Achieving Full Secrecy Rate with Low Packet Delays: An Optimal Control Approach

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

***Abstract*—We consider a single-user, single-hop wireless communication system, in which data packets arrive at a data queue to be transmitted to a receiver over a block fading channel, privately from an eavesdropper. We assume that the eavesdropper listens to the transmitter over another independently fading channel and that the transmitter only has knowledge of the distribution of the eavesdropper's channel. We propose a joint secrecy rate, transmission, and admission controller based on a simple index policy that only relies on the distribution of the eavesdropper's channel rate. Given any arrival sample path, we show that our controller achieves the maximum possible data admission rate, while keeping the data queue stable as well as meeting an upper bound on the rate of secrecy outage, i.e., the fraction of data packets that are in part or fully decodable by the eavesdropper. While the solution is not unique, i.e., there are other schemes that can achieve the aforementioned performance, we show that our scheme also achieves a low queuing delay for the data packets enqueued at the data queue by striking the correct balance between direct secrecy encoding for data bits and secret key generation and utilization. To obtain this result, our transmission controller makes use of the secret key queue to *smooth out* the variations in the achievable secrecy rate of the associated fading wiretap channel.**[1]

Key Words – physical layer secrecy, key generation, delay

I. Introduction

Motivated by the seminal paper [1], there have been a large number of investigations (e.g., [2]–[8]) on wireless information theoretic secrecy. These studies have significantly enhanced our understanding of the basic limits and principles of the design and the analysis of secure wireless communication systems. Despite the significant progress in information theoretic secrecy, most of the work has focused on physical layer techniques. The application of wireless information theoretic secrecy remains mainly unresolved as it relates to the design of wireless networks and its impact on network control and protocol development. Indeed, our understanding of the interplay between the secrecy requirements and the critical functionalities of wireless networks, such as *scheduling, routing, and congestion control* remains very limited.

To that end, there have been some recent efforts to utilize the insights drawn from the aforementioned investigations on information theoretic secrecy to build secure wireless networks. In [9]–[13] the fundamental capacity and connectivity scaling laws of wireless networks with secrecy have been addressed. In [14], [15], single hop uplink scenario has been considered in which nodes enqueue arriving private and open data packets to be transmitted to a base station over block fading channels. A node is scheduled to transmit information privately from the other nodes and rate is controlled carefully to maximize an overall utility. The solution provided follows up on the stochastic network optimization framework (e.g., as treated in [16]–[20]) and generalizes the uplink scenario to incorporate *secrecy as a quality of service requirement*.

In a separate direction, [21] proposed the idea of using a key queue in a single user system. There, a key queue is kept at the transmitter and the receiver, separately from the data queues. Instead of using the entire instantaneous secrecy rate for information transmission at all times, some of it is utilized to transmit key bits, generated randomly at the transmitter. These stored key bits are used later to secure information bits in such a way that, even when the instantaneous secrecy rate is 0, information bits can still be transmitted to the destination securely from the eavesdropper. Hence, the idea of key sharing allows one to "bank" secrecy rates at certain times to be utilized at other times. It is shown in [22] that, using this idea, a long-term *constant* secrecy rate, identical to the secrecy capacity (expected instantaneous secrecy rate) of the channel is achievable. Thus, [22] addresses decoding delays and does not deal with the dynamics of the data arrival process.

Here, we consider a single-user, single-hop wireless communication system, in which data packets arrive at a data queue to be privately transmitted to the receiver over a block fading channel, from an eavesdropper that listens to the transmitter over another independently fading channel, only the distribution of which is known at the transmitter. We formulate the problem to maximize the long-term data admission rate, subject to the stability of the data queue as well as a bound on the rate of secrecy outage. Here, we define the rate of secrecy outage as the fraction of data packets that are in part or fully decodable by the eavesdropper. A brute-force approach to solving this problem is to try to use the entire channel rate to transmit data and to choose the secrecy encoding rate such that the secrecy outage constraint is met. While this aforementioned brute-force approach indeed leads to a greedy solution that achieves the maximum admission rate and meets the desired constraints, we show that it leads to large delays due to variations in the secrecy rate of the channel. *In this paper, our objective is to develop a class of solutions that achieves not only the maximum admission rate for any arrival sample path, but also a low queuing delay*.

[1] Zhoujia Mao, C. Emre Koksal are with Department of ECE, and Ness B. Shroff is with Deparment of ECE and CSE, The Ohio State University. The manuscript is received on September 15, 2012 and revised on March 1, 2013. This work was in part supported by NSF Grants CNS 0831919, CCF 0916664, and CNS 1054738, CNS 1065136, CNS 1012700, CNS 0831060, and by the Army Research Office through its MURI award W911NF-08-1-0238.

To that end, we propose a joint secrecy rate, transmission, and admission controller based on a simple, easily implementable, index policy. We show that, relative to the greedy solution, our scheme provides a much lower queuing delay for the data packets enqueued at the data queue. To achieve this, our transmission controller introduces two unique features. First, it makes use of the secret key queue to smooth out the variations in the achievable secrecy rate of the associated fading wiretap channel. It chooses the correct balance between direct secrecy encoding for data bits and secret key generation and utilization. Second, it introduces a concave utility function, which is not in the original optimization formulation, and exploits it to engineer the *second order* effects caused by the variability of the secrecy rate. The proposed algorithm is a cross-layer algorithm that combines physical, link, and transport layers. Our scheme strikes the optimal balance between secret key generation and information transmission in order to maximize the network utility. While the cryptographic use of the key bits is via a simple one-time pad, our scheme does not fundamentally rule out other symmetric-key-based secrecy mechanisms.

We also investigate the special case in which perfect information of the eavesdropper's instantaneous channel gain is available to the transmitter. We provide a scheme which is sample-path delay optimal for any given sample path of the arrival and channel gain processes.

To summarize our main contributions in this paper:

- Our work is the first that directly aims to achieve a *low queuing delay* for the private packets that lie in the transmission queues. For this, we use a system that shares random secret key bits simultaneously with information transmission. Here, we develop a novel transmission controller that finds the optimal balance between key and data transmission in order to make the secrecy rate smooth. A unique aspect of our controller is that, it artificially introduces a convex utility function in the solution, which allows for *smoothing* the secrecy rate in time, resulting in lower delays.
- We only assume the knowledge of the distribution of the eavesdropper channel. With this assumption, existing solutions achieve equivocation by encoding across multiple blocks, long enough for sufficient averaging of the eavesdropper channel. However, since our objective is to achieve a low delay, such solutions are not applicable. To that end, our secrecy rate controller chooses the rate at which we encode information in each packet in order to keep the fraction of bits that experience a secrecy outage below a pre-specified threshold.

II. System Model

We consider the single-user system illustrated in Fig. 1, in which the transmitter enqueues data packets to be transmitted to the receiver over the main channel at a fixed power, privately from an eavesdropper that overhears the transmission over a separate channel. Time is slotted, and we assume that the achievable rates (the maximum mutual information between the input and the output) of the main and the eavesdropper channel are stationary and ergodic processes $\vec{R}_m = \{R_m(0), R_m(1), \ldots, R_m(T-1), \ldots\}$ and $\vec{R}_e = \{R_e(0), R_e(1), \ldots, R_e(T-1), \ldots\}$, respectively. We assume that at any time t, the transmitter has causal knowledge of $\vec{R}_m$, i.e., up to time t, but only the distribution of the eavesdropper's channel condition. We also assume that the time slots are long enough for sufficient averaging of the noise, and via Wyner encoding [1], the achievable instantaneous secrecy rate at a given slot t is identical to $R_s(t) = \big(R_m(t) - R_e(t)\big)^+ \in [0, R_m(t)]$, $\forall t \geq 0$, where $(\cdot)^+ = \max[\cdot, 0]$. Let $f\big(R_s(t)|R_m(t)\big)$ denote the conditional distribution of $R_s(t)$, given $R_m(t)$, which can be calculated at the transmitter in each time slot t, using the observation of $R_m(t)$ and $f\big(R_e\big)$. In detail, $f\big(R_s(t)|R_m(t)\big) = f\big(R_m(t) - R_s(t)\big)$, if $0 < R_s(t) < R_m(t)$; $f\big(R_s(t)|R_m(t)\big) = 0$ for all other values of $R_s(t)$.

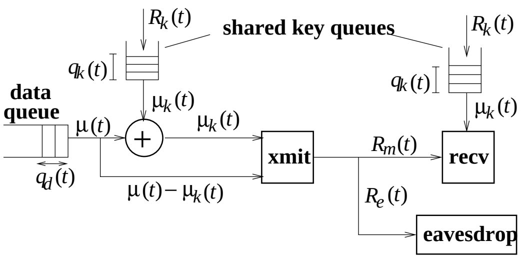


Fig. 1. System model

In any given time slot t, let $\hat{R}_s(t)$ denote the secrecy encoding rate that the secrecy rate controller chooses at time t, i.e., in the secrecy coding structure [1], $\hat{R}_s(t)$ is the number of bits to be transmitted privately, encapsulated by $R_m(t) - \hat{R}_s(t)$ randomization bits. Therefore, if the *actual* secrecy rate is less than the controller's secrecy encoding rate, i.e., $R_s(t) < \hat{R}_s(t)$, then $\hat{R}_s(t) - R_s(t)$ amount of the transmitted data that is supposed to be secure is actually non-secure, which means a *secrecy outage* occurs. We will discuss the implications of a secrecy outage later on. The rate $\hat{R}_s(t)$ is utilized in two possible ways: part of it is used to directly encode data from the data queue and the remaining part is used to transmit randomly generated key bits to be stored at the key queues, both at the transmitter and the receiver (with identical content). The size of the data and the key buffers are assume to be infinite.

As shown in Fig. 1, the amount of total data transmitted at a time t is $\mu(t)$. A part ($\mu_k(t)$ bits) of this data is encrypted using $\mu_k(t)$ key bits by a simple bit-by-bit XOR operation. The remaining $\mu(t) - \mu_k(t)$ bits are secured using the chosen secrecy rate $\hat{R}_s(t)$. Since we assume that $\hat{R}_s(t)$ is fully utilized, the remaining portion not used to secure the current data transmission is used to generate $R_k(t)$ key bits. The data arrivals to the system is represented by the arrival process $\{A(t)\}$. The data queue state is denoted by $q_d(t)$.

