Towards Achieving Full Secrecy Rate and Low Delays in Wireless Networks

Zhoujia Mao  
Department of ECE  
The Ohio State University  
maoz@ece.osu.edu

Can Emre Koksal  
Department of ECE  
The Ohio State University  
koksal@ece.osu.edu

Ness B. Shroff  
Departments of ECE and CSE  
The Ohio State University  
shroff@ece.osu.edu

Abstract—In this paper, we consider a single-user secure data communication system. Data packets arriving at the transmitter are enqueued at a data queue to be transmitted to the receiver over a block fading channel, securely from an eavesdropper that listens to the transmitter over another independent block fading channel. Part of the data is secured by the available secrecy rate while the other part is encrypted by the key bits, enqueued at both the transmitter and the receiver. We first address two separate problems in this paper: with an average power constraint, given any sample path of arrivals, how to admit the arrivals and allocate power such that the long term average secrecy rate is maximized and the maximum admission rate is achieved while the data queue is kept stable; with infinite queue backlog, given any sample path of secrecy rate, how to control the data transmission rate and key generation such that a smooth transmission rate and then a small queueing delay are achieved. We propose a power controller, transmission controller and an admission controller based on simple index policies that do not rely on any prior statistical information on the data arrival process and channel conditions. We show that our controllers has a provably efficient performance and solve the above two problems simultaneously. Furthermore, for any given secrecy rate sample path and correspondingly admissible arrival, we provide a rate allocation policy which is sample path queuing delay optimal.

I. INTRODUCTION

Motivated by the seminal paper by [1], there has 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 the use of 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.

In this paper, we address the single user setting in the presence of arrival of data packets being enqueued at a data queue to be transmitted to the receiver over a block fading channel, securely from an eavesdropper that listens to the transmitter over another independent block fading channel. We consider two separate problems, which involve the maximization of the long term average secrecy rate and admitted arrival rate while keeping data queue stable under an average power constraint, and maximization of a long-term average utility, defined as a function of the number of secure packets transmitted in each time slot. While, one would be inclined to exploit the entire secrecy rate for data transmission in each time slot in a greedy fashion, we show that this approach leads to a performance loss. Instead, the use of a key queue leads to a "smoother" secrecy rate, which in turn maximizes a concave utility, since it is negatively affected by the second order factors caused by the variability of the service. We propose a controller, which chooses the key generation (and transmission) rate along with the secure data transmission rate in each time slot using a transmission control component. The power control
component allocates the power such that the secrecy rate is maximized under the average power constraint. The admission control component chooses the amount of data admitted by the transmitter to be enqueued in the data queue such that the admission rate approaches the maximum secrecy rate. These three components are based on simple index policies that do not rely on any prior statistical information on the data arrival process. We show that our controller achieves a utility, arbitrarily close to the optimal utility. Also, we illustrate via simulations that the use of key queue reduces the queuing delay for the data packets, while serving packets that are admitted at the maximum admissible rate. For any given secrecy sample path and correspondingly admissible arrival, we also provide a rate control policy which is sample path queuing delay optimal.

II. SYSTEM MODEL

We consider a single-user system illustrated in Fig. 1, in which the transmitter enqueues data packets that wait to be transmitted to the receiver over the main channel at a variable power, securely from an eavesdropper, overhearing the transmission over a separate channel. Time is slotted, and the time-varying channel state of the main and the eavesdropper channel follow general processes \( h_m = \{h_m(0), h_m(1), \ldots, h_m(T - 1), \ldots \} \) and \( h_e = \{h_e(0), h_e(1), \ldots, h_e(T - 1), \ldots \} \), respectively. In this paper, we assume perfect knowledge of these channel states at the transmitter. With the transmission power vector \( \vec{P} = \{P(0), P(1), \ldots, P(T - 1), \ldots \} \), the instantaneous rate of the receiver and eavesdropper at slot \( t \) are \( R_m(t) = \log (1 + P(t)h_m(t)) \) and \( R_e(t) = \log (1 + P(t)h_e(t)) \), respectively. We also assume the time slots are long enough and as shown in [1], the achievable instantaneous secrecy rate at a given slot \( t \) is identical to \( R_s(t) = (R_m(t) - R_e(t))^+ \), \( \forall t \geq 0 \), where \((\cdot)^+ = \max[\cdot, 0]\). In a given time slot, this rate is fully utilized: part of it is used to secure data from the data queue and the remaining part is used to transmit randomly generated key bits to be stored at the both key queues at the transmitter and the receiver. The size of the data and the key buffers are infinite.

