses Wyner's encoding scheme [19] to encode the input data $s_i(t)$, and the output data size is $r_i(t)$, which should be equal to the available channel resource that is allocated to user i in time slot t. The output data size should be no less than the input data size, 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.

C. 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 the 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 the eavesdropper are $\gamma_i(t) = |g_i(t)|^2$ and $\gamma_e(t) = |g_e(t)|^2$, respectively.

Furthermore, we assume that 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. As a result, $\{\gamma_e(\cdot)\}$ are i.i.d. random variables[1] and $\{\gamma_i(\cdot)\}$ are known by the BS.

Assume that in each time slot, only one user can transmit its data, but the user does not necessarily use all the time portion in one slot. The resource allocated to user i in time slot t used for transmission is $r_i(t)$ satisfying

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

where $p(t)$ is the allocated power in time slot t and $\tau_i(t)$ is the time portion used for transmission. Note that $\tau_i(t) \leq 1$, so the above equation guarantees the reliable communication between legitimate users and the BS. We further assume that the system is subject to a peak power constraint in each time slot, *i.e.*, $p(t) \leq 1$ and we assume that the maximal power is one unit.

IV. Secrecy Outage Probability Revisited and Problem Formulation

Since the BS does not know the instantaneous CSI of the eavesdropper's channel, it is inevitable that secrecy outage happens. In this section we first revisit the secrecy outage probability defined in the literature for a single-user wireless system with a constant transmission rate, and discuss how the existing definition can be extended to a single-user wireless system with channel-adaptive transmission rate.

For the system illustrated in Fig. 1, in the literature, there are two distinct definitions of secrecy outage probability. In

[1] $\{\gamma_e(\cdot)\}$ can be degraded to a constant if the channel between the BS and the eavesdropper is an AWGN channel.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2645702, IEEE Transactions on Vehicular Technology

[3], the secrecy outage event is defined as $\mathcal{O}(s) := \{C_s < s\}$, where s is the target secrecy rate from Alice to Bob. The secrecy outage probability is defined as

$$P^{\text{out}} = \mathbb{P}(C_s < s).$$

As pointed out in [4], such a definition of the secrecy outage event does not distinguish between reliability and security, therefore may not be a desirable design metric here.

In [4], the author designed an alternative secrecy outage probability, which is a conditional probability as

$$P^{\text{out}} = \mathbb{P}(C_e > r - s|\text{message transmission}),$$

where r is the transmission rate from Alice to Bob, and C_e is the channel capacity from Alice to Eva.

In practice, if Alice can observe Bob's channel and obtain the channel state information, then Alice can adaptively choose s to minimize the secrecy outage probability. Also, in a modern time-slotted wireless communication system, the data are transmitted block-by-block .

Consequently the secrecy outage probability in time slot t can be obtained as

$$P^{\text{out}}(t) = \mathbb{P}(C_e(t) > r(t) - s(t)|\text{message transmission}). \quad (1)$$

Since the message transmission means $s(t) > 0$, and we further have

$$\begin{aligned} C_e(t) &= \tau(t)\log(1+p(t)\gamma_e(t)), \\ r(t) &= \tau(t)\log(1+p(t)\gamma(t)), \end{aligned}$$

where $p(t)$ and $\tau(t)$ is the power and time portion allocated to the user, so (1) can be further presented as

$$P^{\text{out}}(t) = 1 - F(\frac{(1+p(t)\gamma(t))\exp(-\frac{s(t)}{\tau(t)}) - 1}{p(t)}), \quad (2)$$

for $s(t) > 0$, where F is the cumulative distribution function (CDF) of γ_e[2], and $P_{\text{out}}(t)$ is not defined for $s(t) = 0$.

When the secrecy outage happens, the information will be leaked to Eva. In order to quantify how much information is leaked, we define the bit-level secrecy outage probability as follows:

$$\bar{P}^{\text{out}} = \lim_{T\to\infty} \frac{\sum_{t=1}^{T} s(t)P^{\text{out}}(t)}{\sum_{t=1}^{T} s(t)}, \quad (3)$$

Note that due to the special structure of (3), when obtaining $\bar{P}^{\text{out}}$, the defined domain of (2) is relaxed to $s(t) \in [0, +\infty)$.

Problem Formulation

We are interested in a best-effort security solution, since the secrecy outage may be inevitable without the knowledge of eavesdropper's instantaneous CSI information.

In each time slot, the scheduler determines how much data ($s_i(t)$) should be fetched from the queue and sent to the encoder, and determines how to protect the data by choosing an appropriate output data size 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.

In order to achieve a high level of secrecy, we need to minimize the secrecy outage probability of the system, which is defined as the average weighted secrecy outage probability of each user, *i.e.*, $\sum_i \frac{1}{N}(w_i\lambda_i N)\bar{P}_i^{\text{out}} = \sum_i w_i\lambda_i\bar{P}_i^{\text{out}}$, where $w_i\lambda_i N$ is the weight assigned to user i, w_i is the weighting parameter, and

$$\begin{aligned} \bar{P}_i^{\text{out}} &= \lim_{T\to\infty} \frac{\sum_{t=1}^{T} I_i(t)s_i(t)P_i^{\text{out}}(t)}{\sum_{t=1}^{T} I_i(t)s_i(t)}, \\ P_i^{\text{out}}(t) &= 1 - F(\frac{(1+p(t)\gamma_i(t))\exp(-\frac{s_i(t)}{\tau_i(t)}) - 1}{p(t)}), \end{aligned}$$

where $I_i(t) \in \{0, 1\}$ indicates which user is selected in time slot t for transmission, and satisfies $\sum_i I_i(t) \le 1$.

Therefore, the scheduling problem can be formulated as:

$$\begin{aligned} \min_{\boldsymbol{\tau},\mathbf{s},\mathbf{I},p} \quad & \sum_i w_i\lambda_i\bar{P}_i^{\text{out}} && \text{(4a)} \\ s.t. \quad & Q_i \text{ is stable}, && \text{(4b)} \\ & s_i(t) \le \tau_i(t)\log(1+p(t)\gamma_i(t)), && \text{(4c)} \\ & s_i(t) \le Q_i(t), && \text{(4d)} \\ & \tau_i(t) \le 1, \sum_i I_i(t) \le 1, I_i(t) \in \{0,1\}, && \text{(4e)} \\ & p(t) \le 1. && \text{(4f)} \end{aligned}$$

Because $\forall i$, Q_i is stable and every user achieves the rate stability, we have $\lim_{T\to\infty}\frac{1}{T}\sum_{t=1}^{T} I_i(t)s_i(t) = \lim_{T\to\infty}\frac{1}{T}\sum_{t=1}^{T} a_i(t) = \lambda_i$, and the objective function can be simplified as

$$\begin{aligned} & \lim_{T\to\infty}\sum_{t=1}^{T}\sum_i \frac{w_i I_i(t)s_i(t)}{T}P_i^{\text{out}}(t) \\ = & -\lim_{T\to\infty}\sum_{t=1}^{T}\sum_i (F(\frac{(1+p(t)\gamma_i(t))\exp(-\frac{s_i(t)}{\tau_i(t)}) - 1}{p(t)})\cdot \\ & \frac{w_i I_i(t)s_i(t)}{T}) + \sum_i w_i\lambda_i. \end{aligned} \quad (5)$$

Because $((1 + p(t)\gamma_i(t))\exp(-s_i(t)/\tau_i(t)) - 1)/p(t)$ is a monotonically increasing function of $p(t)$, and the CDF function F is a monotonically increasing function, (5) is minimized when $p(t)$ is maximized, which suggests $p^*(t) = 1$.