The Lindley equation that models the state evolution of the key queue is

$$q_k(t+1) = q_k(t) + R_k(t) - \mu_k(t), \tag{1}$$

where $0 \leq \mu_k(t) \leq q_k(t) + R_k(t)$. In time slot t, $q_k(t)$ is the key queue length, i.e., the amount of key bits. Since $R_k(t)$ is the generated key bits stored in the key queue and $\mu_k(t)$ is the key bits utilized from the key queue, the condition $0 \leq \mu_k(t) \leq q_k(t) + R_k(t)$ ensures that the used key bits should not exceed the instantaneous input key bits and the available key bits in the key queue. We provide an equivalent key queue model in the following lemma along with the constraints that specify the relationships between the parameters.

Lemma 1: Equation (1) that models the evolution of the key queue can be replaced by the state evolution equation $q_k(t+1) = q_k(t) + \hat{R}_s(t) - \mu(t)$ with the constraints $0 \leq \mu_k(t) \leq \mu(t) \leq \min[q_k(t) + \hat{R}_s(t), R_m(t)]$ and $\big(\mu(t) - \mu_k(t)\big) + R_k(t) = \hat{R}_s(t)$.

Proof: Note that the system parameters must satisfy:
(1) $0 \leq \mu_k(t) \leq \mu(t) \leq R_m(t)$: the amount of key bits used to secure data does not exceed the amount of total transmitted data, and the total transmission rate is bounded by the rate of the main channel.
(2) $0 \leq [\mu(t) - \mu_k(t)] + R_k(t) = \hat{R}_s(t) \leq R_m(t)$: the chosen instantaneous secrecy rate is fully utilized: $\mu(t) - \mu_k(t)$ is the amount of transmitted data from the data queue in slot t and the rest of it is used to generate key bits. Furthermore, we know that the secrecy rate cannot exceed the main channel rate, i.e., $0 \leq \hat{R}_s(t) \leq R_m(t)$.
(3) $\mu_k(t) \leq \min\{R_m(t), q_k(t) + R_k(t)\}$: the amount of used key bits cannot exceed the main channel rate, since we cannot send data at a higher rate even if all of it is secured using key bits, i.e., $\mu_k(t) \leq R_m(t)$. Also, we cannot use more key bits than the amount available in the key queue, i.e., $\mu_k(t) \leq q_k(t) + R_k(t)$.
Observation 1: Constraints (1) and (2) directly imply $0 \leq \mu_k(t) \leq \mu(t) \leq R_m(t)$ and $\big(\mu(t) - \mu_k(t)\big) + R_k(t) = \hat{R}_s(t)$.
Observation 2: By Constraints (2) and (3), $\mu(t) = \hat{R}_s(t) - R_k(t) + \mu_k(t) \leq q_k(t) + R_k(t) + \hat{R}_s(t) - R_k(t) = q_k(t) + \hat{R}_s(t)$.
Observation 3: The key state evolution is equivalent to $q_k(t+1) = q_k(t) + R_k(t) - \mu_k(t) = q_k(t) + \hat{R}_s(t) - \mu(t)$ by Constraint (2).

Observations 1,2,3 complete the proof. ■

III. Problem Formulation

If at any given slot t, the secrecy encoding rate is larger than the actual secrecy rate, i.e., $\hat{R}_s(t) > R_s(t)$, information is leaked to the eavesdropper in that time slot, which we refer to as a secrecy outage. Given the posterior distribution $f\big(R_s(t)|R_m(t)\big)$ of the secrecy rate given sample value of the main channel rate, the expected number of non-secure bits generated in slot t is

$$\begin{aligned}&\big(R_k(t) + \mu(t) - \mu_k(t)\big)\Pr\big(\hat{R}_s(t) > R_s(t)|R_m(t)\big)\\ =&\big(R_k(t) + \mu(t) - \mu_k(t)\big)\Big[1\\ &- \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big].\end{aligned}$$

By Lemma 1, we have $\hat{R}_s(t) = R_k(t) + \mu(t) - \mu_k(t)$, and the resulting non-secure bits in slot t are

$$\hat{R}_s(t)\Big[1 - \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big].$$

In the long run, we need to keep the average number of non-secure bits (and thus the fraction of bits experiencing a secrecy outage) bounded by a small predetermined threshold.

We assume a general data arrival process, $\{A(t)\}$ at the input of the data queue. In slot t, only a portion, $R(t)$, of all the arrivals are admitted into the data queue in order to keep the data queue stable and the average number of non-secure bits bounded. All the admitted packets are required to be served by the system eventually. Our objective is to maximize the long-term average admitted data rate. Our problem can be formally described as follows:

$$(A) \qquad \max_{\vec{R},\vec{\mu},\vec{\mu}_k,\vec{R}_k} \quad \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} R(t)$$

$$\begin{aligned}\textit{s.t.}\quad & q_d(t+1) = (q_d(t) - \mu(t))^+ + R(t), && (2)\\ & q_k(t+1) = q_k(t) + \hat{R}_s(t) - \mu(t), && (3)\\ & 0 \leq R(t) \leq A(t), && (4)\\ & 0 \leq \mu_k(t) \leq \mu(t) \leq \min[q_k(t) + \hat{R}_s(t), R_m(t)], && (5)\\ & \limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} q_d(t) < \infty, && (6)\\ & \limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \hat{R}_s(t)\Big[1 -\\ & \qquad \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big] \leq \eta, && (7)\\ & \big(\mu(t) - \mu_k(t)\big) + R_k(t) = \hat{R}_s(t), && (8)\end{aligned}$$

where Constraint (2) describes the data queue evolution with $R(t)$ as the arrival process and $\mu(t)$ as the service process. Constraint (3) describes the equivalent key queue evolution as in Lemma 1. Constraint (4) bounds the actual amount, $R(t)$, of data injected into the data queue by the available amount of data $A(t)$ at time t. Constraint (5) states that the amount of transmitted data is bounded by both the main channel rate and the amount of keys available, and the amount of key bits used to secure data does not exceed the amount of transmitted data. Constraint (6) guarantees data queue stability. Recall that $\hat{R}_s(t)\Big[1 - \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big]$ is the transmitted non-secure data bits in time slot t. Then constraint (7) states that the long-term average rate of non-secure bits should be bounded by the predetermined threshold η, where η is a QoS parameter that gives the maximum tolerable average secrecy outage rate when the eavesdropper's channel is not perfectly known. Constraint (8) ensures that the secrecy encoding rate is fully utilized by the transmission of data and generation of key bits. Note that the maximum achievable admission rate, which happens to be the objective function here, is upper bounded by the maximum average secrecy encoding rate $\hat{R}_s^{\text{ave}} \triangleq \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \hat{R}_s(t)$.

As we will show, there exists a solution for Problem (A), for which $R_k(t) = 0$ for all t, i.e., without requiring the use a key queue. However, we will also show that our solution that involves the careful control of the key queue leads to a smoother service for the admitted data, and consequently lower queueing delays. Next, we introduce virtual queues that we will use in our control scheme.

Virtual Queues: In order to keep the average rate of non-secure bits per time slot bounded by η, we construct the following virtual queue of non-secure bits:

$$\tilde{q}_s(t+1) = \Big(\big(\tilde{q}_s(t) - \eta\big)^+ + \hat{R}_s(t)\Big[1 - \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big) dR_s(t)\Big]\Big)^+. \quad (9)$$

We will show later that by keeping this virtual queue stable, Constraint (7) on the non-secure bits is satisfied (similar ideas of utilizing virtual queue are used in [20], [23]).

To ensure that the secrecy rate does not fluctuate dramatically in time (that keeping delays low), we do not want the key queue to be drained frequently. We define $\tilde{q}_k$ as the virtual key queue and reduce key outage by making the virtual key queue stable. The virtual key queue evolves according to the following equation:

$$\tilde{q}_k(t+1) = \Big((\tilde{q}_k(t) - \epsilon)^+ + \mu(t) - \hat{R}_s(t) + 1_o(t) \Big)^+, \quad (10)$$

where $0 < \epsilon < \infty$ can be chosen arbitrarily, and

$$1_o(t) = \begin{cases} 0 & \text{if } \mu(t) = 0 \text{ or } \mu(t) < q_k(t) + \hat{R}_s(t) \\ 1 & \text{otherwise} \end{cases} \quad (11)$$

is the indicator that the key queue visits the 0 state from a non-zero state in slot t. This happens when all the available and newly generated secret key bits are used in slot t. Without loss of generality, the initial state $\tilde{q}_k(0)$ can be set to be zero.

IV. Control Algorithm and Performance Analysis

In this section, we provide a simple control algorithm, analyze its performance, and show that it is provably optimal for Problem (A) described in the previous section.

A. Algorithm

The algorithm comprises of three components: a *secrecy rate control* component, a *transmission control* component and a *admission control* component. Our algorithm uses a constant control parameter, V, which can take on any value in $\Re^+$.

Secrecy Rate Control (SRC): In slot t, the controller chooses the secrecy encoding rate as follows:

$$\hat{R}_s(t) = \arg \max_{0 \le \hat{R} \le R_m(t)} \frac{V}{2}\hat{R} - \tilde{q}_s(t)\hat{R}\Big[1 - \int_{\hat{R}}^{R_m(t)} f\big(R_s(t)|R_m(t)\big) dR_s(t)\Big]. \quad (12)$$

Note that Equation (12) is a single variable nonlinear program. We can compute all stationary points and find the maximizer among the stationary points and boundary points. If a stationary point exist, it must belong to the root set of the equation the first derivative of the objective function equated to 0. The root finding algorithms such as Newton's method can be found in [24] to compute the roots of the derivative equated to 0 efficiently.

