Joint Power and Secret Key Queue Management for Delay Limited Secure Communication

Onur Gungor, Jian Tan, Can Emre Koksal, Hesham El Gamal, Ness B. Shroff

Department of Electrical and Computer Engineering
The Ohio State University, Columbus, 43210

***Abstract*—In recent years, the famous *wiretap channel* has been revisited by many researchers and information theoretic secrecy has become an active area of research in this setting. In this paper, we design a wireless communication system that achieves constant bit rate data transmission over a block fading channel, securely from an eavesdropper that listens to the transmitter over another independent block fading channel. It is well known that, the method of sending secure information using the binning techniques inspired by the wiretap channel fails to secure the information at times when the eavesdropper channel has favorable conditions over the main channel. This phenomenon is called *secrecy outage*. In our system, however, we exploit the times at which the main channel is favorable over the eavesdropper channel for us to be able to transmit some *random secret key* bits along with the data bits. These key bits are stored in a separate key buffer at the transmitter as well as the receiver, and are utilized to secure data bits, whenever the channel conditions favor the eavesdropper. We show that, using our system the outage probability can be made arbitrarily close to 0 by jointly controlling the key buffer with the transmit power. We show that the optimal power control involves a time sharing between *secure waterfilling* and *channel inversion* strategies and the key buffer needs to operate in the *heavy traffic regime* to achieve the maximum delay limited rate possible, under a small outage constraint. This work can be viewed as a first step in providing a framework that combines both information theory and queueing analysis for the study of information theoretic security.**

I. Introduction

Secure communication is a topic that is becoming increasingly important thanks to the proliferation of wireless devices. There have been many applied *encryption* mechanisms proposed to secure data communication. However, as new schemes are being developed, methods to counter the specific encryption methods also appear. This competing effect makes **information theoretic secrecy** a very attractive area of research because it can provide hard guarantees that can not be overcome regardless of the computation power of the devices. For example, the famous **wiretap channel** of Wyner [1] have been revisited recently by many researchers. In a wiretap channel, an eavesdropper *passively* listens to the communication between a transmitter and a receiver over a separate communication channel. Wyner defined the **secrecy capacity** of the main channel as the maximum data rate achievable subject to a zero mutual information between the message and the signal received by the eavesdropper. Hence, information theoretic secrecy is "completely secure," i.e., the message cannot be decoded at the eavesdropper, even with unlimited computational power.

For the Additive White Gaussian Noise (AWGN) channel, it was shown in [2] that the secrecy capacity is the difference between the channel capacity of the main channel and the eavesdropper channel. If the eavesdropper channel has a higher channel gain, information theoretic secure communication is not possible over the main channel. For fading channels, on the other hand, it was shown in [5] that secure communication may be maintained at non-zero rate, even when the eavesdropper channel has favorable conditions on average. The transmitter simply exploits the times when the main channel has a higher gain than the eavesdropper channel, to obtain a positive secrecy rate. At all other times, a positive secrecy rate cannot be achieved, resulting in **secrecy outage**.

In this paper, we design a wireless communication system that achieves constant bit rate data transmission over a block fading channel, securely from an eavesdropper that listens to the transmitter over another independent block fading channel. The channel gains of the main channel and the eavesdropper channel, albeit random, remain unchanged over each block. We assume that the transmitter has the perfect knowledge of both main and eavesdropper channel gains. We require that a certain fixed amount of data needs to be securely transmitted in every single block. This model is motivated by applications that require to secure communication at constant bit rate. We assume that the channel gains are i.i.d. for both the main channel and the eavesdropper channel and they are independent from each other in each block. It is well known that, the method of sending secure information using the binning techniques inspired by the wiretap channel fails to secure the information at times when the eavesdropper channel has favorable conditions over the main channel, hence the *delay*[1]*-limited secrecy capacity* is 0, since outages are unavoidable. It was shown in [6] that, interestingly, a non-zero secrecy rate could be achieved by introducing **private key queues** at both the transmitter and the receiver. The work exploits the times at which the main channel is favorable over the eavesdropper channel to transmit some *random private key* bits along with the data bits. These key bits are stored in a separate key queue at the transmitter as well as the receiver, and are utilized to secure data bits, whenever the channel

This work is supported by NSF under Grants CCF-0916664, CCF-0635242.

[1]Note that, the term 'delay' refers to a single "decodable" block in information theory. In this context, the delay limited capacity is first introduced and analyzed in [4]. This notion of delay is fairly different from the delay experienced at the higher layers due to queueing, etc.

conditions favor the eavesdropper. When the main channel has a worse channel gain than the eavesdropper, by consuming these shared keys (simply using bit-wise EXOR operation), the transmitter can confuse the eavesdropper, despite the limited main-channel rate. However, while [6] investigates the basic limitations of such a system, the optimal power and rate control policy and the queue dynamics of the key buffer are not studied. Furthermore, the system only works for "invertible" channels.

To that end, we develop a delay-limited secure communication system with private key queues similar to the ones in [6]. In particular, we investigate the optimal rate and power control problem at the physical layer as well as the queueing dynamics of the private key queue. We show that, using our system the outage probability can be made arbitrarily close to 0 by jointly controlling the key buffer with the transmit power. Also, we develop the key buffer and power control mechanisms to achieve maximum secure constant bit rate achievable by the system. We show that the optimal power control involves a time sharing between *secure waterfilling* policies and *channel inversion* strategies and the key buffer needs to operate in the *heavy traffic regime* to achieve the maximum delay limited rate possible, under a small outage constraint. Our work provides a natural framework to **combine** both information theory and queueing analysis for studying the problem of information theoretic security.

We also present simulations to support our results. We specifically focus on scenarios that are difficult to analyze. For example, the upper bound of the delay limited secrecy capacity derived in [6] only depends on main channel and eavesdropper channel gains without any power constraint. However, with a finite average power constraint, there is significant difference between the upper and lower bound, especially in the low power region, to delay limited capacity. We show through simulations that, our scheme achieves better performance than the lower bound given in [6].

The rest of this paper is organized as follows. We formally introduce our system model in Section II, which consists of the physical layer model (relying on information theory) and the key queue model (relying on queueing analysis). Then, in Section II-A, we derive the optimal power control for the physical layer model under the assumption that there are no key outages. However, this solution makes the key queue unstable. Hence, in Section II-B, we introduce a small key outage probability to the system, and show that the key queue can be made stable. In this setting, we derive the workload distribution for the key queue in the heavy-traffic region. Finally, we provide simulations to support our main results in Section V, which is followed by the conclusion in Section VI.

II. System Model

Since our system involves both the physical channel and the private key queue dynamics, we present them in Sections II-A and II-B, respectively. Within this setting, we briefly describe the problem that will be addressed and analyzed in this paper in Section II-C. We use "$\stackrel{d}{=}$" and "$\stackrel{d}{\leq}(\stackrel{d}{\geq})$" to denote equal in distribution and less (greater) or equal in distribution, respectively.