As shown in Fig. 1, the amount of secure data transmitted at a time \( t \) is \( \mu(t) \). A part \( (\mu_k(t)) \) bits of this data is secured using \( \mu_k(t) \) key bits by a simple bit-by-bit XOR operation. The remaining \( \mu(t) - \mu_k(t) \) bits is secured using the available secrecy rate \( R_s(t) \). Since the secrecy rate is fully utilized, the portion of the secrecy rate, not used to secure data is used to generate \( R_k(t) \) 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:

\[
q_k(t + 1) = q_k(t) + R_k(t) - \mu_k(t).
\]

The following lemma in [23] provides an equivalent model with the constraints that specify the relationships between the parameters.

**Lemma 1:** The key queue \( q_k \) can be modeled with the state evolution equation \( q_k(t + 1) = q_k(t) + R_s(t) - \mu(t) \) with the constraints \( 0 \leq \mu(t) \leq \min[q_k(t) + R_e(t), R_m(t)], \) \( 0 \leq \mu_k(t) \leq \min[\mu(t), R_e(t)] \), and \( (\mu(t) - \mu_k(t)) + R_k(t) = R_s(t) \).

III. PROBLEM FORMULATION

We aim to design an efficient algorithm to control the power and rate allocation such that the throughput of the system is maximized with small queuing delay, under an average power constraint. To achieve this, we first consider two separate problems.

In our first problem, we assume an infinitely backlogged data queue, i.e., \( q_d(0) = \infty \). The objective is to maximize the long-term average utility, which is a function of the transmission rate given any sample path of secrecy rate. Our control parameters are the amount of used key bits \( \mu_k(t) \), the amount of served data bits \( \mu(t) \), and the amount of generated key bits \( R_k(t) \). In particular, we have:

\[
\begin{align*}
(A) \quad & \max_{\mu, \mu_k, R_k} \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} U(\mu(t)) \\
\text{s.t.} \quad & q_k(t + 1) = q_k(t) + R_k(t) - \mu_k(t), \quad (1) \\
& 0 \leq \mu(t) \leq \min[q_k(t) + R_e(t), R_m(t)], \quad (2) \\
& 0 \leq \mu_k(t) \leq \min[\mu(t), R_e(t)], \quad (3) \\
& (\mu(t) - \mu_k(t)) + R_k(t) = R_s(t), \quad (4)
\end{align*}
\]

where the utility function \( U(\cdot) \) is assumed to be monotonically increasing, reversible and differentiable on the half real line \( \mathbb{R}_+ \cup \{0\} \). Note that if there were no key queue, then we would have \( q_k(t) = 0 \), \( \mu(t) = R_e(t) \), \( \mu_k(t) = 0 \), \( R_k(t) = 0 \), \( \forall t \geq 0 \). Also note that, the maximum achievable average secrecy rate is upper bounded by the average secrecy capacity \( R_s = \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} R_s(t) \).

In our second problem, we assume a general data arrival process, \( \{A(t)\} \) at the input of the data queue. At time \( t \), only a portion \( R(t) \) of all arrivals are admitted into the data queue in order to keep the data queue stable. All the admitted packets are required to be served by the system eventually. In the second problem, our objective is maximize the long-term
average admitted data rate under an average power constraint.

\[
\max_{R_s, \beta, \mu_k, R_e, P} \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} R(t)
\]

subject to

\[
\begin{align*}
q_d(t+1) &= (q_d(t) - \mu(t))^+ + R(t), \\
q_k(t+1) &= q_k(t) + R_s(t) - \mu(t), \\
0 &\leq R(t) \leq A(t), \\
0 &\leq \mu(t) \leq \min[q_k(t) + R_s(t), R_m(t)], \\
\limsup_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} q_d(t) < \infty, \\
0 &\leq \mu_k(t) \leq \min[\mu(t), R_e(t)], \\
(\mu(t) - \mu_k(t)) + R_e(t) &= R_s(t), \\
R_s(t) &= (R_m(t) - R_e(t))^+, \\
R_m(t) &= \log(1 + P(t) h_m(t)), \\
R_e(t) &= \log(1 + P(t) h_e(t)), \\
\limsup_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} P(t) &\leq P_{\text{avg}}, \\
0 &\leq P(t) \leq P_{\text{peak}}.
\end{align*}
\]