Transmission Control (TC): In slot t, the controller solves the following optimization problem and transmits with the calculated rate:

$$\mu(t) = \arg \max_{\mu \in \Pi(t)} \frac{V}{2} U\big(\mu\big) - \tilde{q}_k(t)\mu, \quad (13)$$

where $\Pi(t) = \{\mu(t) : 0 \le \mu(t) \le \min[q_k(t) + \hat{R}_s(t), R_m(t)]\}$ is a compact and nonempty set. Note that the stationary points of $\frac{V}{2}U\big(\mu\big) - \tilde{q}_k(t)\mu$ can be found by using root finding of equation $\frac{V}{2}U'(\mu) - \tilde{q}_k(t) = 0$, then the maximizer can be found among the stationary and boundary points. Especially, when $U(\mu)$ is strictly concave in μ and the inverse function of $U'(\mu)$ is known, Equation (13) has an analytical solution

$$\mu(t) = \max\Big[0, \min\big[U'^{-1}(\frac{2\tilde{q}_k(t)}{V}), \min[q_k(t) + \hat{R}_s(t), R_m(t)]\big]\Big].$$

Key generation and usage rates $\big(R_k(t), \mu_k(t)\big)$ are chosen as follows: If the required transmission rate is larger than the secrecy encoding rate, i.e., $\mu(t) > \hat{R}_s(t)$, then we do not generate new key bits $R_k(t) = 0$ and use $\mu_k(t) = \mu(t) - \hat{R}_s(t)$ amount of key bits in the key queue to secure the transmission that the secrecy rate can not support. If the required transmission rate is less than the secrecy encoding rate, i.e., $\mu(t) \le \hat{R}_s(t)$, then there is no need to use the stored key bits in the key queue $\mu_k(t) = 0$ and the remaining $R_k(t) = \hat{R}_s(t) - \mu(t)$ amount of secrecy rate can be used to generate new key bits into the key queue. This ensures that constraints $\big(\mu(t) - \mu_k(t)\big) + R_k(t) = \hat{R}_s(t)$ and $\mu_k(t) \le \mu(t)$ of Problem (A) are satisfied. Note that, either key generation or key usage is zero, i.e., $\mu_k(t)R_k(t) = 0$ for all t, since any solution with $\mu_k(t) > 0$ and $R_k(t) > 0$, can be equivalently replicated by using the secrecy rate to transmit data rather than generating and using key bits at the same time.

Admission Control (AC): In slot t, the controller solves the following optimization problem and admits the calculated amount of data arrivals:

$$R(t) = \arg \max_{0 \le R \le A(t)} \frac{V}{2} U\big(R\big) - q_d(t)R. \quad (14)$$

One of the unique features of our scheme is that, we introduce a "utility function," $U(\cdot)$, which was not a part of the original problem formulation but is part of the solution. This is done to achieve the desired level of "fairness" in times, i.e., smoothness of $R_s(t)$ that will lead to lower delays. We do not specify this function beforehand, but if $U(\cdot)$ is concave, the objective function (the average data admission rate) also turns out to be a concave function of $\mu(t)$. Consequently, *TC* solves a simple convex optimization problem in each time slot. The positive term $\frac{V}{2}U\big(\mu(t)\big)$ can be viewed as a utility obtained from the transmission rate $\mu(t)$ and the term $\tilde{q}_k(t)\mu(t)$ can be viewed as its associated cost. When the virtual key queue $\tilde{q}_k(t)$ is small, *TC* tries to allocate a large amount of transmitted data to increase the utility; and when $\tilde{q}_k(t)$ is large, *TC* allocates a small amount of transmitted data to reduce cost. This pushes the served data rate, controlled by the virtual queue $\tilde{q}_k(t)$ to be relatively smooth over time.

It is also notable that (13) does not involve the key generation and the key usage rates, which are chosen subsequently. Finally, we would like to emphasize that all components are *index policies*, i.e., the solutions are memoryless and they depend only on the instantaneous values of the system variables and the distribution of the eavesdropper's channel rate.

B. Performance Analysis

Recall that $A(t)$ is the original data arrival process and $R(t)$ is the amount of data injected into the data queue at slot t. The natural question one would ask here is, whether our admission controller rejects too many packets in the first place to *synthetically* keep the data queue stable and average non-secure bits bounded. In the following theorem, we show that this is not the case. Indeed, the admission rate associated with *SRC*, *AC*, and *TC* can be made closer to the optimum by increasing the control parameter V. We use the notation $y = O(x)$ to represent y going to 0 as x goes to 0.

Theorem 1: If
1) $U(\cdot)$ is strictly concave on $\Re^+ \bigcup \{0\}$, and its slope at 0 satisfies[2] $0 \leq \beta = U'(0) < \infty$,
2) $0 \leq \limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} A^2(t) < \infty$ and $0 \leq R_m(t) \leq R_{max} < \infty,\ \forall t \geq 0$,
3) $\int_0^t f\big(R_s(t)|R_m(t)\big)dR_s(t) > 0$ if $t > 0$ given any $R_m(t)$ in any slot t,
then *SRC*, *TC*, and *AC* achieve:

$$\limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \hat{R}_s(t)\Big[1 - \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big] \leq \eta, \tag{15}$$

$$q_d(t) \leq \beta\frac{V}{2}, \quad \forall\ t \geq 0 \tag{16}$$

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} R(t) \rightarrow \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} R^*(t) \ \textit{as}\ V \rightarrow \infty, \tag{17}$$

where $\vec{R}^* = \{R^*(0), R^*(1), \ldots, R^*(T-1), \ldots\}$ is the optimal solution to Problem (A).

Corollary 1: With conditions 1)-3) as in Theorem 1, the algorithms *SRC*, *TC*, and *AC* achieve:

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \hat{R}_s(t) \geq \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \hat{R}'_s(t) - O(\frac{1}{V}), \tag{18}$$

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U\big(R(t)\big) \geq \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U\big(R'(t)\big) - O(\frac{1}{V}), \tag{19}$$

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U\big(\mu(t)\big) \geq \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U\big(\mu'(t)\big) - O(\frac{1}{V}), \tag{20}$$

where $\vec{\hat{R}}'_s = \{\hat{R}'_s(0), \hat{R}'_s(1), \ldots, \hat{R}'_s(T-1), \ldots\}$, $\vec{\mu}' = \{\mu'(0), \mu'(1), \ldots, \mu'(T-1), \ldots\}$ and $\vec{R}' = \{R'(0), R'(1), \ldots, R'(T-1), \ldots\}$ are optimal solutions to Problem (A) with objectives $\max_{\vec{\hat{R}}_s} \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \hat{R}_s(t)$, $\max_\mu \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U\big(\mu(t)\big)$ and $\max_R \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U\big(R(t)\big)$, respectively.

Corollary 2: If there is no key queue, i.e., the transmission controller *TC* is replaced by $\mu(t) = \hat{R}_s(t),\ \forall t$, then with conditions 2)-3) as in Theorem 1, the algorithms *SRC* and *AC* can still achieve Equations (15)-(19), but Equation (20) is no longer achieved.

The proof of Theorem 1, Corollary 1 and Corollary 2 can be found in Appendix A. All three conditions stated in Theorem 1 are merely technical and they are all reasonable. Condition 1) focuses on strictly concave utility functions with a finite derivative 0 (e.g., $\log(1+x)$). Condition 2) limits the second moment of the arrivals in each slot. Condition 3) states that there is a probability mass at $R_s(t) = 0$, for any given $R_m(t)$. Equation (15) implies that the average non-secure bits are bounded and Equation (16) shows that the data queue is kept stable under our algorithm. In Equation (17), the gap between the average admission rate with our algorithm and the optimal average admission rate can be made arbitrarily small by choosing parameter V large. As a tradeoff, the data queue length increases as V increases. From Equation (18) we can see that our algorithm achieves the maximum achievable admission rate (i.e., the average secrecy encoding rate), and when combined with Eq. (19) and (20), we see that the scheme achieves this optimal point in a way in which the data injection rate and the service rate are smooth over time. This is unlike the case without the data queue, where the variations in the secrecy rate are reflected to the service. Based on this observation, we expect the queueing delay to be smaller with a key queue, which we will verify in Section VI using numerical examples.

V. Sample Path Optimal Policy for Minimizing Time-Average Queue Length with Perfect Eavesdropper Information

In this section we focus on the degenerate case when the transmitter also has perfect knowledge of the main and eavesdropper's channel. For this case, we will provide a scheme that is also delay optimal in a very strong sample path sense. Given any general time varying rate process $\vec{R}_m = \{R_m(0), R_m(1), \ldots, R_m(T-1), \ldots\}$ and $\vec{R}_e = \{R_e(0), R_e(1), \ldots, R_e(T-1), \ldots\}$ for the main and the eavesdropper channel respectively, an arrival sample path $\vec{A} = \{A(0), A(1), \ldots, A(T-1), \ldots\}$ is admissible if there exists a transmission and key management policy such that the resulting time-averaged queue length is finite, i.e., $\limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} q_d(t) < \infty$. In this section, we assume $\vec{R}_e$ and $\vec{R}_s$ are perfectly known to the transmitter and study on the delay performance of our system. We limit our attention to only admissible arrival processes and assume no admission control, i.e., all arrivals are admitted to the system. Next, we specify the *work-conserving policy*, μ, for transmission control and show that it achieves the minimum queue length $q_d(t)$ in every time slot t, for any sample path for the channel rates $\vec{R}_m$,

[2] For instance, $U(1+R) = \log(1+R)$.

$\vec{R}_e$, and any associated admissible arrival process, $\vec{A}$. Hence, the work conserving policy is the sample path optimal policy queue size minimization.

Work conserving policy serves the data queue at rate $\mu(t)$, generates keys at rate $R_k(t)$ and utilizes keys at rate $\mu_k(t)$ at time t, where

$$\mu(t) = \min\{q_d(t) + A(t), q_k(t) + R_s(t), R_m(t)\},$$
$$\mu_k(t) = \begin{cases} 0, & \text{if } \mu(t) \le R_s(t) \\ \mu(t) - R_s(t), & \text{otherwise} \end{cases}$$
$$R_k(t) = \begin{cases} 0, & \text{if } \mu(t) > R_s(t) \\ R_s(t) - \mu(t), & \text{otherwise} \end{cases} \tag{21}$$

This policy satisfies all the constraints of the equivalent model characterized in Lemma 1. The work conserving policy allocates as high a service rate to the data queue as the channel rates and the amount of key bits available allows. If the data queue is empty, the available secrecy rate is not wasted and key bits are generated and stored in the key queue.

Theorem 2: The work conserving policy, μ, is sample-path optimal for minimizing the queue size in every time slot.
Proof: The proof is provided in Appendix B.