A. Channel Model

The physical layer channel dynamics are modeled by a slotted system. In each time slot, a block of data is transmitted over N channel uses. At the end of the transmission of block t, the observed signals at the receiver and at the eavesdropper are:

$$\mathbf{y}(t) = g_m(t)\mathbf{x}(t) + \mathbf{w}_m(t)$$

and

$$\mathbf{z}(t) = g_e(t)\mathbf{x}(t) + \mathbf{w}_e(t),$$

respectively, where $\mathbf{x}(t) \in \mathbb{C}^N$ is the transmitted signal, $\mathbf{y}(t) \in \mathbb{C}^N$ is the received signal by the legitimate receiver, and $\mathbf{z}(t) \in \mathbb{C}^N$ is the received signal by the eavesdropper. Flat fading channel gains, $g_m(t)$ for the main channel and $g_e(t)$ for the eavesdropper channel are two independent complex random variables. Furthermore, we assume that $\{g_m(t), t \geq 1\}$ and $\{g_e(t), t \geq 1\}$ are i.i.d. processes that are also independent from each other. The transmitted signal is corrupted by circularly symmetric complex Gaussian Noise vectors with zero mean and unit sample variances at both the receiver $\mathbf{w}_m(t)$ and the eavesdropper $\mathbf{w}_e(t)$. The power gains of the fading channels are denoted by $h_m(t) = \|g_m(t)\|^2$ and $h_e(t) = \|g_e(t)\|^2$.

We restrict ourselves to a class of power policies that only depend on the instantaneous channel state $\mathbf{h}(t) = (h_m(t), h_e(t))$ in block t. Since $\{\mathbf{h}(t)\}$ is i.i.d., we drop the index t and use the notation $\mathbf{h}$ for simplicity. We focus on power allocation functions $P(\mathbf{h})$, that depend on the instantaneous channel gains only. In this paper, we focus on the long term power constraint (or average power constraint), which is defined by

$$E[P(\mathbf{h})] \leq \bar{P} \tag{1}$$

for some $\bar{P} > 0$.

We assume full channel state information (CSI), i.e., the transmitter has full causal knowledge of $\mathbf{h}(t)$. We also assume that, the eavesdropper knows the coding strategy of the transmitter for each block. We define *instantaneous achievable rates* for the legitimate receiver, $R_m(t)$ and eavesdropper, $R_e(t)$, as:

$$R_m(t) = \log\left(1 + P(\mathbf{h})h_m(t)\right) \tag{2}$$

and

$$R_e(t) = \log\left(1 + P(\mathbf{h})h_e(t)\right). \tag{3}$$

For each block t, using Wyner's result [1], we can achieve a *secrecy rate* of

$$R_s(t) = [R_m(t) - R_e(t)]^+, \tag{4}$$

where $[x]^+ = \max\{0, x\}$. The secrecy rate is the number of bits that the receiver can decode per channel use, subject to no decodable bits at the eavesdropper. Since the secrecy rate $R_s(t)$ and the main channel rate $R_m(t)$ are completely

determined by the power allocation function $P(\mathbf{h})$ and channel gains $\mathbf{h}$, we use the notations $R_s(t) \equiv R_s(\mathbf{h}, P)$ and $R_m(t) \equiv R_m(\mathbf{h}, P)$.

Finally, we assume that the application requires a constant amount, b bits/channel use of data (which corresponds to Nb bits/block[2]) to be *securely* transmitted in *every* block over the main channel. If Nb bits cannot be transmitted securely over a given block t, we say that a *secrecy outage* has occurred.

B. Key Queue Model

From Equation (4), we know that the secrecy rate $R_s(t) = 0$ regardless of $P(\mathbf{h})$, whenever $h_m(t) < h_e(t)$. It was shown in [6] that, one can avoid a secrecy outage over block t, even when $R_s(t) = 0$ by introducing *private key queues* at the transmitter and the receiver. Our system, depicted in Fig. 1, is motivated by this idea. The idea is to exploit the times at which the main channel is favorable over the eavesdropper channel to transmit some *random private key* bits along with the data bits. These key bits are stored in a separate key queue at the transmitter as well as the receiver; we denote by $Q_k(t)$ the number of bits stored in the key queue at time t. When the main channel has a worse channel gain than the eavesdropper, by consuming these shared keys (simply using bit-wise EXOR operation), the transmitter can confuse the eavesdropper, despite the limited main-channel rate. Using Shannon's result [3], in order to fully encrypt Nb bits of data, the total number of key bits should be at least equal to Nb. To that end, even with a key buffer, one may not be able to avoid secrecy outages, which can be caused by the occurrence of either one of the following two events:

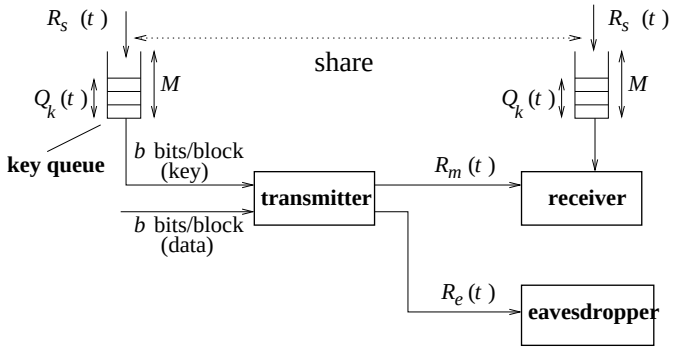

Fig. 1. System model with a private key queue at the transmitter and the receiver.

I. **Channel outage:** $R_m(t) < b$. In case of this event, the desired rate of b bits/channel use cannot be achieved (even without a secrecy constraint), regardless of the key queue state, $Q_k(t)$.
II. **Key outage:** $Q_k(t) + R_s(t) - b < 0$. In this case, $R_s(t)$ is too low to support b bits/channel use even with the aid of all stored key bits.

In case of an outage over block t, we assume that no data is transmitted over that block. Instead $NR_s(t)$ private key bits are generated and only key bits are transmitted to the receiver during that block. Putting it all together, we can write the queueing recursions for $Q_k(t)$ for a given power allocation $P(\mathbf{h})$ (and hence the associated rate allocation $R_s(\mathbf{h}, P)$) as follows:

$$\begin{aligned} Q_k(t+1) &= \Big(Q_k(t) \\ &\quad + (R_s(t) - b)\mathbf{1}\left(\{R_m(t) \geq b\} \cap \{Q_k(t) + R_s(t) - b \geq 0\}\right) \\ &\quad + R_s(t)\mathbf{1}\left(\{R_m(t) < b\} \cup \{Q_k(t) + R_s(t) - b < 0\}\right)\Big)^+ \\ &= \Big(Q_k(t) + R_s(t) \\ &\quad - b\mathbf{1}\left(\{R_m(t) \geq b\} \cap \{Q_k(t) + R_s(t) - b \geq 0\}\right)\Big)^+. \end{aligned} \quad (5)$$

C. Problem Description

We consider the following questions:

- What is the maximum achievable constant (delay-limited) rate b^* achievable by our system, subject to a given upper bound α on the outage probability and a given average power constraint $\bar{P}$? Mathematically it can be formulated as follows:

$$b^* = \max_{\text{P(outage)} \leq \alpha, \mathbb{E}[P(\mathbf{h})] \leq \overline{P}} b. \quad (6)$$

- What is the optimal power allocation to achieve b^*?
- What is the key queue workload distribution when key bits are used efficiently? Clearly, it is undesirable for the key queue to be unstable, since it means that many key bits, which are generated and transmitted from the transmitter to the receiver consuming valuable resources, are simply stored in the key queue without ever being utilized.