Define $R_i^s(t) = s_i(t)(1 - P_i^{\text{out}}(t))|_{p(t)=1} = s_i(t)F((1 + \gamma_i(t))e^{-\frac{s_i(t)}{\tau_i(t)}} - 1)$ as the secure transmission rate of user i in time slot t, so minimizing (5) is equivalent to solving the following weighted-sum secure transmission rate maximization (WSSTRM) problem

$$\begin{aligned} \max_{\boldsymbol{\tau}(t),\mathbf{s}(t),\mathbf{I}(t)} \quad & \lim_{T\to\infty}\frac{1}{T}\sum_{t=1}^{T}\sum_i w_i I_i(t)R_i^s(t) \\ s.t. \quad & Q_i \text{ is stable}, \\ & s_i(t) \le \min(\tau_i(t)\log(1+\gamma_i(t)), Q_i(t)), \\ & \tau_i(t) \le 1, \sum_i I_i(t) \le 1, I_i(t) \in \{0,1\}. \end{aligned}$$

[2]Since $\{\gamma_e(\cdot)\}$ are i.i.d. random variables, t can be ignored.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2645702, IEEE Transactions on Vehicular Technology

Note that in the above formulation we assume that the arrival rate λ_i is known to the scheduler. If λ_i is unknown, by substituting λ_i with $\frac{1}{t}\sum_{k=1}^{t} a_i(k)$, we can obtain the equivalent problem formulation.

V. Weighted-Sum Secure Transmission Rate Maximization

A. Online Algorithm

According to the stochastic network optimization theory [28], 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

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

If the RHS of the above inequality is minimized, which can be achieved by maximizing $\sum_i Q_i(t)s_i(t)$ in each time slot, we have

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

where $\epsilon \geq 0$ 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 [28], the system is stable.

By treating problem (6) as a multi-objective (maximizing secure transmission and stabilizing queues) problem and using the linear scalarization of the two objectives (which is equivalent to the drift-plus-penalty method in [28]), problem (6) is solved by solving the following online problem in each time slot

$$\begin{aligned} \max_{\boldsymbol{\tau},\mathbf{s},\mathbf{I}} \quad & \sum_i I_i Q_i s_i + V w_i I_i R_i^s && \text{(7a)}\\ s.t. \quad & \forall i, s_i \leq \min(\tau_i \log(1+\gamma_i), Q_i), && \text{(7b)}\\ & \tau_i \leq 1, \sum_i I_i \leq 1, I_i \in \{0,1\}, && \text{(7c)} \end{aligned}$$

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.

Note that the method used here is often referred to as the drift-plus-penalty method, and the optimality can be guaranteed according to [28]. However, in the system under consideration, due to the subtle difference between the queueing model presented in Sec. III and [28], the optimality cannot be guaranteed under some circumstances, which will be discussed later. But by using the stochastic network optimization to decompose the problem, it is possible to obtain an online algorithm without the detailed knowledge of the channel information, which is of practical interest.

Algorithm WSSTRM: Define $k_i = s_i/\tau_i$, $g_i(k_i) = (1+\gamma_i)\exp(-k_i) - 1$ and $U_i(k_i) = Q_i k_i + V w_i k_i F(g_i(k_i))$. Problem (7) can be reformulated as

$$\begin{aligned} \max_{\boldsymbol{\tau},\mathbf{k},\mathbf{I}} \quad & \sum_i \tau_i I_i U_i(k_i) && \text{(8a)}\\ s.t. \quad & \forall i, k_i \leq \log(1+\gamma_i), k_i\tau_i \leq Q_i, && \text{(8b)}\\ & \tau_i \leq 1, \sum_i I_i \leq 1, I_i \in \{0,1\}. && \text{(8c)} \end{aligned}$$

Note that for the above problem, we need to solve the following problem for each user i.

$$\begin{aligned} \max_{\tau_i,k_i} \quad & \tau_i U_i(k_i)\\ s.t. \quad & k_i \leq \log(1+\gamma_i), k_i\tau_i \leq Q_i, \tau_i \leq 1. \end{aligned}$$

If $Q_i \geq \log(1+\gamma_i)$, then the problem is equivalent to

$$\begin{aligned} \max_{\tau_i,k_i} \quad & \tau_i U_i(k_i)\\ s.t. \quad & k_i \leq \log(1+\gamma_i), \tau_i \leq 1. \end{aligned}$$

and is solved when $\tau_i = 1$.

If $Q_i \leq \log(1+\gamma_i)$, then we must have $k_i\tau_i = Q_i$ so that the problem is equivalent to

$$\begin{aligned} \max_{\tau_i,k_i} \quad & \tau_i Q_i k_i + V w_i k_i F(g_i(k_i))\\ s.t. \quad & k_i\tau_i = Q_i, 1 \geq \tau_i \geq Q_i/\log(1+\gamma_i). \end{aligned}$$

which is further equivalent to

$$\begin{aligned} \max_{\tau_i,k_i} \quad & F(g_i(Q_i/\tau_i))\\ s.t. \quad & 1 \geq \tau_i \geq Q_i/\log(1+\gamma_i). \end{aligned}$$

Because $F(g_i(Q_i/\tau_i))$ is an increasing function of τ_i, so that the problem is solved when $\tau_i = 1$.

In summary, problem (8) is solved by selecting user i^* to transmit, where

$$i^* \in \arg\max_i U_i^*(k_i^*),$$

and

$$U_i^*(k_i^*) = \max_{k_i \leq \min(Q_i, \log(1+\gamma_i))} U_i(k_i). \quad (13)$$

The portion of time user i^* used is $\tau_i^* = 1$.

$U_i^*(k_i^*)$ is obtained by solving (13) which might not be a convex problem, since the convexity depends on function F and is generally unknown. But since (13) is a one-dimensional problem in a closed set, the optimum solution can be obtained by one-dimensional line search algorithms [29].

However, in order to perform the line search algorithm efficiently, it is important to know the trend of $U_i(k_i)$, which is critical to the choice of the initial point and when the algorithm should stops once a local optimum is found.