VI. Numerical Evaluation

In this section we simulate our algorithms and numerically compare them with the optimal performance. In the simulation, the number of time slots used is $T = 10^6$. We use the utility function $U(x) = \log(1+x),\ \forall x \ge 0$. The channel states follow a Markov chain. In each time slot, the channel rates have two possible states: In state 1, the main channel rate follows Rayleigh distribution $f(R_m) = \frac{R_m}{\sigma_1^2} e^{-\frac{R_m^2}{2\sigma_1^2}}$ and the generated sample value is known to the transmitter. The eavesdropper channel rate also follows Rayleigh distribution $f(R_e) = \frac{R_e}{\sigma_1^2} e^{-\frac{R_e^2}{2\sigma_1^2}}$ but the resulting sample value is not known to the transmitter. Then, the posterior distribution of R_s given R_m is $f\big(R_s|R_m\big) = \frac{R_m - R_s}{\sigma_1^2} e^{-\frac{(R_m - R_s)^2}{2\sigma_1^2}}$ for $0 < R_s \le R_m$, and $\Pr\big(R_s = 0|R_m\big) = \int_{R_m}^{\infty} \frac{t}{\sigma_1^2} e^{-\frac{t^2}{2\sigma_1^2}} dt$; Similarly in state 2, the main channel rate follows Rayleigh distribution $f(R_m) = \frac{R_m}{\sigma_2^2} e^{-\frac{R_m^2}{2\sigma_2^2}}$ and the generated sample value is known to the transmitter. The eavesdropper channel rate also follows Rayleigh distribution $f(R_e) = \frac{R_e}{\sigma_2^2} e^{-\frac{R_e^2}{2\sigma_2^2}}$ but the resulting sample value is not known to the transmitter. The posterior distribution of R_s given R_m is then $f\big(R_s|R_m\big) = \frac{R_m - R_s}{\sigma_2^2} e^{-\frac{(R_m - R_s)^2}{2\sigma_2^2}}$ for $0 < R_s \le R_m$, and $\Pr\big(R_s = 0|R_m\big) = \int_{R_m}^{\infty} \frac{t}{\sigma_2^2} e^{-\frac{t^2}{2\sigma_2^2}} dt$. The transition probability matrix of the Markov channels is $[0.8, 0.2; 0.7, 0.3]$. We also set the bound on the average rate of non-secure bits per slot $\eta = 0.3$ and the virtual key queue parameter $\epsilon = 0.01$.

Real-life Internet traffic is typically characterized using heavy tailed behavior. For example, heavy-tailed distributions such as Zipf, have been found to accurately model the amount of traffic between distinct domains in the Internet [25]. Hence, in the first scenario, we used the Zipf law: the number of packets arriving in each time slot $A(t),\ t \ge 0$ follows a Zeta distribution with parameter 3.5. We choose $\sigma_1 = 1.5$ and $\sigma_2 = 3$ for the Rayleigh parameter in two channel states. We run the simulation for different values of the control coefficient V and compare the results with the optimal value[3]. Figure 2 (a) shows that, as V increases, the average admission rate (both with and without a key queue) increases to the optimum, which is consistent with Equation (17). In Figure 2 (b), we plot the tail distribution of instantaneous queue length where the control parameter V is 2000 and the Y-axis is $\log$ scaled. We can see that with a key queue, the proportion of time slots with larger queue length is smaller than that without a key queue since the curve without a key queue has heavier tail. Furthermore, the average queueing delay performance with a key queue is also better than that without a key queue, as we can see in Figure 2 (c) and (d). From Figure 2 (c) and (d), we can see that as we choose $V = 2000$ (average admission rate approaches its optimal value 1.19), the average queue length with a key queue is 3.5, which is 1 less than that without a key queue. Therefore, there is a 30% improvement of average queue length with a key queue.

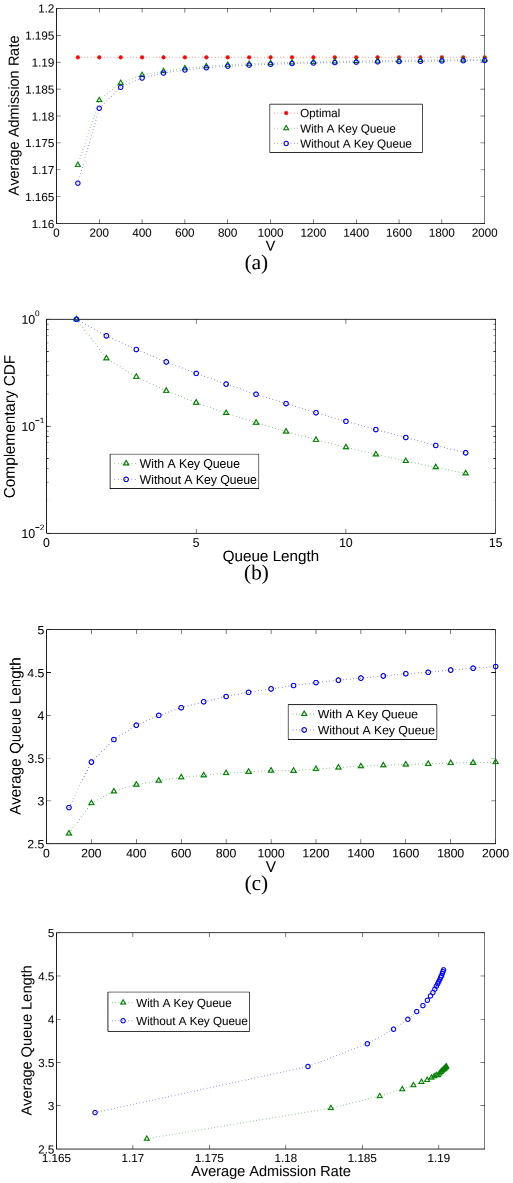
Figure 3 illustrates the scenario with a real traffic trace (traces of LAN and WAN traffic seen on an Ethernet from Internet traffic archive http://ita.ee.lbl.gov/html/traces.html). We choose $\sigma_1 = 2$ and $\sigma_2 = 5$ for the Rayleigh parameter in two channel states. Figure 3 (a) shows that, as V increases, the average admission rate (both with and without a key queue) increases to the optimum, which is consistent with Equation (17). In Figure 3 (b), we plot the tail distribution of instantaneous queue length where the control parameter V is 60 and the Y-axis is $\log$ scaled. We can see that with a key queue, the proportion of time slots with larger queue length is smaller than that without a key queue since the curve without a key queue has heavier tail. From Figure 3 (c) and (d), we can see that as we choose $V = 60$ (average admission rate is 1.85), the average queue length with a key queue is 5.3, which is 0.5 less than that without a key queue. Therefore, there is a 10% improvement of average queue length with a key queue in this scenario.

Note that the reason for using data queues at the input of wired/wireless links is to average out the variability in the arrival and the service processes. In our system, as well as a data queue, we use a key queue, whose function is to average out the variations in the secrecy rate of the wiretap channel. Intuitively, by averaging out the variations of the secrecy rate using a key queue in a variable channel, the queueing delay performance will be improved.

VII. Conclusion

In this paper, we consider a single-user, single-hop wireless communication system, in which data packets arrive at a data queue to be transmitted to a receiver over a block fading channel, privately from an eavesdropper. We assume that the eavesdropper listens to the transmitter over another independently fading channel and that the transmitter only has knowledge of the distribution of the eavesdropper's channel.

[3] Note that the optimal value for Problem (A) is $\min[\bar{A}, \hat{R}_s^{\text{ave}}]$.



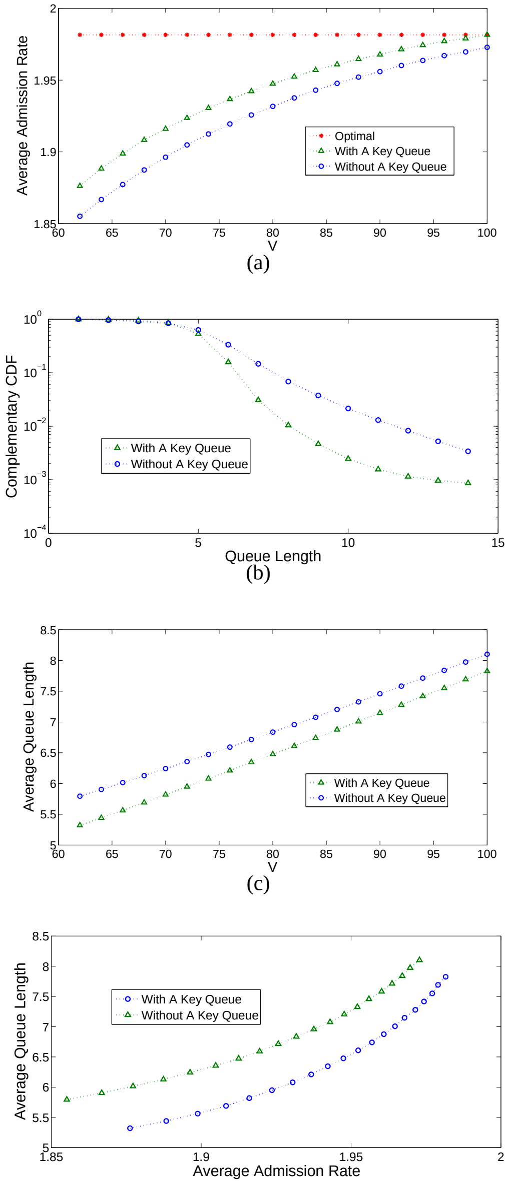
(a)

(b)

(c)

(d)

Fig. 2. Performance of *AC* and *TC* related to the solution of Problem (A) under Heavy-tailed Traffic: (a) Control Parameter V v.s. Average Admission Rate; (b) Tail distribution of instantaneous queue length; (c) Control parameter V v.s. Average Queue Length; (d) Admission Rate (Throughput) v.s. Average Queue length (Delay) Curve



(a)

(b)

(c)

(d)

Fig. 3. Performance Evaluation of *TC* and *AC* for Problem (A) under Real Traffic Trace

We propose a joint secrecy rate, transmission, and admission controller based on simple index policies. We show that our controller achieves the maximum possible data admission rate, while keeping the data queue stable as well as meeting an upper bound on the rate of secrecy outage given any arrival sample path. Also, we illustrate via simulations that the use of a key queue reduces the *queuing delay* for the data packets, while serving packets that are admitted at the maximum admissible rate. This is due to the fact that, the transmission controller is designed to choose the rate of served packets as uniformly over time as possible. Finally, for admissible arrival processes and perfect eavesdropper's information, we showed that the work conserving policy is sample-path optimal for time-averaged queue size.