In our system, finding the optimal power and queue control policies are extremely complicated, due to apparent coupling between the two. The two issues need to be jointly considered and the optimal solution is based on a constrained infinite horizon dynamic program. Solving the dynamic program does not give much intuition on the operation of the system and even less valuable in understanding the dynamics of the private key queue and its interaction with the channel variations.

Alternatively, we resort to a sub-optimal scheme that can approximate the original problem by two subproblems, using which we decouple power allocation and queue control. This division gives us insights into how the delay limited secrecy system should be designed. Moreover, the decoupling does not lead to a significant loss in performance in certain scenarios as we will illustrate using simulations. We study power control in Section III and the private key queue management in Section IV.

The construction of these two subproblems is based on the following arguments.

1) We start with a general optimization problem that solves the maximum expected secrecy rate $R(b, \bar{P}, \alpha_1)$ for

[2]To achieve the theoretical limits one needs to pass the block size N to infinity. However, in practice, the typical packet sizes allow the achievable rates given in (2) and (3) to be met fairly closely at reasonably low probability of error.

fixed $b>0$, α_1 and $\bar{P}>0$,

$$R(b,\bar{P},\alpha_1)=\max_{P(\mathbf{h})}\mathbb{E}\left[R_s\right] \tag{7}$$

$$\text{subject to: } P(\mathbf{h})\geq 0, \tag{7a}$$

$$\mathbb{E}[P(\mathbf{h})]\leq \bar{P}, \tag{7b}$$

$$\mathbb{P}\left[R_m(\mathbf{h},P)<b\right]\leq \alpha_1 \tag{7c}$$

Note that $R(b,\bar{P},\alpha_1)$ is a non-increasing function with respect to b. This policy involves a time sharing between *secure waterfilling* and *channel inversion* strategies.

2) As will be shown later in Lemma 2, b^* satisfies

$$R(b^*,\bar{P},\alpha_1)=b^*(1-\mathbb{P}\left[R_m(\mathbf{h},P^*)<b^*\right]), \tag{8}$$

and with $b=b^*$, our system indeed achieves a zero key outage probability, where P^* is the optimal power allocation policy, i.e. the solution of (7). Since solving (7) gives us the optimal power control policy for a fixed $b>0$ and a $\bar{P}>0$ under the condition that there are no key outages, our problem boils down to finding the maximum b^* that satisfies Equation (8).

3) However, we show that, the preceding power policy leads to an unstable private key queue, i.e., the mean and the variance of $Q_k(t)$ grows unboundedly as $t\to\infty$, which is untenable because in practice the key buffer size is finite. To address this issue, we choose a suboptimal key rate b, which is slightly larger than b^*. This choice stabilizes the key queue at the expense of some non-zero key outage probability. In order to preserve high performance, we show that the key queue needs to be operated in the heavy-traffic regime, under which we derive the key queue workload distribution.

III. The Power control Policy

In this section we study the power control policy for our system. Following the argument given in the preceding section, we investigate this problem in two steps. First, we derive the optimal power control policy ignoring key queue outages in Section III-A. Then, using the problem as a building block, we provide an equation, the solution of which gives the optimal data transmission rate b^*, and show that with the optimal key rate $b=b^*$, the key outage probability is indeed 0.

A. The power control policy

The objective of (7) is to maximize the expected secrecy rate for a fixed rate b, a channel outage probability constraint of α_1 and the average power constraint of $\bar{P}$. The solution of Problem[3] (7) depends on three parameters $(\bar{P},b,\alpha_1)$.

Lemma 1: Problem (7) does not have a feasible solution if

$$\bar{P}<\quad P_{\min} \\ =\quad \int_{h_m\geq c}\frac{2^b-1}{h_m}f(\mathbf{h})d\mathbf{h}.$$

where the constant, c is chosen such that the marginal probability distribution function of h_m satisfies $\mathbb{P}[h_m\leq c]=\alpha_1$.

[3]A similar problem was solved in [8], without the secrecy requirement.

Proof: The proof is given in our online technical report [12]. ■

To introduce our optimal power allocation policy, we first define the power control policies $P_{wf}(\mathbf{h},\lambda)$ and $P_{inv}(\mathbf{h})$ as

$$P_{wf}(\mathbf{h},\lambda)=\frac{1}{2}\Big[\sqrt{\left(\frac{1}{h_e}-\frac{1}{h_m}\right)^2+\frac{4}{\lambda}\left(\frac{1}{h_e}-\frac{1}{h_m}\right)} -\left(\frac{1}{h_e}+\frac{1}{h_m}\right)\Big]^+, \tag{9}$$

$$P_{inv}(\mathbf{h})=\frac{2^b-1}{h_m} \tag{10}$$

where $\lambda\in\mathbb{R}^+$. We refer to $P_{wf}(\cdot)$ and $P_{inv}(\cdot)$ as the secure waterfilling and the channel inversion policies, respectively. Also, we define the region

$$\mathcal{G}(\lambda,k)=\Big\{\mathbf{h}:\left[R_s(\mathbf{h},P_{inv})-R_s(\mathbf{h},P_{wf})\right]^+ -\lambda\left[P_{inv}(\mathbf{h})-P_{wf}(\mathbf{h},\lambda)\right]^+\geq k\Big\} \tag{11}$$

for some $k\in\mathbb{R}^-\cup\{0\}$.

Theorem 1: If $\bar{P}\geq P_{min}$, the optimal power allocation policy is

$$P^*(\mathbf{h})=P_{wf}(\mathbf{h},\lambda^*)+ \mathbf{1}\left(\mathbf{h}\in\mathcal{G}(\lambda^*,k^*)\right)\left(P_{inv}(\mathbf{h})-P_{wf}(\mathbf{h},\lambda^*)\right)^+ \tag{12}$$

where λ^* and k^* satisfy the average power constraint (7b) with equality, and $\mathbb{P}(\mathbf{h}\in\mathcal{G}(\lambda^*,k^*))=(1-\alpha_1)$.

The proof is motivated by that approach given in [8]. We provide the complete proof in our online technical report [12]. Here, we give some intuition on the solution. We first solve (7) by relaxing the main channel outage constraint (7c). The optimal power allocation policy without (7c) is $P_{wf}(\mathbf{h},\lambda^{**})$, where λ^{**} is chosen such that the average power constraint (7b) is met with equality.