Define $\hat{F}(k_i) = F(g_i(k_i))$, and $G(k_i) = k_i\hat{F}(k_i)$. Taking derivative of k_i, we have

$$\begin{aligned} G^{'}(k_i) &= k_i\hat{F}^{'}(k_i) + \hat{F}(k_i),\\ G^{''}(k_i) &= k_i\hat{F}^{''}(k_i) + 2\hat{F}^{'}(k_i),\\ g_i^{'}(k_i) &= -1 - g_i(k_i),\\ g_i^{''}(k_i) &= g_i(k_i) + 1,\\ \hat{F}^{'}(k_i) &= F^{'}(g_i(k_i))(-1-g_i(k_i)),\\ \hat{F}^{''}(k_i) &= (g_i(k_i)+1)^2(F^{''}(g_i(k_i)) + \frac{F^{'}(g_i(k_i))}{g_i(k_i)+1}). \end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2645702, IEEE Transactions on Vehicular Technology

Typically, for a wireless channel, the distribution of the SNR has the following property: when $\gamma < \gamma_t$, $F^{''}(\gamma) > 0$; when $\gamma > \gamma_t$, $F^{''}(\gamma) < 0$, where γ_t is an SNR threshold[3]. As a result, $F^{''}(g_i(k_i)) < 0$ when $k_i < k_i^{t1}$; $F^{''}(g_i(k_i)) > 0$ when $k_i > k_i^{t1}$. Since $\frac{F^{'}(g_i(k_i))}{g_i(k_i)+1} > 0$ always holds, we have when $k_i < k_i^{t2}$, $\hat{F}^{''}(k_i) < 0$; when $k_i > k_i^{t2}$, $\hat{F}^{''}(k_i) > 0$.

Note that $\hat{F}^{'}(k_i) < 0$, so if $\hat{F}^{''}(k_i) < 0$, then $G^{''}(k_i) < 0$. If $\hat{F}^{''}(k_i) > 0$, then for $k_i < k_i^{t3}$, $G^{''}(k_i) < 0$, and for $k_i > k_i^{t3}$, $G^{''}(k_i) > 0$. In summary, we have that $G^{'}(k_i)$ first decreases and then possibly increases[4]. Since $G^{'}(0) > 0$ and $G^{'}(\log(1+\lambda_i)) < 0$, so $G^{'}(k_i)$ decreases from a positive value to a negative value, and possibly will increase to another negative value. So $G(k_i)$ should be first increasing and then decreasing, the local maximum of $G(k_i)$ is the global maximum, and near the local maximum, $G(k_i)$ is concave.

Since $U_i(k_i) = Q_i k_i + V w_i G(k_i)$, $U_i(k_i)$ only has three possible trends. First is that $U_i(k_i)$ first increases and then decreases. Second is that it always increases. Third is that it has an increase-decrease-increase trend.

Based on the above observation, (13) can be solved by finding the first local maximum starting from 0, and comparing it with the boundary value to choose the larger one.

B. Alternative Relaxed Offline Problem and Optimal Solution

After some manipulation we have $R_i^s|_{\tau_i=1} = G(k_i)$. So, $R_i^s|_{\tau_i=1}$ first increases and then decreases, and near the maximum of $R_i^s|_{\tau_i=1}$ it is concave. Although this cannot guarantee the objective is concave, as the local maximum of $R_i^s|_{\tau_i=1}$ is also the global maximum, by solving the following relaxed problem, it yields the maximum secure transmission in the long term.

The relaxed problem is as follows

$$\begin{aligned} \max_{\boldsymbol{\tau},\mathbf{s},\mathbf{I}} \quad & \sum_i w_i \mathbb{E}[R_i^s(\boldsymbol{\gamma}) I_i(\boldsymbol{\gamma})] && \text{(14a)} \\ s.t. \quad & s_i(\boldsymbol{\gamma}) \le \tau_i(\boldsymbol{\gamma}) \log(1+\gamma_i), && \text{(14b)} \\ & \tau_i(\boldsymbol{\gamma}) \le 1, \mathbb{E}[s_i(\boldsymbol{\gamma}) I_i(\boldsymbol{\gamma})] = \lambda_i, && \text{(14c)} \\ & \sum_i I_i(\boldsymbol{\gamma}) \le 1, I_i(\boldsymbol{\gamma}) \in \{0,1\}, && \text{(14d)} \end{aligned}$$

where $\boldsymbol{\gamma}$ is the instantaneous channel gain vector. The partially augmented Lagrangian dual problem is

$$\begin{aligned} \min_{\mathbf{u}} \quad & \max \textstyle\sum_i \mathbb{E}[I_i(\boldsymbol{\gamma})(w_i R_i^s(\boldsymbol{\gamma}) + u_i s_i(\boldsymbol{\gamma}))] - u_i \lambda_i \\ s.t. \quad & \forall i, s_i(\boldsymbol{\gamma}) \le \tau_i(\boldsymbol{\gamma}) \log(1+\gamma_i), \tau_i(\boldsymbol{\gamma}) \le 1, \\ & \textstyle\sum_i I_i(\boldsymbol{\gamma}) \le 1, I_i(\boldsymbol{\gamma}) \in \{0,1\}. \end{aligned}$$

Using the primal decomposition, and denoting $k_i(\boldsymbol{\gamma}) = s_i(\boldsymbol{\gamma})/\tau_i(\boldsymbol{\gamma})$, for each $\boldsymbol{\gamma}$, we need to solve the following problem

$$\begin{aligned} \max_{\boldsymbol{\tau},\mathbf{k},\mathbf{I}} \quad & \sum_i I_i(\boldsymbol{\gamma}) \tau_i(\boldsymbol{\gamma}) k_i(\boldsymbol{\gamma}) (u_i + \\ & w_i F((1+\gamma_i) e^{-k_i(\boldsymbol{\gamma})} - 1)) \\ s.t. \quad & k_i(\boldsymbol{\gamma}) \le \log(1+\gamma_i), \tau_i(\boldsymbol{\gamma}) \le 1, \\ & \sum_i I_i(\boldsymbol{\gamma}) \le 1, I_i(\boldsymbol{\gamma}) \in \{0,1\}. \end{aligned}$$

The optimal solution to the above problem is selecting user $i^*(\boldsymbol{\gamma})$ and using all the time portion for transmission ($\tau^*_{i^*(\boldsymbol{\gamma})}(\boldsymbol{\gamma}) = 1$), such that $i^*(\boldsymbol{\gamma}) \in \arg\max_i \tilde{U}_i^*(k_i^*(\boldsymbol{\gamma}))$, where

$$\tilde{U}_i^*(k_i^*(\boldsymbol{\gamma})) = \max_{k_i(\boldsymbol{\gamma}) \le \log(1+\gamma_i)} \tilde{U}_i(k_i(\boldsymbol{\gamma})), \qquad (17)$$

and

$$\tilde{U}_i(k_i(\boldsymbol{\gamma})) = k_i(\boldsymbol{\gamma})(w_i F((1+\gamma_i) e^{-k_i(\boldsymbol{\gamma})} - 1) + u_i).$$

Since $k^*_{i^*(\boldsymbol{\gamma})}(\boldsymbol{\gamma})$ should further satisfy

$$\mathbb{E}[k^*_{i^*(\boldsymbol{\gamma})}(\boldsymbol{\gamma}) | i = i^*(\boldsymbol{\gamma})] = \lambda_i,$$

and $k_i^*(\boldsymbol{\gamma})$ is a function of u_i, as a result we can obtain u_i^*. A typical algorithm to obtain u_i^* is the gradient descent method, and u_i is updated based on

$$u_i^{(l+1)} = u_i^{(l)} - \epsilon^{(l)} (\mathbb{E}[k_i^{(l)}(\boldsymbol{\gamma}) \tau_i^{(l)}(\boldsymbol{\gamma})] - \lambda_i),$$

where $\epsilon^{(l)}$ is a step sequence and square summable [29], and $k_i^{(l)}(\boldsymbol{\gamma})$ and $\tau_i^{(l)}(\boldsymbol{\gamma})$ are the solutions of step l.