Note that, the maximum achievable average secrecy rate, which happens to be the objective function here, is upper bounded by the average secrecy capacity \( R_s \). By controlling the power allocation, we can first maximize the long term average secrecy rate. Then, by using an independent admission controller, we maximize the average admission rate that is bounded by the maximum secrecy rate. Further, as we shall show, \( R_s \) can be achieved even without a key queue. However, we will also illustrate that our solutions that involve the use of the key queue lead to smaller queueing delays, compared to the one without the key queue.

In these three problems, constraint (5) describes the data queue evolution, and constraints (1) and (6) describe the key queue evolution. Constraint (7) bounds the actual amount of sensed data \( R(t) \) by the available amount of data \( A(t) \) at time \( t \). Constraints (2) and (8) state that the amount of transmitted data is bounded by both the main channel rate and the amount of keys available. Constraint (9) guarantees data queue stability. Constraints (3) and (10) state that the amount of key bits used to secure data is bounded by the eavesdropper channel rate and does not exceed the amount of transmitted data. Constraints (4) and (11) mean that the secure capacity is fully utilized by the transmission of secure data and key bits. Constraints (12), (13) and (14) are definitions of instantaneous secrecy rate \( R_s(t) \), rate of receiver \( R_m(t) \) and eavesdropper \( R_e(t) \). Constraint (15) is the average power constraint and constraint (16) is the peak power constraint.

**Virtual Queues:** In order to have a fair rate allocation, we do not want the key queue to be drained frequently, which would lead to outages whenever \( R_s(t) = 0 \). We define \( \tilde{q}_k \) as the virtual key queue and try to avoid key outages by making the virtual key queue stable (similar ideas of utilizing virtual queue are used in [20], [24]). The virtual queue evolves according to the following equation:

\[
\tilde{q}_k(t+1) = (\tilde{q}_k(t) - \epsilon^+ + \mu(t) - R_s(t) + I_o(t))^+, 
\]

where \( \epsilon > 0 \) can be chosen arbitrarily, and

\[
I_o(t) = \mathbf{1}_{\text{key queue hits zero state from higher states in slot } t}
\]

is the indicator that the key queue is drained in slot \( t \). Without loss of generality, the initial state \( \tilde{q}_k(0) \) can be set to be zero.

Similarly, we define the following virtual power queue to avoid the average power constraint being violated:

\[
\tilde{q}_p(t+1) = (\tilde{q}_p(t) - P_{\text{avg}}^+) + P(t).
\]

**IV. Control Algorithm and Performance Analysis**

In this section, we provide a simple control algorithm, analyze its performance, and show that its provably optimal for all three problems described in the previous section.

**A. Algorithm**

Our algorithm for Problem (A) involves only a transmission rate controller. The transmission controller attempts to provide a smooth service by the help of the key bits.

**Transmission Control (TC):** We define \( V \in \mathbb{R}^+ \) to be the control parameter of our algorithm. In slot \( t \), the controller solves the following optimization problem and transmits with the calculated rate:

\[
\max_{\mu(t) \in \Pi(t)} \frac{V}{2} U(\mu(t)) - \tilde{q}_k(t)\mu(t),
\]