1) If for this case, the main channel outage constraint (7c) is also satisfied, then $P^*(\mathbf{h})=P_{wf}(\mathbf{h},\lambda^{**})$. Note that, $P_{wf}(\mathbf{h},\lambda^{**})$ is also the power allocation function that leads to the ergodic secrecy capacity [5]. Furthermore, it could easily be shown that distinct values of $\bar{P}$ lead to distinct values of λ^{**}.
2) If $\mathbb{P}(R_m(\mathbf{h},P_{wf})<b)>\alpha_1$, then we utilize channel inversion power control, $P_{inv}(\mathbf{h})$ to overcome channel outages when $P_{wf}(\mathbf{h},\lambda^{**})$ yields a rate lower than b. In order to satisfy the average power constraint, we decrease the water level of the secure waterfilling solution by increasing λ such that it is slightly larger than λ^{**}, and use the excess power to *invert* the channel at *some* instants.
Note that, if for some h, $P_{wf}(\mathbf{h},\lambda)$ results in main channel outage, we need to use $(P_{inv}(\mathbf{h})-P_{wf}(\mathbf{h},\lambda))$ [4] amount of additional power to satisfy main channel rate b. Therefore, we optimize over the region such that, probability that the main channel rate is at least b, should be at least $(1-\alpha_1)$, due to (7c). The solution to this optimization turns out to be the region $G(\lambda^*,k^*)$.

[4]This is referred to as "residual power" in [8]

In summary, the power control policy is a time-sharing between $P_{inv}(\mathbf{h})$ and $P_{wf}(\mathbf{h},\lambda^*)$. In the Figure 2, we plot the scheme for the power control policy in different regions with respect to h_m and h_e, where to the right of the solid boundary corresponds to the region $\mathcal{G}(\lambda^*,k^*)$, in which $P^*(\mathbf{h}) = \max(P_{inv}(\mathbf{h}), P_{wf}(\mathbf{h},\lambda^*))$. To the left of the solid boundary, $P^*(\mathbf{h}) = P_{wf}(\mathbf{h},\lambda^*)$. To further illustrate the power control, we plot the allocated power versus main channel gain h_m in Figure 3 for a constant eavesdropper channel gain h_e, i.e., along a horizontal dotted line as shown in Figure 2.

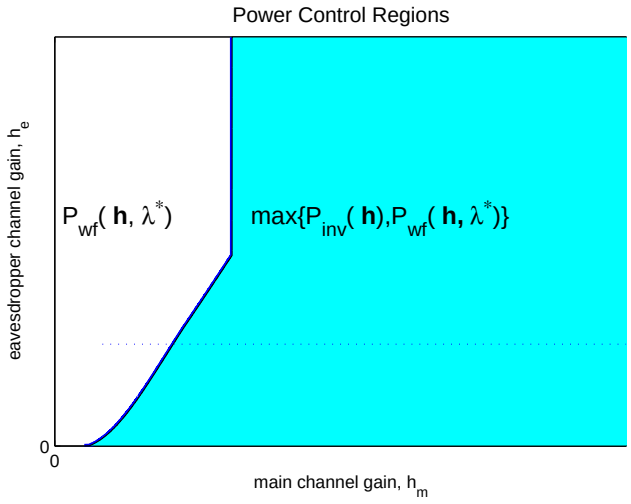

Fig. 2. The power control policy in different regions with respect to h_m and h_e.

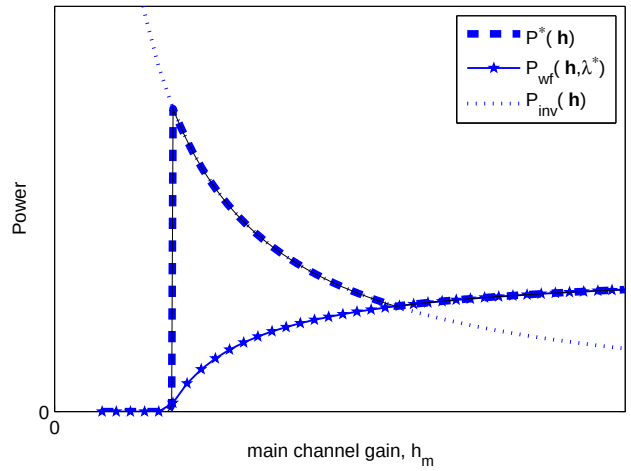

Fig. 3. The power control policy with respect to h_m for a fixed h_e.

B. Avoiding key queue outages

Before investigating the power control problem in the presence of the key queue, we first explain how it relates with Problem (7) in the preceding section that does not depend on the key queue. As shown in the following lemma, by carefully controlling the rate b and the channel outage probability $\mathbb{P}[R_m < b]$, we can guarantee that the probability of key outage is zero.

Lemma 2: If the process $Q(t)$ is stationary and ergodic, and the outage probability (including both channel and key outages) satisfies $\mathbb{P}[\text{outage}] \leq \alpha$, $\alpha > 0$, then,

$$b = \frac{\mathbb{E}[R_s]}{1-\mathbb{P}[\text{outage}]} \leq \frac{\mathbb{E}[R_s]}{1-\alpha}.$$

Proof: Using the condition that $\{Q_k(t)\}$ is stationary and ergodic, we obtain

$$1-\mathbb{P}[\text{outage}] = \lim_{n\to\infty} \frac{\sum_{i=1}^{n} \mathbf{1}\left(\{R_m(i)\geq b\}\cap\{Q_k(i)+R_s(i)-b\geq 0\}\right)}{n}.$$

Note that

$$\sum_{i=1}^{n} \mathbf{1}\left(\{R_m(i)\geq b\}\cap\{Q_k(i)+R_s(i)-b\geq 0\}\right) = \frac{\sum_{i=1}^{n} R_s(i) - Q_k(n)}{b},$$

which, using the fact $\lim_{n\to\infty} Q_k(n)/n = 0$ and law of large numbers, yields

$$\mathbb{E}[R_s] = \lim_{n\to\infty} \frac{\sum_{i=1}^{n} R_s(i)}{n} = (1-\mathbb{P}[\text{outage}])\, b \geq (1-\alpha)b.$$

Therefore, we prove $b^* \leq \mathbb{E}[R_s]/(1-\alpha)$. ■

Remark 1: If $b = \mathbb{E}[R_s]/(1-\mathbb{P}[R_m < b])$, we only have channel outages, and the key outage probability is equal to zero.