Discussion

Noting that u_i^* can be any value as long as $u_i^* + w_i > 0$, this results that the solution to (17) is not necessarily always positive. For some $\boldsymbol{\gamma}$ and $\mathbf{u}$, $k^*_{i^*(\boldsymbol{\gamma})}(\boldsymbol{\gamma}) = 0$, which means that the user should not transmit in order to achieve a better secure transmission rate in the long term. However, the online algorithm WSSTRM always selects a user to transmit as long as the user has data to send, and hence it is not always optimal. Comparing function $U_i(k_i)$ in the online algorithm with function $\tilde{U}_i(k_i(\boldsymbol{\gamma}))$ in the offline optimal algorithm, we can see that the purpose of Q_i/V in $U_i(k_i)$ is similar to u_i in $\tilde{U}_i(k_i(\boldsymbol{\gamma}))$ and conceptually Q_i/V can be considered as an "online" Lagrangian multiplier. However, as $Q_i/V \ge 0$ and u_i^* can be negative, conceptually the two algorithms are not identical, if $u_i^* < 0$. As $u_i^* < 0$ only if λ_i is small, which suggests that the algorithm WSSTRM cannot achieve optimality if λ_i is small. The algorithm WSSTRM tries to make a tradeoff between two objectives: maximizing the secure transmission rate and stabilizing the queues in the system. Note that when the arrival rate is small, the requirement for stabilizing the queue becomes less important, as it is possible that any resource allocation algorithm can stabilize the queue. Consequently, the scheduler only has one objective: to maximize the secure transmission rate and the algorithm WSSTRM is failed to do so.

[3] γ_t might be negative. If so, we have $\gamma \ge 0$, $F^{''}(\gamma) < 0$.

[4] Whether $G^{'}(k_i)$ has the increasing trend depends on the threshold value k_i^{t3}, as it might be out of the domain of function $G^{'}(k_i)$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2645702, IEEE Transactions on Vehicular Technology

C. Refined Online Algorithm: Algorithm WSSTRM-R

Based on the above analysis, if we can replace Q_i/V by another term which is a more proper "online representation" of u_i, then the refined online algorithm is optimal in terms of its performance.

Replacing $U_i(k_i)$ in Algorithm WSSTRM by

$$\hat{U}_i(k_i) = (Q_i - Vw_i)k_i + Vw_ik_iF(g_i(k_i)),$$

with the same iteration structure as that in Algorithm WSSTRM, we have a queue-length-shifted online algorithm, which is referred to as Algorithm WSSTRM-R.

Note that Algorithm WSSTRM-R needs to solve

$$\hat{U}_i^*(k_i^*) = \max_{k_i \le \min(Q_i, \log(1+\gamma_i))} \hat{U}_i(k_i), \quad (18)$$

for each user, which is slightly different from Algorithm WSSTRM, as the possible increasing trend of $\hat{U}_i(k_i) = (Q_i - Vw_i)k_i + Vw_iG(k_i)$ might be different from $U_i(k_i) = Q_ik_i + Vw_iG(k_i)$, which depends on the value of Q_i. But because $G^{'}(k_i)$ first decreases and then increases, if $Q_i - Vw_i < 0$, then $\hat{U}_i(k_i)$ either decreases or first increases and then decreases. As a result, if $\hat{U}_i^{'}(k_i) < 0$ then the global maximum is achieved at $k_i = 0$, otherwise the algorithm to solve problem (18) is identical to the one solving problem (13).

Note that Algorithm WSSTRM-R solves the following problem in each time slot:

$$\begin{aligned} \max_{\boldsymbol{\tau},\mathbf{s},\mathbf{I}} \quad & \sum_i I_iQ_is_i + Vw_iI_i(R_i^s - s_i) \\ s.t. \quad & s_i \le \min(\tau_i \log(1+\gamma_i), Q_i), \\ & \tau_i \le 1, \sum_i I_i \le 1, I_i \in \{0,1\}, \end{aligned}$$

which is a decomposed sub-problem of the following problem

$$\max_{\boldsymbol{\tau},\mathbf{s},\mathbf{I}} \quad \lim_{T\to\infty} \frac{1}{T}\sum_{t=1}^{T}\sum_i w_iI_i(R_i^s(t) - s_i(t)) \quad (20a)$$

$$s.t. \quad Q_i \text{ is stable}, \quad (20b)$$

$$s_i(t) \le \min(\tau_i(t)\log(1+\gamma_i(t)), Q_i(t)), \quad (20c)$$

$$\tau_i(t) \le 1, \sum_i I_i(t) \le 1, I_i(t) \in \{0,1\}. \quad (20d)$$

Due to the stability constraint, we have

$$\lim_{T\to\infty} \frac{1}{T}\sum_{t=1}^{T}\sum_i w_iI_i(t)s_i(t) = \sum_i w_i\lambda_i,$$

which is a constant. As a result, problem (20) is equivalent to problem (6). Consequently, Algorithm WSSTRM-R can stabilize the system and the performance in terms of maximizing the weighted-sum secure rate should be no worse than Algorithm WSSTRM. Furthermore, comparing $\hat{U}_i(k_i)$ with $\tilde{U}_i(k_i(\boldsymbol{\gamma}))$, the feasible region of $Q_i/V - w_i$ is identical to u_i, and as a result, $Q_i/V - w_i$ can be considered as a proper "online representation" of u_i. In Sec. VII, we will show that indeed Algorithm WSSTRM-R is an online optimal algorithm.

D. Algorithm Implementation Details

In order to implement the proposed algorithms, a proper V should be chosen; the queue length information and the channel rate of the legitimate users of each time slot are needed in the base station. In this subsection, we discuss these implementation details.

1) The choice of V: Since $Q_i(t)/V - w_i$ can be considered as a proper "online representation" of $\mu_i^{(l)}$, we can discuss the choice of V based on certain properties of $\mu_i^{(l)}$. First we note that $\lim_{l\to\infty}\mu_i^{(l)}$ should strongly converge to μ_i^*; however $Q_i(t)/V - w_i$ cannot strongly converge but will oscillate around a point. The oscillation bound can be controlled by V and obviously a larger V results in a tighter bound. However we also know that the convergence speed of μ_i^* is associated with the step size. If the step size is a constant, a larger step size means a faster convergence, but may not lead to optimum; a smaller step size means a slower convergence, but leads to a tighter bound. Based on this idea we can see that the step size of $Q_i(t)/V - w_i$ is associated with V, and a larger V means a smaller step size and a slower convergence speed.