References

[1] A. D. Wyner, "The Wire-Tap Channel," *The Bell System Technical Hournal*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[2] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[3] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symposium Inform. Theory*, Seattle, WA, July 2006, pp. 356–360.

[4] D. Gunduz, R. Brown, and H. V. Poor, "Secret communication with feedback," in *Proc. IEEE Intl. Symposium on Information Theory and its Applications*, Auckland, New Zealand, Dec. 2008.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088 – 3104, July 2010.

[6] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[7] E. Ekrem and S. Ulukus, “The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel,” Mar. 2009, submitted.

[8] M. Yuksel, X. Liu, and E. Erkip, “A secure communication game with a relay helping the eavesdropper,” Taormina, Italy, Oct 2009.

[9] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, “On secrecy capacity scaling in wireless networks,” vol. 58, no. 5, pp. 3000–3015, May 2012.

[10] ——, “On the effect of colluding eavesdroppers on secrecy scaling,” in *Proceedings of European Wireless, EW*, Lucca, Italy, 2010.

[11] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, “Modeling location uncertainty for eavesdroppers: A secrecy graph approach,” Austin, TX, June 2010.

[12] S. Vasudevan, D. Goeckel, and D. F. Towsley, “Security-capacity trade-off in large wireless networks using keyless secrecy,” Chicago, IL, September 2010.

[13] A. Sarkar and M. Haenggi, “Secrecy coverage,” Pacific Grove, CA, Nov. 2010.

[14] C. E. Koksal and O. Ercetin, “Control of wireless networks with secrecy,” in *”Asilomar Conference on Signals, Systems, and Computers”*, Pacific Grove, CA, Nov. 2010.

[15] C. E. Koksal, O. Ercetin, and Y. Sarikaya, “Control of wireless networks with secrecy,” *IEEE/ACM Transactions on Networking*, 2012, to appear.

[16] L. Tassiulas and A. Ephremides, “Jointly optimal routing and scheduling in packet ratio networks,” *IEEE Transactions on Information Theory*, vol. 38, no. 1, pp. 165 –168, Jan. 1992.

[17] X. Liu, E. K. P. Chong, and N. B. Shroff, “A framework for opportunistic scheduling in wireless networks,” *Computer Networks*, vol. 41, no. 4, pp. 451–474, 2003.

[18] X. Lin and N. B. Shroff, “The Impact of Imperfect Scheduling on Cross-Layer Congestion Control in Wireless Networks,” *IEEE/ACM Transactions on Networking*, vol. 14, no. 2, pp. 302–315, April 2006.

[19] A. Eryilmaz and R. Srikant, “Joint Congestion Control, Routing and MAC for Stability and Fairness in Wireless Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 1514–1524, August 2006.

[20] M. J. Neely, “Energy Optimal Control for Time Varying Wireless Networks,” *IEEE Transactions on Information Theory*, vol. 52, no. 7, pp. 2915–2934, July 2006.

[21] K. Khalil, M. Youssef, O. O. Koyluoglu, and H. El Gamal, “On the delay limited secrecy capacity of fading channels,” Seoul, Korea, June - July 2009.

[22] O. Gungor, J. Tan, C. E. Koksal, H. El Gamal, and N. B. Shroff, “Joint power and secret key queue management for delay limited secure communication,” San Diego, CA, March 2010.

[23] Z. Mao, C. E. Koksal, and N. B. Shroff, “Near Optimal Power and Rate Control of Multi-hop Sensor Networks with Energy Replenishment: Basic Limitations with Finite Energy and Data Storage,” *IEEE Transactions on Automatic Control*, vol. 57, no. 4, pp. 815–829.

[24] J. Stoer and R. Bulirsch, *Introduction to numerical analysis 2nd Edition*. Springer-Verlag New York Inc., 1993.

[25] A. Feldmann, N. Kammenhuber, O. Maennel, B. Maggs, R. D. Prisco, and R. Sundaram., “A Methodology for Estimating Interdomain Web Traffic Demand,,” *In IMC*, 2004.

APPENDIX A
PROOF OF THEOREM 1, COROLLARY 1 AND COROLLARY 2

Proof of Equation (15): Note that *SRC* chooses $\hat{R}_s(t)$ that maximizes $\frac{V}{2}\hat{R}_s(t) - \tilde{q}_s(t)\hat{R}_s(t)\Big[1 - \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big]$ which means $\frac{V}{2}\hat{R}_s(t) - \tilde{q}_s(t)\hat{R}_s(t)\Big[1 - \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big] \geq 0$ since $0 \leq R_s(t) \leq R_m(t)$.

Since the secrecy encoding rate is counted in data bits, if $\hat{R}_s(t) > 0$, then $\hat{R}_s(t) \geq 1$. By condition 3) stated in Theorem 1, $1 - \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)] \geq \int_0^1 f\big(R_s(t)|R_m(t)\big)\ dR_s(t)] > 0$ if $\hat{R}_s(t) > 0$. Let $\gamma \triangleq \min_t \int_0^1 f\big(R_s(t)|R_m(t)\big)dR_s(t)] > 0$. Without loss of generality, let $\tilde{q}_s(0) \leq \frac{V}{2\gamma}$. Suppose for all $t \geq 1$, $\tilde{q}_s(t-1) \leq \frac{V}{2\gamma}$ holds. In slot t, if $\hat{R}_s(t) = 0$, then $\tilde{q}_s(t) \leq \tilde{q}_s(t-1) \leq \frac{V}{2\gamma}$ by Equation (9). Otherwise, $\hat{R}_s(t) > 0$, and we then have $\tilde{q}_s(t) \leq \frac{V}{2\Big[1-\int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big]} \leq \frac{V}{2\gamma}$. We can then conclude that $\tilde{q}_s(t) < \frac{V}{2\gamma},\ \forall t \geq 0$, and $\lim_{T\to\infty}\frac{\tilde{q}_s(T)}{T} = 0$. From Equation (9), we have

$$\tilde{q}_s(t+1) \geq \tilde{q}_s(t) - \eta + \hat{R}_s(t)\Big[1- \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big].$$

By adding from 0 to $T-1$, dividing by T and taking $\limsup$ on both sides, we have

$$\lim_{T\to\infty}\frac{\tilde{q}_s(T)}{T} \geq \lim_{T\to\infty}\frac{\tilde{q}_s(0)}{T} - \eta + \limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\hat{R}_s(t) \Big[1 - \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big],$$

i.e., $\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\hat{R}_s(t)\Big[1 - \int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big] \leq \eta$.

Note that this result is not related to *TC* and Equation (15) holds for both with or without key queue. ■

Proof of Equation (16): Equation (16) directly follows from the following lemma:

Lemma 2: Under algorithm *AC* and *TC*, we have

$$q_d(t) \leq \frac{\beta V}{2}, \quad \tilde{q}_k(t) \leq \frac{\beta V}{2}.$$

Proof: Since $U(\cdot)$ is concave on $\Re^+\bigcup\{0\}$, we have $U\big(\mu(t)\big) \leq U(0) + \beta\mu(t),\ \forall t \geq 0$, where $0 \leq \beta = U'(0) < \infty$. Then, $\frac{V}{2}U\big(\mu(t)\big) - \tilde{q}_k(t)\mu(t) \leq \frac{V}{2}U(0) + \frac{\beta V}{2}\mu(t) - \tilde{q}_k(t)\mu(t)$ where $\mu(t)$ is the solution of *TC*.

If $\frac{\beta V}{2}\mu(t) - \tilde{q}_k(t)\mu(t) < 0$, then we get $\frac{V}{2}U\big(\mu(t)\big) - \tilde{q}_k(t)\mu(t) < \frac{V}{2}U(0)$. However, *TC* chooses $\mu(t)$ that maximizes $\frac{V}{2}U\big(\mu(t)\big) - \tilde{q}_k(t)\mu(t)$ which means $\frac{V}{2}U\big(\mu(t)\big) - \tilde{q}_k(t)\mu(t) \geq \frac{V}{2}U(0)$ since $0 \in \Pi(t)$. Then, we must have $\frac{\beta V}{2}\mu(t) - \tilde{q}_k(t)\mu(t) \geq 0$, i.e.,

$$\tilde{q}_k(t)\mu(t) \leq \frac{\beta V}{2}\mu(t). \tag{22}$$

We now prove the result by induction. Without loss of generality, let $\tilde{q}_k(0) \leq \frac{\beta V}{2}$. Suppose for all $t \geq 1$, $\tilde{q}_k(t-1) \leq \frac{\beta V}{2}$ holds. In slot t, if $\mu(t) = 0$, then $\tilde{q}_k(t) \leq \tilde{q}_k(t-1) \leq \frac{\beta V}{2}$ by Equation (10) and Equation (11). Otherwise, $\mu(t) \neq 0$, and by Equation (22), we have $\tilde{q}_k(t) \leq \frac{\beta V}{2}$.

$q_d(t) \leq \frac{\beta V}{2}$ can be obtained using the same argument and it holds for both with and without key queue since it is only related to *AC*. ■

Proof of Equation (18): We define the Lyapunov function $L(\tilde{q}_s(t)) = (\tilde{q}_s(t))^2$ and $\Delta(\tilde{q}_s(t)) = L(\tilde{q}_s(t+1)) - L(\tilde{q}_s(t))$.

From Equation (9), we have

$$\begin{aligned}\big(\tilde{q}_s(t+1)\big)^2 \le&\big(\tilde{q}_s(t)-\eta\big)^2 + 2\tilde{q}_s(t)\hat{R}_s(t)\Big[1- \\ &\int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big] + R_{max}^2 \\ \le&\big(\tilde{q}_s(t)\big)^2 + 2\tilde{q}_s(t)\hat{R}_s(t)\Big[1- \\ &\int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big] - 2\eta\tilde{q}_s(t) \\ &+ \eta^2 + R_{max}^2,\end{aligned}$$

and

$$\begin{aligned}&\Delta(\tilde{q}_s(t)) \\ \le& V\hat{R}_s(t) - 2\bigg\{\frac{V}{2}\hat{R}_s(t) - \tilde{q}_s(t)\hat{R}_s(t)\Big[1- \\ &\int_{\hat{R}_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big]\bigg\} \\ &- 2\eta\tilde{q}_s(t) + \eta^2 + R_{max}^2 \\ \le& V\hat{R}_s(t) - 2\bigg\{\frac{V}{2}\hat{R}'_s(t) - \tilde{q}_s(t)\hat{R}'_s(t)\Big[1- \\ &\int_{\hat{R}'_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big]\bigg\} \\ &- 2\eta\tilde{q}_s(t) + \eta^2 + R_{max}^2 \\ \le& V\hat{R}_s(t) - V\hat{R}'_s(t) + 2\tilde{q}_s(t)\bigg\{\hat{R}'_s(t)\Big[1- \\ &\int_{\hat{R}'_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big] - \eta\bigg\} \\ &+ \eta^2 + R_{max}^2,\end{aligned} \tag{23}$$

since $0 \le \hat{R}'_s(t) \le R_m(t)$.