Based on this insight, we formulate the optimal power control in the presence of key queue as follows:

$$\begin{aligned} b^*(1-\mathbb{P}[R_m(\mathbf{h},P^*)<b^*]) = \max_{P(\mathbf{h})} \mathbb{E}\left[R_s\right] \\ \text{subject to: } P(\mathbf{h})\geq 0, \\ \mathbb{E}[P(\mathbf{h})]\leq \bar{P}, \\ \mathbb{P}\left[R_m(\mathbf{h},P)<b^*\right]\leq\alpha, \end{aligned} \quad (13)$$

where P^* is the optimal power control policy that maximize $\mathbb{E}\left[R_s\right]$ in (13). Note that b^* appears both in the constraint and the objective function. By Remark (1), we know that if $b = b^*$ where b^* is the solution of (13), then we only have channel outages and the key outage probability is equal to zero.

Remark 2: The delay limited secrecy **capacity** was also addressed in [6]. There, outages were not allowed and it was shown that

$$\lim_{\bar{P}\to\infty,\alpha\to 0} b^* = \mathbb{E}_{h_m>h_e} \log\left[\frac{h_m}{h_e}\right]. \quad (14)$$

Note that, since $\bar{P}\to\infty$ above, there is no power control. Our simulation results also illustrate that the power allocation policy has minimal impact on the performance in the very-high power regime. On the other hand, when the average power is limited, we show that our power allocation scheme outperforms the sole channel inversion policy, which is shown in [6] to achieve the delay limited secrecy capacity in the infinite-power regime.

IV. Key Queue Dynamics

In the preceding section, we derived the optimal power policy for the case in which the probability of key outages is forced to be zero. As will be shown in Lemma 4, this scenario will result in an unstable key queue and both the mean and variance of the number of keys in the key queue will grow to infinity as $t \to \infty$. In this section, using the power policy in the preceding section and allowing key outages, we show that the key queue in fact can be made stable at the expense of some minimal increase in the overall outage probability. Under the condition that the key outage probability is small, we derive the workload distribution for the key queue in the heavy-traffic regime in Theorem 3. In the rest of this section, except for cases explicitly stated, we assume that the system has a steady state, and when the system reaches stationarity, $\{Q_k(t)\}$ is a stationary and ergodic process.

Specifically, we study the queueing dynamics for the private key queue under the condition that the total outage probability is equal to α, i.e.,

$$\mathbb{P}\left[\{R_m(t) < b\} \cup \{Q_k(t) + R_s(t) - b < 0\}\right] = \alpha, \quad (15)$$

and

$$\mathbb{P}\left[R_m(t) < b\right] = \beta(b) < \alpha \quad (16)$$

when the system reaches stationarity. By (13), we know $\beta(b^*) = \alpha$ if $b = b^*$. When the key queue outage probability is very small, the key queue is in the heavy traffic region (see Theorem 3 in Section IV).

Recall the queueing dynamics for the private key queue described in Equation (5). This recursion is highly complicated since the indicator functions involve $Q_k(t)$. To better understand this recursion, we introduce a new variable $Q^*(t)$ as described below.

Definition 1: Let $\{Q^*(t)\}_{t\geq 0}$ be the process that satisfies the following recursion

$$Q^*(t+1) = \left(Q^*(t) + R_s(t) - b\mathbf{1}(R_m(t) \geq b)\right)^+ \quad (17)$$

with $Q^*(0) = Q_k(0)$.

The following lemma relates $Q^*(t)$ to $Q(t)$.

Lemma 3: In the presence of both channel and key outages, for all t, we have

$$Q^*(t) \leq Q_k(t) \leq Q^*(t) + b. \quad (18)$$

Remark 3: Lemma 3 implies that the stability of $Q^*(t)$ guarantees that $Q(t)$ is also stable and vice versa.

Proof: First, we prove the lower bound $Q^*(t) \leq Q_k(t)$. By induction, assuming $Q^*(t) \leq Q_k(t)$, we need to verify that $Q^*(t+1) \leq Q_k(t+1)$. Using (5), we obtain

$$\begin{aligned} Q_k(t+1) &= \Big(Q_k(t) + R_s(t) \\ &\quad - b\mathbf{1}\left(\{R_m(t) \geq b\} \cap \{Q_k(t) + R_s(t) - b \geq 0\}\right)\Big)^+ \\ &\geq \left(Q_k(t) + R_s(t) - b\mathbf{1}(R_m(t) \geq b)\right)^+ \\ &\geq \left(Q^*(t) + R_s(t) - b\mathbf{1}(R_m(t) \geq b)\right)^+ \\ &= Q^*(t+1), \end{aligned}$$

which finishes the proof of the lower bound.

Next, we prove the upper bound. Again, we use induction. Assuming $Q_k(t) \leq Q^*(t) + b$, we need to show that $Q_k(t+1) \leq Q^*(t+1) + b$. There two different scenarios.

1) If $Q^*(t) + R_s(t) - b\mathbf{1}\left(\{R_m(t) \geq b\}\right) \geq 0$, then, using $Q^*(t) \leq Q(t)$, we obtain

$$\begin{aligned} &Q_k(t) + R_s(t) \\ &\quad - b\mathbf{1}\left(\{R_m(t) \geq b\} \cap \{Q_k(t) + R_s(t) - b \geq 0\}\right) \\ &\quad \geq Q^*(t) + R_s(t) - b\mathbf{1}\left(\{R_m(t) \geq b\}\right) \geq 0, \end{aligned}$$

which, using (5), implies

$$\begin{aligned} Q_k(t+1) = Q_k(t) + R_s(t) \\ - b\mathbf{1}\left(\{R_m(t) \geq b\}\right). \end{aligned} \quad (19)$$

Observe that, by (17),

$$Q^*(t+1) = Q^*(t) + R_s(t) - b\mathbf{1}\left(\{R_m(t) \geq b\}\right),$$

which, in conjunction with (19) and $Q_k(t) \leq Q^*(t) + b$, yields $Q_k(t+1) \leq Q^*(t+1) + b$.

2) If $Q^*(t) + R_s(t) - b\mathbf{1}\left(\{R_m(t) \geq b\}\right) < 0$, then $Q^*(t+1) = 0$. We further consider two cases. First, if $Q_k(t) + R_s(t) - b \geq 0$, then,

$$\begin{aligned} Q_k(t+1) &= \Big(Q_k(t) + R_s(t) - b\mathbf{1}\left(\{R_m(t) \geq b\}\right)\Big)^+ \\ &\leq \Big(Q^*(t) + b + R_s(t) - b\mathbf{1}\left(\{R_m(t) \geq b\}\right)\Big)^+ \\ &\leq b \\ &= Q^*(t+1) + b. \end{aligned} \quad (20)$$

Next, if $Q_k(t) + R_s(t) - b < 0$, then

$$Q_k(t+1) = Q_k(t) + R_s(t) < b = Q^*(t+1) + b,$$

which, combined with (20), yields

$$Q_k(t+1) \leq Q^*(t+1) + b.$$

■

Before we state our main result, we begin with the critical situation when the system only has channel outages, i.e., $b = b^*$.