2) Channel rate estimation and queue length information: Although we only discuss the downlink scheduling, the same framework can also be applied to the uplink scheduling. Instead of having the channel estimation in every time slot, the channel rates may be periodically measured and estimated, and there is a tradeoff between the feedback frequency and performance. In [30] the authors showed that an infrequent queue length information update can still ensure the system stability, which is useful when considering the uplink scheduling as there is overhead to obtain such information in base station. Besides the poor delay performance mentioned in [30], infrequent queue length information update also result in a suboptimal secure transmission rate since in each time slot the scheduling decision and resource allocation might be non-optimal and in the long term the scheduling algorithm cannot minimize the secure outage probability which is calculated by taking average over time.

VI. Case Study: Eavesdropper with an AWGN channel

A. Algorithm WSSTRM

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

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

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

Thus we have

$$U_i(k_i) = Q_ik_i + Vw_ik_i\delta([\log(\frac{1+\gamma_i}{1+\gamma_e})]^+ - k_i).$$

Denote $R_e^i = \max(\log(1+\gamma_i) - \log(1+\gamma_e), 0)$, which is the maximal supported secure data size[5] of user i that does

[5] R_e^i can also be viewed as the maximal supported secure rate, as we assume the slot length is one second.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2645702, IEEE Transactions on Vehicular Technology

not lead to secrecy outage. The transmission strategy for user i is as follows

$$U_i^*(k_i^*) = (Q_i + Vw_i)k_i^* \tag{21}$$

if $Q_i \le R_e^i$ or $\min(\frac{Q_i}{Vw_i}\log(1+\gamma_e), \frac{Q_i^2}{Q_i+Vw_i}) \le R_e^i \le Q_i$, where $k_i^* = \min(Q_i, R_e^i)$; otherwise

$$U_i^*(k_i^*) = Q_i k_i^*, \tag{22}$$

where $k_i^* = \min(Q_i, \log(1+\gamma_i))$.

The above transmission strategy can be explained as follows. When the available data (Q_i) is smaller than the maximal supported secure data size (R_e^i), the user should use all the resources to transmit all the available data, and the data are fully protected by the physical-layer encoder. If the SNR of the user is larger than a threshold, the maximal supported secure data size is chosen and all the data are fully protected by the physical-layer encoder; if the SNR of the user is worse, then the user should use all the available resource or transmit all the available data, but the data are not fully protected and secrecy outage happens with probability one.

B. Algorithm WSSTRM-R

Similar to Algorithm WSSTRM, the transmission strategy for user i is as follows:

$$U_i^*(k_i^*) = Q_i k_i^*$$

if $Q_i \le R_e^i$ or $(Q_i - Vw_i)\min(\frac{\log(1+\gamma_e)}{Vw_i}, 1) \le R_e^i \le Q_i$, where $k_i^* = \min(Q_i, R_e^i)$; otherwise

$$U_i^*(k_i^*) = (Q_i - Vw_i)k_i^*,$$

where $k_i^* = \min(Q_i, \log(1+\gamma_i))$.

Comparing Algorithm WSSTRM-R with Algorithm WSSTRM we can find that the key difference lies in a threshold and such difference results in that the long-term secure transmission rate can be improved when λ_i is small, *i.e.,* Q_i is small due to Little's law. If λ_i is small, $Q_i - Vw_i < 0$ should almost always hold. Consequently the data transmitted are always fully protected and the secure transmission rate is identical to λ_i. While for Algorithm WSSTRM, when λ_i is small but $Q_i > R_e^i$, whether the data can be fully protected also depends on the channel condition of user i, and the transmitted data are not always fully protected and thus cannot be optimal.

C. Offline Problem and Analysis

Similarly, we can obtain the solution to the relaxed offline problem as in Sec. V-B, and the transmission strategy for each user depends on the Lagrangian multiplier u_i^* and is shown as follows.

Case 1) when $u_i^* > 0$: if $\gamma_i \ge (1+\gamma_e)^{1+u_i^*/w_i} - 1$, then $U_i^*(k_i^*) = (u_i^* + w_i)k_i^*(\gamma_i)$ and $k_i^*(\gamma_i) = R_e^i$; otherwise $U_i^*(k_i^*) = u_i^* k_i^*(\gamma_i)$ and $k_i^*(\gamma_i) = \log(1+\gamma_i)$.

Case 2) when $u_i^* = 0$: if $\gamma_i \ge \gamma_e$ then $U_i^*(k_i^*) = w_i k_i^*(\gamma_i)$ and $k_i^*(\gamma_i) = R_e^i$; otherwise $U_i^*(k_i^*) = 0$ and $k_i^*(\gamma_i) \in [0, \log(1+\gamma_i)]$.

Case 3) when $-w_i < u_i^* < 0$: if $\gamma_i \ge \gamma_e$ then $U_i^*(k_i^*) = (u_i^* + w_i)k_i^*(\gamma_i)$ and $k_i^*(\gamma_i) = R_e^i$; if $\gamma_i \le \gamma_e$ then $U_i^*(k_i^*) = 0$ and $k_i^*(\gamma_i) = 0$.

Case 4) when $u_i^* \le -w_i$: $U_i^*(k_i^*) = 0$ and $k_i^*(\gamma_i) = 0$.

Furthermore, the Lagrangian multiplier is determined by the arrival rate $\boldsymbol{\lambda}$ through (18).

First we can see that Case 4 should never happen as using this transmission strategy cannot achieve the rate stability. Second, if $\gamma_i \ge (1+\gamma_e)^{1+[u_i^*]^+} - 1$, then the strategy is to always transmit data in R_e^i to achieve the maximal secure transmission rate. Third, if $\gamma_i < (1+\gamma_e)^{1+[u_i^*]^+} - 1$, then depending on the value of u_i^*, the strategy decides whether to transmit and how many data to transmit. If $u_i^* \ge 0$ then the user transmits at a positive rate in order to achieve the rate stability; if $u_i^* < 0$, then the user does not transmit as the rate-stable condition can be satisfied by the transmission strategy when $\gamma_i \ge \gamma_e$, which implies that the traffic load should be small. Fourth, by comparing the offline optimal transmission strategy with the online algorithm, the key difference is how to transmit data if the legitimate receiver's channel is bad. The online algorithm always tries to empty the queue, while the offline strategy will stop transmission if the traffic load is small, which utilizes the information about the traffic load explicitly.

In order to analyze the property of the solution, we restrict our attention to the single legitimate receiver case.