Lemma 3:

$$\begin{aligned}&\frac{1}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\tilde{q}_s(t)\bigg\{\hat{R}'_s(t)\Big[1- \\ &\int_{\hat{R}'_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big] - \eta\bigg\} \le O(\frac{1}{V}).\end{aligned}$$

Proof: Note that

$$\begin{aligned}&\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\bigg\{\hat{R}'_s(t)\Big[1- \\ &\int_{\hat{R}'_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big] - \eta - \delta\bigg\} < 0.\end{aligned} \tag{24}$$

Construct an auxiliary queue with the following evolution:

$$\begin{aligned}\bar{q}_s^*(t+1) = \Big(\bar{q}_s^*(t) - \eta - \delta\Big)^+ + \hat{R}'_s(t)\Big[1- \\ \int_{\hat{R}'_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big],\end{aligned}$$

then with Equation (24) and by applying Lemma 2 in [23], $\bar{q}_s^*(t)$ is strongly stable. Using the idea similar to [20], we have the fact that if any queue represented with $Q(t)$ is strongly stable, then $\limsup_{T\to\infty}\frac{Q(T)}{T} = 0$. Therefore, we have $\limsup_{T\to\infty}\frac{\bar{q}_s^*(T)}{T}$. By multiplying $\tilde{q}_s(t)$ for both sides of the inequality $\bar{q}_s^*(t+1) \ge \bar{q}_s^*(t) - \eta - \delta + \hat{R}'_s(t)\Big[1 - \int_{\hat{R}'_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big]$ and rearranging terms, we obtain $\tilde{q}_s(t)\bigg\{\hat{R}'_s(t)\Big[1 - \int_{\hat{R}'_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big] - \eta\bigg\} \le \tilde{q}_s(t)\Big[\bar{q}_s^*(t+1) - \bar{q}_s^*(t) + \delta\Big]$. By summing from 0 to $T-1$, dividing by T and taking $\limsup_{T\to\infty}$, we have

$$\begin{aligned}&\frac{1}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\tilde{q}_s(t)\bigg\{\hat{R}'_s(t)\Big[1- \\ &\int_{\hat{R}'_s(t)}^{R_m(t)} f\big(R_s(t)|R_m(t)\big)dR_s(t)\Big] - \eta\bigg\} \\ \le&\frac{1}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=1}^{T}\bar{q}_s^*(t)\big(\tilde{q}_s(t-1) - \tilde{q}_s(t)\big) + \\ &+ \frac{1}{V}\limsup_{T\to\infty}\frac{\tilde{q}_s(T)\bar{q}_s^*(T) - \tilde{q}_s(0)\bar{q}_s^*(0)}{T} \\ &+ \limsup_{T\to\infty}\frac{1}{T}\sum_{t=1}^{T}\frac{\tilde{q}_s(t)}{V}\delta \\ \le&\frac{R_{max}+\eta}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\bar{q}_s^*(t) + \frac{\delta}{V}\frac{V}{2\gamma} = O(\frac{1}{V}) + \frac{\delta}{2\gamma},\end{aligned}$$

since the average queue length of the auxiliary queue remains stable and is not related to V, and $\tilde{q}_s(t) < \frac{V}{2\gamma}$, $\forall t$ from the proof of Equation (15). By letting $\delta \to 0$, we finish the proof. ■

By summing from 0 to $T-1$, dividing by T and V, taking $\liminf_{T\to\infty}$ over Equation (23), combined with Lemma 3, we obtain Equation (18). ■

Proof of Equation (20): We define $L(\tilde{q}_k(t)) = (\tilde{q}_k(t))^2$ and $\Delta(\tilde{q}_k(t)) = L(\tilde{q}_k(t+1)) - L(\tilde{q}_k(t))$. From Equation (10), we have

$$\begin{aligned}\big(\tilde{q}_k(t+1)\big)^2 \le&\big(\tilde{q}_k(t)-\epsilon\big)^2 + \big(\mu(t) - \hat{R}_s(t) + 1_o(t)\big)^2 \\ &+ 2\big(\tilde{q}(t)-\epsilon\big)^+\big(\mu(t) - \hat{R}_s(t) + 1_o(t)\big) \\ \le&\big(\tilde{q}_k(t)\big)^2 + \epsilon^2 + \big(1 + R_{max}\big)^2 + 2\epsilon R_{max} \\ &+ 2\tilde{q}_k(t)1_o(t) + 2\tilde{q}_k(t)\mu(t) - 2\tilde{q}_k(t)\hat{R}_s(t),\end{aligned}$$

then

$$\begin{aligned}&\Delta(\tilde{q}_k(t)) \\ \le& VU\big(\mu(t)\big) - VU\big(\mu(t)\big) + \epsilon^2 + \big(1 + R_{max}\big)^2 + 2\epsilon R_{max} \\ &+ 2\tilde{q}_k(t)1_o(t) + 2\tilde{q}_k(t)\mu(t) - 2\tilde{q}_k(t)\hat{R}_s(t) \\ \le& VU\big(\mu(t)\big) + \epsilon^2 + \big(1 + R_{max}\big)^2 + 2\epsilon R_{max} + \beta V1_o(t) \\ &- 2\left[\frac{V}{2}U\big(\mu(t)\big) - \tilde{q}_k(t)\mu(t)\right] - 2\tilde{q}_k(t)\hat{R}_s(t).\end{aligned}$$

It is apparent that *TC* is trying to maximize the value of the term $\left[\frac{V}{2}U\big(\mu(t)\big)-\tilde{q}_k(t)\mu(t)\right]$. Since the optimal solution for Problem (A) with objective $\max_\mu \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U\big(\mu(t)\big)$ may not be unique, we let $\mathcal{U}'$ be the optimal solution set and $\vec{\mu}'\in\mathcal{U}'$ be any optimal solution, for Problem (A) with objective $\max_\mu \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U\big(\mu(t)\big)$ given any sample path. Since the constraint set $\Pi(t)$ is queue dynamic related, it is possible that $\mu'(t)\notin\Pi(t)$.

Lemma 4: In slot t, if by solving *TC*, we get $\left[\frac{V}{2}U\big(\mu(t)\big)-\tilde{q}_k(t)\mu(t)\right]<\left[\frac{V}{2}U\big(\mu'(t)\big)-\tilde{q}_k(t)\mu'(t)\right]$, then $\mu(t)<\mu'(t)$ and $\mathit{1}_o(t')=1$ for some $t'\le t$ and $t-t'<\infty$.

Proof: In time slot t, let $\mu^m(t)$ be the value that maximize the unconstrained objective function $\frac{V}{2}U(\mu(t))-\tilde{q}_k(t)\mu(t)$.
Claim 1: $q_k(t)+\hat{R}_s(t)\le R_m(t)$. Otherwise, $\Pi(t)=[0,R_m(t)]$ which is not queue dynamic related, then $\left[\frac{V}{2}U\big(\mu(t)\big)-\tilde{q}_k(t)\mu(t)\right]\ge\left[\frac{V}{2}U\big(\mu'(t)\big)-\tilde{q}_k(t)\mu'(t)\right]$.
Claim 2: $\mu^m(t),\mu'(t)>q_k(t)+\hat{R}_s(t)$. If $\mu^m(t),\mu'(t)\in\Pi(t)$, we must have $\left[\frac{V}{2}U\big(\mu(t)\big)-\tilde{q}_k(t)\mu(t)\right]\ge\left[\frac{V}{2}U\big(\mu'(t)\big)-\tilde{q}_k(t)\mu'(t)\right]$, then $\mu'(t)>q_k(t)+\hat{R}_s(t)$. If $\mu^m(t)<0$, we will have $\frac{V}{2}U(0)=\left[\frac{V}{2}U\big(\mu(t)\big)-\tilde{q}_k(t)\mu(t)\right]\ge\left[\frac{V}{2}U\big(\mu'(t)\big)-\tilde{q}_k(t)\mu'(t)\right]$, then $\mu^m(t)>q_k(t)+\hat{R}_s(t)$.

By the above claims, $\mu(t)<\mu'(t)$ and $\mu(t)<\mu^m(t)$. Suppose $\mu(t)<q_k(t)+\hat{R}_s(t)$, since the objective function of *TC* is concave in $\mu(t)$, we can increase $\mu(t)$ to increase the objective without violating the constraint. Thus, $\mu(t)=q_k(t)+\hat{R}_s(t)$ and $\mathit{1}_o(t)=1$. It is also possible that $\mathit{1}_o(t')=1$ for some $t'<t$ and $\hat{R}_s(\tau)=0,\ \forall\tau\in[t',t]$. Note that $t-t'<\infty$, otherwise, $\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\hat{R}_s(t)=0$ which contradicts Equation (18). ■

Let $N=\max\{n:\ \textit{for any}\ t\ge0,\ \hat{R}_s(\tau)=0,\ \forall\tau\in[t,t+n]\}$. By using Lemma 4 and $\mu(t),\mu'(t)\le R_m(t)\le R_{\mathit{max}},\ \forall t\ge0$, we have $N<\infty$ and

$$\begin{aligned}\Delta\le&VU\big(\mu(t)\big)-VU\big(\mu'(t)\big)+\epsilon^2+\big(1+R_{\mathit{max}}\big)^2+\\&2\epsilon R_{\mathit{max}}+2\tilde{q}_k(t)\Big[\mu'(t)-\hat{R}_s(t)\Big]+\\&V(\beta+NU(R_{\mathit{max}}))\mathit{1}_o(t).\end{aligned}\tag{25}$$

Lemma 5:

$$\frac{1}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\tilde{q}_k(t)[\mu'(t)-\hat{R}_s(t)]\le O(\frac{1}{V}).$$