Lemma 4: If $b = b^*$ and the optimal power allocation $P^*(\cdot)$ is used, i.e., $\mathbb{E}[R_s] = b^*\mathbb{P}[R_m \geq b^*]$, then,

$$\lim_{t\to\infty} \frac{Q_k(t)}{\sqrt{\mathbb{V}ar\left[R_s(0) - b\mathbf{1}(R_m(0) \geq b^*)\right]t}} \stackrel{d}{=} |N(0,1)|,$$

where $|N(0,1)|$ is the absolute value of a normal random variable with mean zero and variance one.

Proof: Using standard queueing result, e.g., see Proposition 1.2 of [10], we obtain

$$\lim_{t\to\infty} \frac{Q^*(t)}{\sqrt{\mathbb{V}ar\left[R_s(0) - b\mathbf{1}(R_m(0) \geq b^*)\right]t}} \stackrel{d}{=} |N(0,1)|,$$

which, in conjunction with Lemma 3, completes the proof. ■

This lemma implies that, if we only have channel outages, the private key queue will be unstable, since $Q_k(t)$ is asymptotically distributed as $\sqrt{\mathbb{V}ar\left[R_s(0) - b^*\mathbf{1}(R_m(0) \geq b^*)\right]t}|N(0,1)|$, which has an increasing mean and variance. This result suggests that

avoiding key outages completely is costly, since the necessary buffer size grows unboundedly. In order to make the key queue stable, next, we introduce key outages by choosing b close to b^* such that $\mathbb{E}[R_s] < b\mathbb{P}[R_m \geq b]$.

Heavy traffic approximation

In the rest of this section, under the conditions (15) and (16), we present our main result on the queueing dynamics of the private key queue. Since we require that key outage probability is small and at the same time the key queue is stable, we show that the traffic intensity of the private key queue must be very close to 1. Consequently, the key queue must be operated in the heavy traffic regime. In this regime we derive the workload distribution of the key queue using heavy-traffic approximation.

Lemma 5: If $\mathbb{E}[R_s] < b\mathbb{P}[R_m \geq b]$, then there exists an almost surely finite random variable Q^* such that, for all x,

$$\liminf_{t\to\infty} \mathbb{P}[Q_k(t) > x] \geq \mathbb{P}[Q^* > x], \tag{21}$$

and

$$\limsup_{t\to\infty} \mathbb{P}[Q_k(t) > x] \leq \mathbb{P}[Q^* + b^* > x], \tag{22}$$

and thus the private key queue is stable.

Remark 4: Additionally, if $Q_k(t)$ is stationary and ergodic, there exists an almost surely finite random variable Q_k such that, for all x,

$$\lim_{t\to\infty} \mathbb{P}[Q_k(t) > x] = \mathbb{P}[Q_k > x]. \tag{23}$$

Proof: By (17), we know

$$Q^*(t+1) = \left(Q^*(t) + R_s(t) - b\mathbf{1}(R_m(t) \geq b)\right)^+.$$

Using Loynes's result [9], the condition $\mathbb{E}[R_s] < b\mathbb{P}[R_m \geq b]$ implies that, there exists a finite random variable Q^* such that

$$\lim_{t\to\infty} \mathbb{P}[Q^*(t) > x] = \mathbb{P}[Q^* > x].$$

Using (18) of Lemma 3, we finish the proof of the lemma. ∎

Note that $\{R_s(t) - b\mathbf{1}(R_m(t) \geq b)\}_{t\geq 0}$ is a sequence of i.i.d. random variables, and we define G_+ to be the ladder height distribution of the random walk $\{S_n = \sum_{t=1}^n R_s(t) - b\mathbf{1}(R_m(t) \geq b)\}_{n\geq 1}$ with $\|G_+\| = \mathbb{P}[S_n > 0 \text{ for some } n \geq 1]$. Under the condition $\mathbb{E}[R_s] < b\mathbb{P}[R_m \geq b]$, we can show that the distribution of $Q_k(t)$ exhibits an exponential tail, as shown in the following result.

Theorem 2: Under condition (23), if $R_s(t) - b\mathbf{1}(R_m(t) \geq b)$ is nonlattice, satisfying $\mathbb{E}\left[\left(R_s(t) - b\mathbf{1}(R_m(t) \geq b)\right)^{\theta^*}\right] = 1$, $\theta^* > 0$, and $\left(\mathbb{E}\left[\left(R_s(t) - b\mathbf{1}(R_m(t) \geq b)\right)^{\theta}\right]\right)'\Big|_{\theta=\theta^*} < \infty$, then

$$\frac{1 - \|G_+\|}{\theta^* \int_0^\infty x e^{\theta^* x} G_+(dx)} \leq \lim_{x\to\infty} \mathbb{P}[Q_k > x] x^{\theta^*} \leq \frac{(1 - \|G_+\|)\, b^{\theta^*}}{\theta^* \int_0^\infty x e^{\theta^* x} G_+(dx)}.$$

Proof: Using Theorem 5.3 in Chapter XIII of [10], we obtain

$$\lim_{x\to\infty} \mathbb{P}[Q_k > x] x^{\theta^*} = \frac{1 - \|G_+\|}{\theta^* \int_0^\infty x e^{\theta^* x} G_+(dx)},$$

which, by Lemma 18, completes the proof. ∎

In view of Lemma 2, it is easy to check that the condition $\mathbb{E}[R_s] < b\mathbb{P}[R_m \geq b]$ is equivalent to $\mathbb{P}[R_m(t) < b] < \mathbb{P}[\text{outage}]$, i.e., the key outage probability is strictly positive. The requirement of small key outage probabilities makes the system operate in the heavy traffic region, as shown in the following theorem.

Theorem 3: If $\beta(b) = \mathbb{P}[R_m < b] < \alpha$, $\mathbb{E}[R_s^2] < \infty$, $\mu_b = \mathbb{E}[R_s] - b\mathbb{P}[R_m \geq b] < 0$ and $\mathbb{P}[R_m < b]$ is continuous in a neighborhood of $b = b^*$, then, we have, for $\sigma_b = \mathbb{V}ar[R_s - b\mathbf{1}([R_m \geq b)]$ and $y \geq 0$,

$$\lim_{b\to b^*} \mathbb{P}\left[\frac{|\mu_b| Q_k(t)}{\sigma_b^2} > y\right] = e^{-2y}.$$

Remark 5: As an approximation, we have, for small α,

$$\mathbb{P}\left[Q_k(t) > z\right] \approx e^{-\frac{2|\mu_b|}{\sigma_b^2} z},$$

and $\mathbb{E}[Q_k(t)] \approx \sigma_b^2 / (2|\mu_b|)$. Therefore, after introducing key outages, the workload in the private key queue roughly follows an exponential distribution.

Proof: This theorem is based on the heavy traffic limit for queues developed in [11]; see also Theorem 7.1 in [10].

In order the prove this result, we only need to verify the following three conditions: i) $\lim_{b\to b^*} \mu_b = 0$; ii) $\lim_{b\to b^*} \sigma_b = \sigma_0 > 0$; and iii) the class of random variables $\left\{\left(R_s(0) - b\mathbf{1}(R_m(0) \geq b)\right)^2\right\}$ indexed by b is uniformly integrable.