Denote

$$\begin{aligned}
\lambda_i^{\text{th1}} &= \int_{\gamma_e}^{\infty} \log(\frac{1+\gamma_i}{1+\gamma_e}) f_i(\gamma_i) d\gamma_i, \\
\lambda_i^{\text{th2}} &= \mathbb{E}[\log(1+\gamma_i)] - \log(1+\gamma_e)[1 - F(\gamma_e)], \\
\bar{R}_i &= \mathbb{E}[\log(1+\gamma_i)], \\
\bar{R}_i^{\text{th}}(\gamma) &= \int_0^{\gamma} \log(1+\gamma_i) f_i(\gamma_i) d\gamma_i, \\
R_e &= \log(1+\gamma_e).
\end{aligned}$$

after some calculation steps, the maximal secure transmission rate can be obtained as:

if $\lambda_i \le \lambda_i^{\text{th1}}$,

$$R_i^{s*} = \lambda_i,$$

and $u_i^* < 0$; if $\lambda_i^{\text{th1}} \le \lambda_i \le \lambda_i^{\text{th2}}$,

$$R_i^{s*} = \lambda_i^{\text{th1}},$$

$u_i^* = 0$; if $\lambda_i \ge \lambda_i^{\text{th2}}$,

$$R_i^{s*} = \lambda_i - \bar{R}_i^{\text{th}}(\gamma_{\text{th}}),$$

where γ_{th} is the solution to $\frac{\bar{R}_i - \lambda_i}{R_e} = 1 - F(\gamma_{\text{th}})$ and $u_i^* > 0$.

As the secrecy outage probability for a single user is $\bar{P}_i^{\text{out}} = \frac{\lambda_i - R_i^{s*}}{\lambda_i}$, we have

$$\bar{P}_i^{\text{out}} = \begin{cases} 0, & \lambda_i \le \lambda_i^{\text{th1}}, \\ 1 - \frac{\lambda_i^{\text{th1}}}{\lambda_i}, & \lambda_i^{\text{th1}} \le \lambda_i \le \lambda_i^{\text{th2}}, \\ \frac{\bar{R}_i^{\text{th}}(\gamma_{\text{th}})}{\lambda_i}, & \lambda_i^{\text{th2}} \le \lambda_i. \end{cases}$$

From the above equation we can see that when the arrival rate is small, the user does not experience secrecy outage,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2645702, IEEE Transactions on Vehicular Technology

as the arrival traffic lies inside the secrecy capacity region. When the arrival rate further increases, the secrecy outage probability also increases, but with two different increasing speeds, relative to the arrival rate.

D. Further Discussion

In this paper we have assumed that the PDF of the eavesdropper's channel is known in the base station, so if the eavesdropper's channel is an AWGN channel, the base station knows the exact channel SNR. Here we briefly discuss the impact of the system performance if the channel SNR estimation is not accurate at the base station.

We assume that the SNR of eavesdropper's channel used to perform the scheduling and resource allocation is $\tilde{\gamma_e}$, and the accurate SNR of eavesdropper's channel is γ_e. As a result, for the proposed algorithms, we need to replace γ_e with $\tilde{\gamma_e}$.

The inaccurate channel SNR has two impacts on the scheduling algorithms, as the scheduling algorithm essentially tries to minimize the secrecy outage probability and stabilize the system.

1) Impacts on the system stability or queue length stability: By looking closely at problem (6) and (20), we can see that the probability distribution of the SNR of the eavesdropper's channel is only associated with the objective function, and the estimation error has no effect on the feasible region. Since the objective of stabilizing the system is also not associated with the SNR of eavesdropper's channel, and the feasible region of the problem is not related to the SNR of eavesdropper's channel and thus algorithms WSSTRM and WSSTRM-R can always stabilize the system.

These can also be observed by considering two extreme cases, and we first analyze algorithm WSSTRM, as the same approach can be applied to analyze algorithm WSSTRM-R.

If $\tilde{\gamma_e} > \gamma_e$ and we assume $\tilde{\gamma_e}$ is sufficiently large. We have $R_e^i = 0$, so in algorithm WSSTRM, only equation (22) takes effects and obviously the scheduling algorithms degraded to a normal max-weight scheduling algorithm, which is throughput-optimal [31], and the system is stable.

If $\tilde{\gamma_e} < \gamma_e$ and we assume $\tilde{\gamma_e} = 0$. We have $R_e^i = \log(1+\gamma_i)$ so only equation (21) takes effects and obviously the scheduling algorithms degraded to a normal shifted-queue-length max-weight scheduling algorithm, which is throughput-optimal [31], and the system is stable.

2) Impacts on the secrecy outage probability: The inaccurate channel SNR may have a great impact on the secrecy outage probability. If $\tilde{\gamma_e} > \gamma_e$, the outage probability performance is bounded by the one calculated based on the inaccurate SNR, i.e. $\bar{P}^{\text{out}}(\gamma_e) <= \bar{P}^{\text{out}}(\tilde{\gamma_e})$ which is as in any instance, the scheduler thinks the eavesdropping is more severe and makes a more conservative scheduling decision to protect less data. However, if $\tilde{\gamma_e} < \gamma_e$, this may result in a significant performance degradation. For instance, we may choose a rate to transmit based on the $\tilde{\gamma_e}$ and the corresponding scheduling decision, which should fully protect the data if $\tilde{\gamma_e} = \gamma_e$. However, it is possible that the data are not protected at all because of the step function property of the PDF function of AWGN channel. This results in a significant performance loss in the secure transmission rate when the queue length is neither too large nor too small, and a performance degeneration on the secrecy outage probability. If possible, we should try to avoid the case that $\tilde{\gamma_e} < \gamma_e$ to avoid the severe performance degradation.

VII. Evaluation and Discussion

In this section, extensive simulations are conducted to study the performance of the proposed algorithms. Since our work focuses on the scheduling algorithm design to minimize the secrecy outage probability in the wireless systems, and thus in the simulation, we studied the secrecy outage probability in various network settings, including the single-legitimate-receiver scenario with Rayleigh fading, Nakagami fading and AWGN channel for the eavesdropper, and the multi-legitimate-receiver scenario with Rayleigh fading for legitimate receivers and AWGN channel for the eavesdropper. The results show that the Algorithm WSSTRM cannot achieve the optimal secrecy outage probability when the arrival rate is small; Algorithm WSSTRM-R is an optimal online scheduling algorithm that can achieve the optimal secrecy outage probability. The simulation results also confirmed our analysis presented in Sec. V and Sec. VI.

A. Simulation Setting

In the simulation, we consider a system that contains N legitimate receivers and one eavesdropper. The base station transmits data through the shared wireless channel to legitimate receivers while the eavesdropper tries to decode the message over-heard due to the broadcast feature of the wireless channel. Although the number of eavesdropper is limited to one, it is sufficient to quantify the performance of the proposed algorithms and investigate the relationship between the system performance and different network configurations. The wireless channels between the base station and any legitimate receivers (and eavesdropper) are modeled as Nakagami-m fading channels, and the channel gains of the receivers γ_i and the eavesdropper γ_e are Gamma distributed random variables. The probability density function of γ_i is

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

and the CDF of γ_i is

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

where m_i is the fading parameter of user i, and $\bar{\gamma}_i$ is the average channel gain 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 $m_i \to \infty, \gamma_i = \bar{\gamma}_i$, the channel becomes an AWGN channel.