Proof: Note that even the optimal solution should satisfy the conservation rule

$$\sum_{t=0}^{T-1}\mu'(t)-\left[q_k(0)+\sum_{t=0}^{T-1}\hat{R}'_s(t)\right]\le0,$$

then

$$\sum_{t=0}^{T-1}\Big(\mu'(t)-\hat{R}'_s(t)-\frac{\delta}{2}\Big)<q_k(0),$$

where δ can be arbitrarily small. By divided by T and taking $\limsup_{T\to\infty}$ of both sides, we have $\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\Big(\mu'(t)-\hat{R}'_s(t)-\frac{\delta}{2}\Big)<0$. Similar to the proof of Equation (18), we can obtain $\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\Big(\hat{R}'_s(t)-\hat{R}_s(t)-\frac{\delta}{2}-O(\frac{1}{V})\Big)<0$. Therefore,

$$\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\Big(\mu'(t)-\hat{R}_s(t)-\delta-O(\frac{1}{V})\Big)<0.\tag{26}$$

Construct an auxiliary queue with the following evolution:

$$\bar{q}^*_k(t+1)=\Big(\bar{q}^*_k(t)-\hat{R}_s(t)-\delta-O(\frac{1}{V})\Big)^+ +\mu'(t),$$

then with Equation (26) and by applying Lemma 2 in [23], $\bar{q}^*_k(t)$ is strongly stable. The remaining argument is similar as in Lemma 3. ■

Lemma 6: If $\tilde{q}_k(t)\le\frac{\beta V}{2}$, then $q_k(t)\le\beta\frac{V}{2}$.

Proof: First, we provide a rough idea of the proof: by exploring the relations between $\tilde{q}_k(t)$ and $q_k(t)$, we notice that as $q_k(t)$ increases from 0 to at most $\beta\frac{V}{2}$, $\tilde{q}_k(t)$ will hit zero at some slot. Once $\tilde{q}_k(t)$ becomes zero, *TC* results in $\mu(t)=\min[q_k(t)+\hat{R}_s(t),R_m(t)]$. Since $\hat{R}_s(t)\le R_m(t)$, $q_k(t)$ will either be zero or decrease. We now give the proof details.

Without loss of generality, let $q_k(0)=0$. We have the following cases:
i) if $\mu(t)\ge\hat{R}_s(t)$, $\mathit{1}_o(t)=0$ and $\tilde{q}_k(t)>0$, then $q_k(t+1)\le q_k(t)$ and $\tilde{q}_k(t+1)-\tilde{q}_k(t)\le q_k(t)-q_k(t+1)$, i.e., even if $\tilde{q}_k(t)$ increases, the increment is no larger than the decrement of $q_k(t)$;
ii) if $\mu(t)<\hat{R}_s(t)$, $\mathit{1}_o(t)=0$, then if $\tilde{q}_k(t+1)>0$, $\tilde{q}_k(t)-\tilde{q}_k(t+1)\ge q_k(t+1)-q_k(t)$, i.e., the decrement of $\tilde{q}_k(t)$ is no less than the increment of $q_k(t)$, else if $\tilde{q}_k(t+1)=0$, it goes to case iv);
iii) if $\mathit{1}_o(t)=1$, then $q_k(t+1)=0$ by Equation (3) and Equation (11);
iv) if $\tilde{q}_k(t)=0$, by Equation (13), *TC* chooses $\mu(t)=\min[q_k(t)+\hat{R}_s(t),R_m(t)]$, then either $q_b(t+1)=0$, or $q_k(t+1)=q_k(t)-R_m(t)+\hat{R}_s(t)\le q_k(t)$.

From the above discussion, we have $q_k(t)\le\beta\frac{V}{2}$. ■

Lemma 7: If both the key queue $q_k(t)$ and virtual key queue $\tilde{q}_k(t)$ are strongly stable, i.e.,

$$\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\big(q_k(t)+\tilde{q}_k(t)\big)<\infty,$$

then $\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\mathit{1}_o(t)\le\epsilon$.

Proof: By Lemma 2 and Lemma 6, $\limsup_{T\to\infty}\frac{q_k(T)}{T}=\limsup_{T\to\infty}\frac{\tilde{q}_k(T)}{T}=0$. From Equation (10), we have

$$\tilde{q}_k(t+1)\ge\tilde{q}_k(t)-\epsilon+\mathit{1}_o(t)+\mu(t)-\hat{R}_s(t).$$

Note that $q_k(t+1)=q_k(t)-\mu(t)+\hat{R}_s(t)$. By adding from 0 to $T-1$, dividing by T and taking $\limsup$ on both sides, we have

$$\begin{aligned}\limsup_{T\to\infty}\frac{\tilde{q}_k(T)}{T}\ge&\lim_{T\to\infty}\frac{\tilde{q}_k(0)}{T}-\epsilon+\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\mathit{1}_o(t)\\&+\lim_{T\to\infty}\frac{q_k(0)-q_k(T)}{T}.\end{aligned}$$

Since $\limsup_{T\to\infty}\frac{\tilde{q}_k(T)}{T}=\lim_{T\to\infty}\frac{\tilde{q}_k(0)}{T}=$

$\lim_{T\to\infty}\frac{q_k(0)}{T} = \lim_{T\to\infty}\frac{q_k(T)}{T} = 0$, so we get $\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1} 1_o(t) \leq \epsilon$. ■

By summing from 0 to $T-1$, dividing by T and V, taking $\liminf_{T\to\infty}$ over Equation (25), combined with Lemma 2, Lemma 5, Lemma 6, and Lemma 7, we get

$$\begin{aligned}\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(\mu(t)) \geq& \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(\mu'(t)) - O(\frac{1}{V})\\ &- \epsilon(NU(R_{max})+\beta).\end{aligned}$$

By letting $\epsilon \to 0$, we obtain Equation (20). ■

Proof of Equation (17) and Equation (19): We define $L(q_d(t)) = (q_d(t))^2$, and $\Delta(q_d(t)) = L(q_d(t+1)) - L(q_d(t))$. By Equation (2), we have

$$\begin{aligned}\Delta =& \Delta(q_d(t)) \leq VU(R(t)) - 2\left[\frac{V}{2}U(R(t)) - q_d(t)R(t)\right]\\ &+ A^2(t) + R_{max}^2 - 2q_d(t)\mu(t) \qquad (27)\end{aligned}$$

$$\begin{aligned}(P1) \qquad & \max_{\vec{R}}\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R(t)\\ (P2) \qquad & \max_{\vec{R}}\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(R(t))\\ \textit{s.t.} \qquad & q_d(t+1) = \big(q_d(t)-\mu(t)\big)^+ + R(t),\\ & 0 \leq R(t) \leq A(t),\\ & \limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\big[\hat{R}_s(t)-\mu(t)\big] = 0,\\ & \limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}q_d(t) < \infty,\end{aligned}$$

Lemma 8: (P1) and (P2) have different objective functions under the same set of constraints. Let $\vec{R}^*$ be a maximizer of (P2), then it is also a maximizer of (P1).

Proof: Suppose there exists $\vec{R}_1^*$ such

$$\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R^*(t) < \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R_1^*(t),$$

then there exists $\vec{R}_2^*$ such that $R^*(t) \leq R_2^*(t) \leq A(t),\ \forall t \geq 0$ and

$$\begin{aligned}\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R^*(t) <& \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R_2^*(t)\\ \leq& \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R_1^*(t).\end{aligned}$$

i.e., there are infinitely many slots in which $R^*(t) - R_2^*(t) < 0$. Since $U(\cdot)$ is strictly concave, $U(R^*(t)) - U(R_2^*(t)) < \beta_m(R^*(t) - R_2^*(t)) < 0$ if $R^*(t) - R_2^*(t) < 0$, where $0 < \beta_m = \min\{\frac{U(R^*(t))-U(R_2^*(t))}{R^*(t)-R_2^*(t)} :\ R^*(t) - R_2^*(t) < 0\}$. Thus,

$$\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(R^*(t)) < \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(R_2^*(t)),$$

which contradicts the fact that $\vec{R}^*$ is a maximizer of (P2). ■

Note that $q_k(t+1) = q_k(t) + \hat{R}_s(t) - \mu(t)$. Then by summing from 0 to $T-1$, dividing by T and applying Lemma 6, we have the fact that *TC* with a key queue results into

$$\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\big[\hat{R}_s(t)-\mu(t)\big] = 0, \qquad (28)$$

For the scenario without a key queue, Equation (28) trivially holds since $\mu(t) = \hat{R}_s(t),\ \forall t$. Problem (A) is then reduced to (P1). By Lemma 8, $\vec{R}^*$ is also the maximizer of Problem (A). Substituting $R^*(t)$ into Equation (27), we obtain

$$\begin{aligned}\Delta \leq& VU(R(t)) - VU(R^*(t)) + A^2(t) + R_{max}^2\\ &+ 2q_d(t)\Big[R^*(t) - \mu(t)\Big].\end{aligned}$$

Note that $\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\big[R^*(t) - \hat{R}'_s(t))\big] \leq 0$ and $\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}A^2(t) < \infty$. combining with Equation (28), Equation (18) and using the similar arguments as in Lemma 3 and Lemma 5, we have

$$\frac{1}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}q_d(t)[R^*(t)-\mu(t)] \leq O(\frac{1}{V}).$$

Then, we further obtain

$$\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(R(t)) \geq \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(R^*(t)) - O(\frac{1}{V}),$$

where $\vec{R}^*$ is the maximizer of (P2), (P1) and Problem (B). Note that $\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(R(t)) \leq \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(R^*(t))$ due to the optimality of $\vec{R}^*$. By letting $V \to \infty$, $\vec{R}$ is also a maximizer of (P2). By applying Lemma 8 again, we have

$$\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R(t) \to \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R^*(t) \textit{ as } V \to \infty. \qquad ■$$

APPENDIX B
PROOF OF THEOREM 2

It is sufficient to show that $\forall t \geq 0$, the policy gives the smallest queue length among all policies, i.e., $q_d^{\mu}(t) \leq q_d^{\gamma}(t),\ \forall t \geq 0$ for any policy γ, where q_d^{μ} and q_d^{γ} are the data queue sizes under policy μ and γ, respectively. We show this by induction. Initially, the data queue is empty, i.e., $q_d(0) = q_k(0) = 0$.