Since $\mathbb{P}[R_m < b]$ is continuous in a neighborhood of $b = b^*$, we obtain

$$\lim_{b\to b^*} \mu_b = \mathbb{E}[R_s] - b^*\mathbb{P}[R_m \geq b^*] = 0,$$

and

$$\begin{aligned}
\lim_{b\to b^*} \sigma_b^2 &= \lim_{b\to b^*} \mathbb{V}ar[R_s(0) - b^*\mathbf{1}([R_m(0) \geq b^*)] \\
&= \mathbb{V}ar[R_s(0)] \\
&\quad - 2\text{Cov}\left(R_s(0), \mathbf{1}\left(R_m(0) \geq \frac{\mathbb{E}[R_s(0)]}{1-\beta}\right)\right) \\
&\quad + \left(\frac{\mathbb{E}[R_s(0)]}{1-\alpha}\right)^2 \mathbb{P}\left[R_s(0) \geq \frac{\mathbb{E}[R_s(0)]}{1-\beta}\right] \\
&\quad \times \left(1 - \mathbb{P}\left[R_s(0) \geq \frac{\mathbb{E}[R_s(0)]}{1-\beta}\right]\right) \\
&\triangleq \sigma_0^2 > 0.
\end{aligned}$$

Next, for some $0 < \epsilon < b^*$, notice that when b lies on the interval $[b^* - \epsilon, b^* + \epsilon]$, we have

$$\begin{aligned}
\left(R_s(0) - b\mathbf{1}([R_m(0) \geq b)\right)^2 &\leq R_s(0)^2 \\
&\quad - 2R_s(0)(b^* - \epsilon)\mathbf{1}\left(R_m(0) \geq b^* + \epsilon\right) \\
&\quad + (b^* + \epsilon)^2 \mathbf{1}\left(R_m(0) \geq b^* - \epsilon\right).
\end{aligned}$$

The three random variables on the right hand side of the preceding inequality do not depend on b and thus provide a uniform bound on the class of random variables $(R_s(0) - b\mathbf{1}([R_m(0) \geq b))^2$ that are indexed by b. The condition $\mathbb{E}[R_s(0)^2] < \infty$ implies that this class of random variables $(R_s(0) - b^*\mathbf{1}([R_m(0) \geq b^*))^2$ is uniformly integrable.

Thus, by Theorem 7.1 in [10], we have, for all $y > 0$,

$$\lim_{b \to b^*} \mathbb{P}\left[\frac{|\mu_b| Q^*(t)}{\sigma_b^2} > y\right] = e^{-2y},$$

which, in conjunction with Lemma 3, finishes the proof. ■

V. Numerical Examples

In this section, we conduct simulations to illustrate our main results. In Example 1, we study the situation when the power control policy achieves the delay limited secrecy without any outages. To satisfy these conditions, we investigate an invertible chi-square channel under the assumption that there is always enough keys in the key queue ($b = \mathbb{E}[R_s]$). Next, we proceed to study a more realistic and complex scenario when both channel outages and key outages occur. For this purpose, we study the non-invertible Rayleigh channel with the condition $b > \mathbb{E}[R_s]$, which results in both channel and key outages.

Specifically, we focus on scenarios that are difficult to analyze. For example, the upper bound of the delay limited secrecy capacity derived in [6] only depends on main channel and eavesdropper channel gains without any power constraint. However, with a finite average power constraint, there is significant difference between the upper and lower bound (especially in the low power region) of the delay limited capacity. We show through simulations that our scheme achieves better performance than the lower bound in [6].

Example 1: In this example, we assume that both the main and eavesdropper power gains follow a chi-square distribution of degree 4, mean 4 and variance 8. Therefore, the main and eavesdropper power gains actually are identically distributed. Since the main channel is invertible in this setting, we can assume that the channel outage probability is zero. Hence, we can compare our power policy with the lower and upper bound developed in [6]. Furthermore, Lemma (4) implies that $b = \mathbb{E}[R_s]$ would result in no key outages (key queue becomes unstable). We plot in Figure 4 the achieved delay limited secrecy rate as a function of the average power constraint $\bar{P}$. In the same figure, the upper and lower bounds given in [6] are also plotted along with the asymptote computed using (14). The lower bound is computed by using channel inversion policy, and the upper bound is defined by the delay limited capacity in [6]. When there is no average power constraint, the delay limited secrecy capacity does not change with power policies, as shown in Equation (14). However, when the average power is limited, there is significant difference between the upper bound and the lower bound in [6]. It is clear from Figure 4 that the performance of our power control policy obtained from (13) is very close to the upper bound derived in [6], hence even closer to the optimal solution.

Example 2: Next, we assume that both the main channel and the eavesdropper channel are characterized by Rayleigh

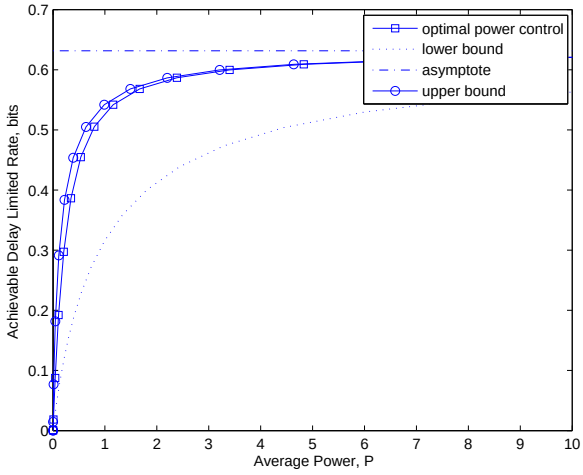

Fig. 4. Achievable delay limited rate under optimal power control without outages for Gaussian channel

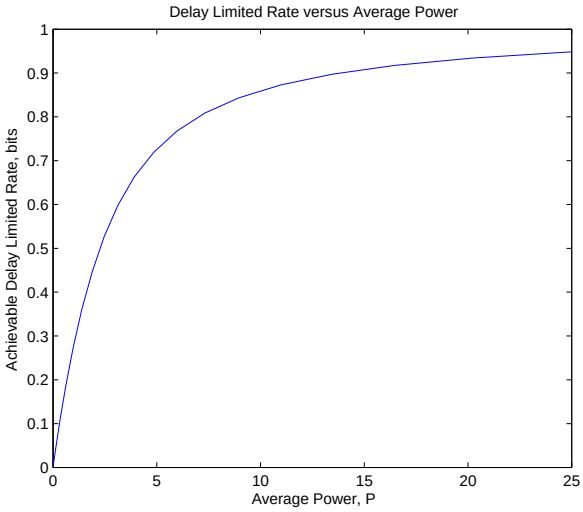

Fig. 5. Achievable delay limited rate under optimal power control with channel outage probability 0.01 for Rayleigh channel

fading, where the main channel and eavesdropper channel power gains follow exponential distribution with mean 1. Since Rayleigh channel is non-invertible, to maintain a non-zero delay limited rate without any outage is impossible. In this example, we choose the desired channel outage probability equal to 0.01 with the optimal b^* computed from Problem (13). Note that this combination will not result in key outages. We plot the achievable delay limited secrecy rate in Figure 5.