The amount of traffic arrival in each time slot $a_i(t)$ is a Poisson random variable with mean λ_i, which is the traffic arrival rate of user i, 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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2645702, IEEE Transactions on Vehicular Technology

We choose the parameter V as 100 which is sufficiently large to obtain a tight bound. During the simulation, we have run a sufficiently large number of time slots in order to ensure that the system converges to its steady state, and the results are collected from the steady state. 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. Single Legitimate Receiver

We assume that the legitimate receiver experiences Rayleigh fading ($m_i = 1$) with mean SNR as 10dB ($\bar{\gamma}_i = 10$dB). By changing the channel setting for the eavesdropper and the arrival rate of the data for the legitimate receiver we can investigate the performance of the secrecy outage probability. The optimal results in the following discussion are obtained based on the solution in Section V-B.

When the eavesdropper experiences a Rayleigh fading channel ($m_e = 1$), the corresponding secrecy outage probability is illustrated in Fig. 3-a. With the increase of the arrival rate λ, the secrecy outage probability increases. However, with different $\bar{\gamma}_e$, *i.e.*, the SNR of the eavesdropper's channel, the increasing speed is different. When $\bar{\gamma}_e = 7$dB, the secrecy outage probability is roughly linear with λ. With a large $\bar{\gamma}_e$, when λ is small, the secrecy outage probability increases quickly w.r.t. λ, and a small increment of λ results in a large secrecy outage probability increase.

When the eavesdropper experiences Nakagami fading with $m_e = 10$, the results are shown in Fig. 3-b. A similar trend as in Fig. 3-a can be observed. But note that when $\bar{\gamma}_e$ is small and λ is also small, the secrecy outage probability is almost zero and is not related to λ.

Fig. 3-c illustrates the secrecy outage probability when the eavesdropper experiences an AWGN channel without fading ($m_e = \infty$). Similar to Fig. 3-b, we can see when λ is small, the system is able to achieve zero secrecy outage, which confirms the analysis in Sec. VI.

From all the above three figures we can see that, Algorithm WSSTRM cannot achieve the optimal secrecy outage probability when the arrival rate is small, which validates our analysis in Sec. V, as when the arrival rate is small, Q_i/Vw_i is not a proper "online representative" of the Lagrangian multiplier. But when the arrival rate is large, Algorithm WSSTRM can achieve the optimal secrecy outage probability, as under this circumstance Q_i/Vw_i can properly represent the Lagrangian multiplier as it is positive. Further note that the curves of Algorithm WSSTRM-R are always overlapped with the curves of the optimal results, which indicates that Algorithm WSSTRM-R is optimal.

C. Multiple Legitimate Receivers

As Algorithm WSSTRM cannot achieve optimality even in a system with a single legitimate receiver, in this subsection, we only discuss Algorithm WSSTRM-R and the optimal results, showing that in the multiple legitimate receivers case, Algorithm WSSTRM-R is also optimal.

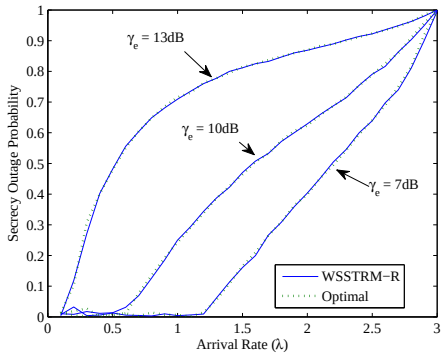


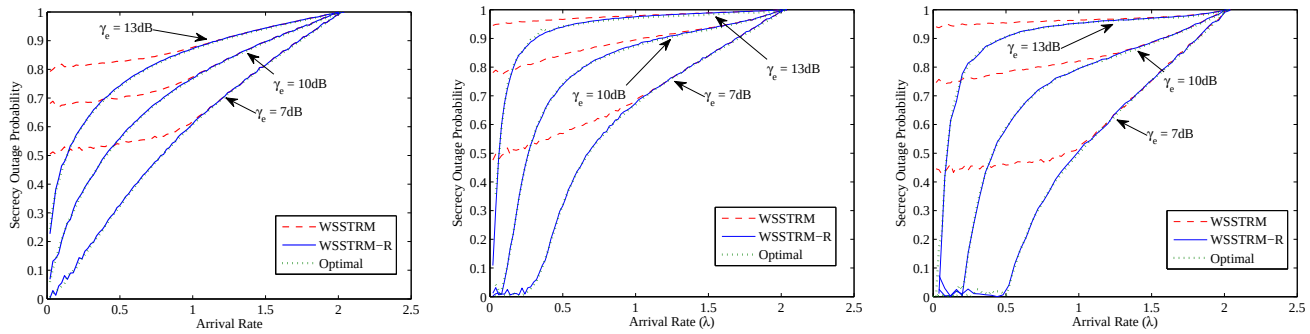
Fig. 4. Secrecy outage probability, multiple legitimate receivers, $\bar{\gamma}_i = 10$dB, $m_i = 1$, $m_e = \infty$

During the simulation, we use $N = 5$, $\boldsymbol{\lambda} = [1, 2, 3, 4, 5]/15 \times \lambda$, where λ is the aggregated arrival rate. We assume that all legitimate receivers experience Rayleigh fading ($m_i = 1$) and have identical $\bar{\gamma}_i = 10$dB. The result that when the eavesdropper experiences an AWGN channel is illustrated in Fig. 4. Firstly, comparing with Fig. 3-c, the trend in Fig. 3-c is preserved in the multiple legitimate receivers case. Furthermore, in the multiple legitimate receivers case, the secrecy outage probability is smaller than that in the single legitimate receiver case when the system is subject to the same arrival rate, because of the capacity increasing thanks to the multi-user diversity. Secondly, the curve of Algorithm WSSTRM-R is overlapped with that of the optimal result suggests that Algorithm WSSTRM-R is an optimal online algorithm in the multi-legitimate-receiver case, and is able to stabilize the queues in the system, achieve reliable communication and minimize the secrecy outage probability.