I) Clearly, $q_d^{\mu}(1) \leq q_d^{\gamma}(1)$ is true regardless of the channel rates and the number of arrivals at time $t = 1$.

II) Suppose $q_d^{\mu}(T) \leq q_d^{\gamma}(T)$ for $T \geq 1$. Under policy μ, the queue evolution follows:

$$\begin{aligned}q_d^{\mu}(t+1) =& q_d^{\mu}(t) - \mu(t) + A(t),\\ q_k^{\mu}(t+1) =& q_k^{\mu}(t) - \mu(t) + R_s(t),\end{aligned}$$

and for policy γ, the queue evolution follows:

$$\begin{aligned}q_d^{\gamma}(t+1) =& \Big(q_d^{\gamma}(t) - \gamma(t)\Big)^+ + A(t),\\ q_k^{\gamma}(t+1) =& q_k^{\gamma}(t) - \gamma(t) + R_s(t).\end{aligned}$$

Thus, we have

$$\begin{aligned} q_d^{\mu}(T) &= \sum_{t=0}^{T-1} A(t) - \sum_{t=0}^{T-1} \mu(t), \\ q_k^{\mu}(T) &= \sum_{t=0}^{T-1} R_s(t) - \sum_{t=0}^{T-1} \mu(t), \\ q_d^{\gamma}(T) &\geq \sum_{t=0}^{T-1} A(t) - \sum_{t=0}^{T-1} \gamma(t), \\ q_k^{\gamma}(T) &= \sum_{t=0}^{T-1} R_s(t) - \sum_{t=0}^{T-1} \gamma(t), \end{aligned}$$

which implies

$$\begin{aligned} q_k^{\mu}(T) + R_s(T) =& \sum_{t=0}^{T} R_s(t) - \sum_{t=0}^{T} A(t) \\ &+ q_d^{\mu}(T) + A(T), \qquad (29) \\ q_k^{\gamma}(T) + R_s(T) \leq& \sum_{t=0}^{T} R_s(t) - \sum_{t=0}^{T} A(t) \\ &+ q_d^{\gamma}(T) + A(T). \qquad (30) \end{aligned}$$

(i) If $\sum_{t=0}^{T} R_s(t) \leq \sum_{t=0}^{T} A(t)$, then

$$\begin{aligned} \mu(T) =& \min\{q_k^{\mu}(T) + R_s(T), R_m(T)\}, \\ \gamma(T) \leq& \min\{q_k^{\gamma}(T) + R_s(T), R_m(T)\}, \end{aligned}$$

and we also have

$$\begin{aligned} q_d^{\mu}(T+1) =& q_d^{\mu}(T) - \mu(T) + A(T), \\ q_d^{\gamma}(T+1) \geq& q_d^{\gamma}(T) - \gamma(T) + A(T), \end{aligned}$$

then combine with Equation (29) and (30), we have

$$\begin{aligned} & q_d^{\mu}(T+1) - q_d^{\gamma}(T+1) \\ \leq& q_d^{\mu}(T) - q_d^{\gamma}(T) + \gamma(T) - \mu(T) \qquad (31) \\ \leq& q_k^{\mu}(T) - q_k^{\gamma}(T) + \gamma(T) - \mu(T), \qquad (32) \end{aligned}$$

(i.1) when $q_k^{\gamma}(T) + R_s(T) \leq R_m(T)$ and $q_k^{\mu}(T) + R_s(T) \leq R_m(T)$, then continue from Equation (32), we have

$$\begin{aligned} & q_d^{\mu}(T+1) - q_d^{\gamma}(T+1) \\ \leq& q_k^{\mu}(T) - q_k^{\gamma}(T) + q_k^{\gamma}(T) + R_s(T) - \mu(T) \\ =& q_k^{\mu}(T) - q_k^{\gamma}(T) + q_k^{\gamma}(T) - q_k^{\mu}(T) = 0. \end{aligned}$$

(i.2) when $q_k^{\gamma}(T) + R_s(T) \leq R_m(T)$ and $q_k^{\mu}(T) + R_s(T) > R_m(T)$, then continue from Equation (31), we have

$$\begin{aligned} & q_d^{\mu}(T+1) - q_d^{\gamma}(T+1) \\ \leq& q_d^{\mu}(T) - q_d^{\gamma}(T) + q_k^{\gamma}(T) + R_s(T) - \mu(T) \\ =& q_d^{\mu}(T) - q_d^{\gamma}(T) + q_k^{\gamma}(T) + R_s(T) - R_m(T) \\ \leq& q_d^{\mu}(T) - q_d^{\gamma}(T) \leq 0, \end{aligned}$$

by the hypothesis.

(i.3) when $q_k^{\gamma}(T) + R_s(T) > R_m(T)$ and $q_k^{\mu}(T) + R_s(T) \leq R_m(T)$, then continue from Equation (32), we have

$$\begin{aligned} & q_d^{\mu}(T+1) - q_d^{\gamma}(T+1) \\ \leq& q_k^{\mu}(T) - q_k^{\gamma}(T) + R_m(T) - \mu(T) \\ <& q_k^{\mu}(T) - q_k^{\gamma}(T) + q_k^{\gamma}(T) + R_s(T) - \mu(T) \\ =& q_k^{\mu}(T) - q_k^{\gamma}(T) + q_k^{\gamma}(T) + R_s(T) - q_k^{\mu}(T) - R_s(T) = 0. \end{aligned}$$

(i.4) when $q_k^{\gamma}(T) + R_s(T) > R_m(T)$ and $q_k^{\mu}(T) + R_s(T) > R_m(T)$, then continue from Equation (31), we have

$$\begin{aligned} & q_d^{\mu}(T+1) - q_d^{\gamma}(T+1) \\ \leq& q_d^{\mu}(T) - q_d^{\gamma}(T) + R_m(T) - \mu(T) \\ =& q_d^{\mu}(T) - q_d^{\gamma}(T) + R_m(T) - R_m(T) \leq 0. \end{aligned}$$

Thus, $q_d^{\mu}(T+1) \leq q_d^{\gamma}(T+1)$ if $\sum_{t=0}^{T} R_s(t) \leq \sum_{t=0}^{T} A(t)$.

(ii) If $\sum_{t=0}^{T} R_s(t) > \sum_{t=0}^{T} A(t)$, then

$$\begin{aligned} \mu(T) =& \min\{q_d^{\mu}(T) + A(T), R_m(T)\}, \\ \gamma(T) \leq& \min\{q_k^{\gamma}(T) + R_s(T), R_m(T)\}, \end{aligned}$$

(ii.1) when $q_d^{\mu}(T)+A(T) \leq R_m(T)$, we have $\mu(T) = q_d^{\mu}(T)+A(T)$, and $q_d^{\mu}(T+1) = 0 \leq q_d^{\gamma}(T+1)$.

(ii.2) when $q_d^{\mu}(T) + A(T) > R_m(T)$, then

$$\begin{aligned} & q_d^{\mu}(T+1) - q_d^{\gamma}(T+1) \\ \leq& q_d^{\mu}(T) - q_d^{\gamma}(T) + \gamma(T) - R_m(T) \\ \leq& 0 + R_m(T) - R_m(T) = 0. \end{aligned}$$

Thus, $q_d^{\mu}(T+1) \leq q_d^{\gamma}(T+1)$ if $\sum_{t=0}^{T} R_s(t) > \sum_{t=0}^{T} A(t)$ as well. ■

Zhoujia Mao received the B.S. degree from the University of Science and Technology of China. He is currently working toward the Ph.D. degree in the Department of Electrical and Computer Engineering, The Ohio State University. His research interests include wireless networks, resource allocation, scheduling and optimization.

C. Emre Koksal (IEEE senior member) received the B.S. degree in electrical engineering from the Middle East Technical University, Ankara, Turkey, in 1996, and the S.M. and Ph.D. degrees in electrical engineering and computer science from Massachusetts Institute of Technology (MIT), Cambridge, in 1998 and 2002, respectively. He was a Postdoctoral Researcher in the Electrical Engineering and Computer Science Department, MIT, and in the School of Communication and Computer Sciences, EPFL, Lausanne, Switzerland, until 2006. Since then, he has been an Assistant Professor in the Electrical and Computer Engineering Department at The Ohio State University. His general areas of interest are wireless communication, information theory, and communication networks. Dr. Koksal is the recipient of the National Science Foundation CAREER Award, the OSU College of Engineering Lumley Research Award, and the co-recipient of an HP LabsCInnovation Research Award, all in 2011. The paper he coauthored was a best student paper candidate in ACM MobiCom 2005. Since 2013, he has been an Assciate Editor for IEEE Transactions on Wireless Communications and Elsevier Computer Networks.

Ness B. Shroff (S91 / M93 / SM01/ F07) received his Ph.D. degree in Electrical Engineering from Columbia University in 1994. He joined Purdue university immediately thereafter as an Assistant Professor in the school of ECE. At Purdue, he became Full Professor of ECE in 2003 and director of CWSA in 2004, a university-wide center on wireless systems and applications. In July 2007, he joined The Ohio State University, where he holds the Ohio Eminent Scholar endowed chair professorship in Networking and Communications, in the departments of ECE and CSE. From 2009-2012, he served as a Guest Chaired professor of Wireless Communications at Tsinghua University, Beijing, China, and currently holds an honorary Guest professor at Shanghai Jiaotong University in China. His research interests span the areas of communication, social, and cyberphysical networks. He is especially interested in fundamental problems in the design, control, performance, pricing, and security of these networks. Dr. Shroff is a past editor for IEEE/ACM Trans. on Networking and the IEEE Communication Letters. He currently serves on the editorial board of the Computer Networks Journal, IEEE Network Magazine, and the Networking Science journal. He has chaired various conferences and workshops, and co-organized workshops for the NSF to chart the future of communication networks. Dr. Shroff is a Fellow of the IEEE and an NSF CAREER awardee. He has received numerous best paper awards for his research, e.g., at IEEE INFOCOM 2008, IEEE INFOCOM 2006, Journal of Communication and Networking 2005, Computer Networks 2003 (two of his papers received runner-up awards at IEEE INFOCOM 2005 and IEEE INFOCOM 2013), and also student best paper awards (from all papers whose first author is a student) at IEEE WiOPT 2012 and IEEE IWQoS 2006.