However, this scheme will make the key queue unstable. We illustrate this point in Figure 6 for $E[Rs] = 0.6934$, $\bar{P} = 4.5846$, $b^* = 0.6993$ and channel outage probability 0.01. As clearly shown in this figure, the number of private keys in the queue has a trend to keep increasing.

To make the key queue stable, we increase b^* above $\mathbb{E}[R_s]/(1-\alpha_1)$ a little bit. By doing so, we can deliberately introduce key queue outages to make the key queue stable. For the case $\bar{P} = 4.6585$, $\mathbb{E}[R_s] = 0.6945$, $b = 0.7164$, channel

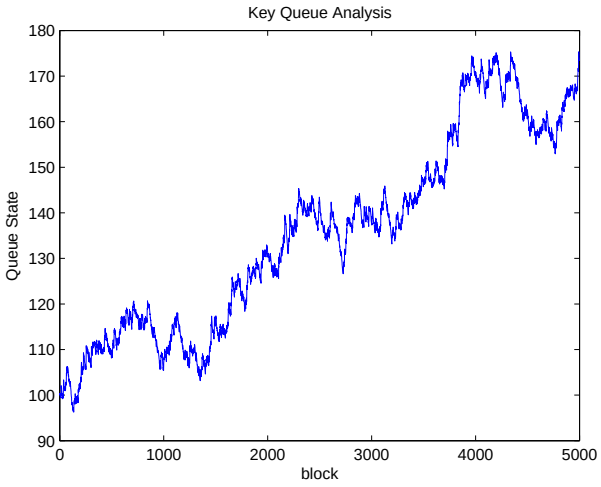

Fig. 6. Evolution of the key queue workload under the optimal power control with only channel outages for Rayleigh channel

outage probability 0.01, and key queue outage probability 0.02, we simulate the Rayleigh channel of the parameters, and plot the key queue workload distribution in Fig. 7. From this

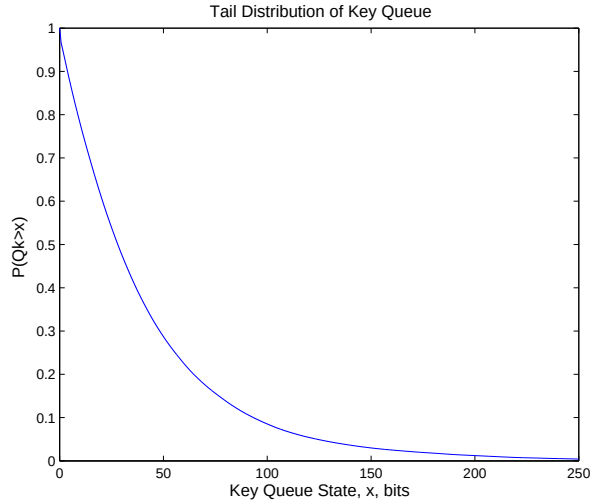

Fig. 7. Key queue workload distribution with both channel outages and key outages for Rayleigh channel

result, we see that even with a small increase of the maximal b^*, the key queue size can be reduced dramatically.

VI. Conclusion

In this paper, we design a wireless communication system that achieves constant bit rate data transmission over a block fading channel, which is secure from an eavesdropper that listens to the transmitter over another independent block fading channel. By introducing private key queues at both the transmitter and the receiver, we can exploit the times at which the main channel is favorable over the eavesdropper channel to transmit some random private key bits along with the data bits. These key bits are stored in a separate key queue at the transmitter as well as the receiver, and are utilized to secure data bits, whenever the channel conditions favor the eavesdropper. When the main channel has a worse channel gain than the eavesdropper, by consuming these shared keys (simply using bit-wise EXOR operation), the transmitter can confuse the eavesdropper, despite the limited main-channel rate.

We investigate the optimal rate and power control policies at the physical layer as well as the queueing dynamics of the private key queue. The optimal power control involves time sharing between secure waterfilling and channel inversion strategies and the key buffer needs to operate in the heavy traffic regime to achieve capacity under a small outage constraint. This work is our first step towards combining information theory and queueing analysis for studying the information theoretic security. Along this direction, there are many other interesting questions that can be further pursued. For example:

- The delay limited transmission rate is kept at a constant value b in this study. In practice, we may have to consider applications with varying transmission rate as well. This adds another dimension to this problem, and one may need to possibly resort to bang-bang control type of management scheme.
- In real systems, the buffer size of the key queue is also an important issue for designing an efficient system since we do not want the private keys stored in the key queue to overflow.

References

[1] A. D. Wyner, "The Wire-Tap Channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, October 1975.
[2] Leung-Yan-Cheong, S.; Hellman, M., "The Gaussian wire-tap channel," *Information Theory, IEEE Transactions on* , vol.24, no.4, pp. 451-456, Jul 1978
[3] C. E. Shannon, "Communication Theory of Secrecy Systems," *The Bell System Technical Journal*, vol. 28, pp. 656-715, October 1949.
[4] S. V. Hanly and D. N. C. Tse, "Multiaccess fading channels. II. Delay-limited capacities," *Information Theory, IEEE Transactions on*, vol.44, no.7, pp.2816-2831, November 1998.
[5] P. K. Gopala, L. Lai, and H. El-Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Transactions on Information Theory*, vol.54, no.10, pp.4687-4698, October 2008.
[6] K. Khalil, M. Youssef, O. O. Koyluoglu, and H. El-Gamal, "On the delay limited Secrecy Capacity of Fading Channels," *arXiv:0901.2616v2 [cs.IT]*, May 2009.
[7] R. A. Berry and R. G. Gallager, "Communication over fading channels with delay constraints," *Information Theory, IEEE Transactions on*, vol.48, no.5, pp.1135-1149, May 2002.
[8] J. Luo, L. Lin, R. Yates, and P. Spasojevic, "Service outage based power and rate allocation," *Information Theory, IEEE Transactions on* , vol.49, no.1, pp. 323-330, January 2003.
[9] R. M. Loynes. The stability of a queue with non-independent inter-arrival and service times. *Mathematical Proceedings of the Cambridge Philosophical Society*, 58:497–520, 1962.
[10] S. Asmussen. *Applied Probability and Queues*. Wiley, New York, 1987.
[11] J. F. C. Kingman, "On Queues in Heavy Traffic," *Journal of the Royal Statistical Society. Series B (Methodological)*, vol.24, no.2, pp.383-392, 1962.
[12] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. Shroff, "Joint Power and Secret Key Queue Management for Delay Limited Secure Communication," *Technical Report, Department of Electrical Engieerng and Computer Science, The Ohio State University*, July 2009.