VIII. Conclusions

In this paper, we investigated the secrecy outage probability in multiuser wireless systems with stochastic traffic. We defined the secrecy outage probability in a system with channel-adaptive transmission rates and secrecy rates, and discussed how to minimize it subject to the communication reliability and queue stability constraints. Stochastic network optimization framework has been used to decompose the problem into an online problem, and an online algorithm WSSTRM was proposed. We further discussed a related offline problem and based on the study of the offline problem, we found that the first proposed online algorithm may not be optimal. Motivated by this, we proposed a refined online algorithm WSSTRM-R. Furthermore, We discussed and analyzed the transmission strategy if the eavesdropper experiences an AWGN channel and further compared the proposed algorithms. Simulation results confirmed that when the traffic load is small, Algorithm WSSTRM is not optimal, but the Algorithm WSSTRM-R is indeed optimal. Several observations were obtained on the relationship between the secrecy outage probability 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 systems using secure communication technologies.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2016.2645702, IEEE Transactions on Vehicular Technology



(a) $m_e = 1$ (b) $m_e = 10$ (c) $m_e = \infty$

Fig. 3. Secrecy outage probability, single legitimate receiver, $\bar{\gamma}_i = 10$dB, $m_i = 1$

REFERENCES

[1] X. Wang, Y. Chen, L. Cai, J. Pan, "Scheduling in a secure wireless network", in *IEEE INFOCOM'14*, 27 April - 2 May 2014.

[2] 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.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515 - 2534, June 2008.

[4] X. Zhou, M. R. McKay, B. Maham, A. Hjrungnes, "Rethinking the secrecy outage formulation: a secure transmission design perspective," *IEEE Communications Letters*, vol. 15, no. 3, pp. 302 - 304, March 2011.

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

[6] 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*, 10-15 April 2011.

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

[8] N. Patwari, S. K. Kasera, "Robust location distinction using temporal link signatures," in *ACM MobiCom'07*, 9-14 Sept. 2007.

[9] J. Zhang, M. H. Firooz, N. Patwari, S. K. Kasera, "Advancing wireless link signatures for location distinction," in *ACM MobiCom'08*, 14-19 Sept. 2008.

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

[11] 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.

[12] 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.

[13] S. Goel, R. Negi, "Secret communication in presence of colluding eavesdroppers", in *IEEE Military Communications Conference 2005*, Oct. 2005.

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

[15] 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.

[16] 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.

[17] 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.

[18] S. K. L.-Y.-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, pp. 451-456, July 1978.

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

[20] 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.

[21] D. Qiao, M. C. Gursoy, S. Velipasalar, "Secure Broadcasting over Fading Channels with Statistical QoS Constraints," in *IEEE GLOBECOM*, 6-10 Dec. 2010

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

[23] C. Koksal, O. Ercetin, and Y. Sarikaya, "Control of wireless networks with secrecy," in *Proc. IEEE ASILOMAR*, 7-10 Nov. 2010.

[24] 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.

[25] 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.

[26] 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.

[27] J. Wang, P. Huang, X. Wang and Y. Yang "Cross-Layer Scheduling for Physical Layer Secrecy and Queue Stability in a Multi-User System," in *IEEE GLOBECOM*, 9-13 Dec. 2013.

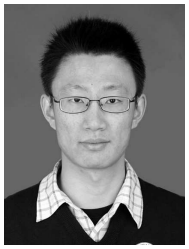
[28] M. J. Neely, "Stochastic network optimization with application to communication and queueing systems," *Synthesis Lectures on Communication Networks*, 2010.

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

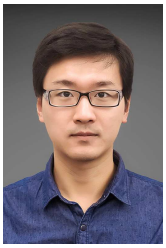
[30] A. Eryilmaz, R. Srikant, J. R. Perkins, "Stable scheduling policies for fading wireless channels," *IEEE/ACM Trans. Networking*, vol. 13, pp. 411-424, April 2005.

[31] S. Meyn, "Stability and asymptotic optimality of generalized MaxWeight policies," *SIAM Journal on Control and Optimization*, vol. 47, pp. 3259-3294, 2009.

[32] A. H. Abd El-Malek, A. M. Salhab, S. A. Zummo, M. Alouini, "Security-Reliability Trade-off Analysis for Multiuser SIMO Mixed RF/FSO Relay Networks with Opportunistic User Scheduling," *IEEE Transactions on Wireless Communications*, no. 99, 2016, to be published.



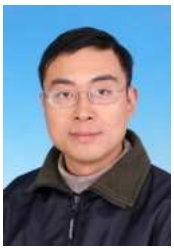
Xuan Wang obtained his Ph.D degree in Electrical Engineering from Department of Electrical and Computer Engineering at the University of Victoria, under the supervision of Prof. Lin Cai. He received the B.Eng. degree in Information Security in 2007 and the M.S. degree in Signal and Information Processing in 2010, both from the Beijing University of Posts and Telecommunications. His research interests include scheduling, resource allocation, and cross-layer design in wireless networks.



Yi Chen (S'14) obtained his Ph.D. degree in Computer Engineering from the Department of Electrical and Computer Engineering at University of Victoria, Canada in 2016, under the supervision of Prof. Lin Cai. He received the B.Eng. degree and M.A.Sc. degree in communications and information engineering from the Northwestern Polytechnical University, Xi'an, China, in 2008 and 2011, respectively. His research interests include scheduling design and resource allocation in wireless networks.

Lin Cai (S'00-M'06-SM'10) received her M.A.Sc. and PhD degrees in electrical and computer engineering from the University of Waterloo, Waterloo, Canada, in 2002 and 2005, respectively. Since 2005, she has been with the Department of Electrical & Computer Engineering at the University of Victoria, and she is currently a Professor. Her research interests span several areas in communications and networking, with a focus on network protocol and architecture design supporting emerging multimedia traffic over wireless, mobile, ad hoc, and sensor networks.

She has been a recipient of the NSERC Discovery Accelerator Supplement Grants in 2010 and 2015, respectively, and the best paper awards of IEEE ICC 2008 and IEEE WCNC 2011. She has served as a TPC symposium co-chair for IEEE Globecom'07, Globecom'10 and Globecom'13, the Associate Editor for IEEE Transactions on Wireless Communications, IEEE Transactions on Vehicular Technology, EURASIP Journal on Wireless Communications and Networking, International Journal of Sensor Networks, and Journal of Communications and Networks (JCN), and the Distinguished Lecturer (DL) of IEEE VTS society.



Jianping Pan (S'96–M'98–SM'08) is currently a professor of computer science at the University of Victoria, Victoria, British Columbia, Canada. He received his Bachelors and PhD degrees in computer science from Southeast University, Nanjing, Jiangsu, China, and he did his postdoctoral research at the University of Waterloo, Waterloo, Ontario, Canada. He also worked at Fujitsu Labs and NTT Labs. His area of specialization is computer networks and distributed systems, and his current research interests include protocols for advanced networking, performance analysis of networked systems, and applied network security. He received the IEICE Best Paper Award in 2009, the Telecommunications Advancement Foundations Telesys Award in 2010, the WCSP 2011 Best Paper Award, the IEEE Globecom 2011 Best Paper Award, the JSPS Invitation Fellowship in 2012, and the IEEE ICC 2013 Best Paper Award, and has been serving on the technical program committees of major computer communications and networking conferences including IEEE INFOCOM, ICC, Globecom, WCNC and CCNC. He is the Ad Hoc and Sensor Networking Symposium Co-Chair of IEEE Globecom 2012 and an Associate Editor of IEEE Transactions on Vehicular Technology. He is a senior member of the ACM and a senior member of the IEEE.