where \( \Pi(t) = \{ \mu(t) : 0 \leq \mu(t) \leq \min[q_k(t) + R_s(t), R_m(t)] \} \) is a compact and nonempty set. Furthermore, key generation and usage rates \( (R_k(t), \mu_k(t)) \) are chosen as follows: If \( \mu(t) > R_k(t) \), then \( R_k(t) = 0 \) and \( \mu_k(t) = \mu(t) - R_k(t) \); if \( \mu(t) \leq R_k(t) \), then \( \mu_k(t) = 0 \) and \( R_k(t) = R_s(t) - \mu(t) \). This ensures that constraint \( (\mu(t) - \mu_k(t)) + R_k(t) = R_s(t) \) is satisfied. It is not surprising that \( \mu_k(t) R_k(t) = 0 \), since any solution with \( \mu_k(t) R_k(t) > 0 \), can be equivalently replicated by using the secrecy rate to transmit data rather than generating and using key bits at the same time. Note that \( R_s(t) = (R_m(t) - R_e(t))^+ \geq R_m(t) - R_e(t) \), then for \( \mu(t) > R_k(t) \), we have \( \mu_k(t) = \mu(t) - R_k(t) \leq R_m(t) - R_e(t) \leq R_s(t) \). This leads to constraint \( 0 \leq \mu_k(t) \leq \min[\mu(t), R_e(t)] \) being satisfied.

The set, \( \Pi(t) \) of possible data transmission guarantees constraint (2) on \( \mu(t) \) in Problem (A). If \( U(\cdot) \) is concave, the objective function is a concave function of \( \mu(t) \). Consequently, TC solves a simple convex optimization problem in each time slot. The positive term \( \frac{V}{2} U(\mu(t)) \) 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 high 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 to be smoother
over time. It is also notable that (20) involves only \( \mu(t) \). The key generation and usage rates are not part of this optimization, and are chosen subsequently.

In Problem (B), we need to control the transmission power, admission and transmission rate such that the admitted rate is maximized while keeping the data queue stable under an average power constraint. In our algorithm, there are three components: a admission control component, a transmission control component, and a power control component. The transmission control component is the identical to the one described above for Problem (A), and the admission control and power control component are as follows:

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

\[
\max_{0 \leq R(t) \leq A(t)} \frac{V}{2} U(R(t)) - q_d(t) R(t). \tag{21}
\]

**Power Control (PC):** In slot \( t \), the controller solves the following optimization problem and allocate the calculated amount of power:

\[
\max_{0 \leq P(t) \leq P_{\text{max}}} \frac{V}{2} \left( \log \left( \frac{1 + P(t) h_m(t)}{1 + P(t) h_e(t)} \right) \right)^+ - \bar{q}_p(t) P(t). \tag{22}
\]

When \( h_m(t) < h_e(t) \), i.e., the channel condition of the eavesdropper is better, \( P(t) = 0 \) is the solution of Equation (22). The reason is that under such a situation, the instantaneous secrecy rate is zero with any power allocation. In order to satisfy the power constraint, it is obvious to save power for future usage. When \( h_m(t) \geq h_e(t) \), we have

\[
\left( \log \left( \frac{1 + P(t) h_m(t)}{1 + P(t) h_e(t)} \right) \right)^+ = \log \left( \frac{1 + P(t) h_m(t)}{1 + P(t) h_e(t)} \right) \geq \log \left( \frac{h_m(t)}{h_e(t)} \right) - \frac{1}{1 + P(t) h_e(t)}. \tag{23}
\]

which is concave in \( P(t) \). Then, Equation (22) is a concave maximization problem under this situation.

Note that \( TC, AC \) and \( PC \) are all index policies, i.e., the solutions are memoryless and they depend only on the instantaneous values of the system variables.

**B. Performance Analysis**

Recall that \( A(t) \) is the original data arrival and \( R(t) \) is the amount of data admitted to the data queue. 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. In the following theorem, we show that this is not the case. Indeed, the admission rate associated with \( AC \) 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 \( \mathbb{R}^+ \cup \{0\} \), and its slope at 0 satisfies

\[
0 \leq \beta = U'(0) < \infty, \tag{24}
\]

2) \( 0 \leq \limsup_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} A^2(t) < \infty \),

then \( TC \) achieves:

\[
\liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} U(\mu(t)) \geq \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} U(\mu^*(t)) - O\left( \frac{1}{V} \right),
\]

**PC achieves:**

\[
\liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} R_e(P(t)) \geq \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} R_e(P^*(t)) - O\left( \frac{1}{V} \right),
\]

and \( AC \) achieves:

\[
q_d(t) \leq \beta \frac{V}{2}, \quad \forall \ t \geq 0 \tag{27}
\]

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

where \( \mu^* = \{ \mu^*(0), \mu^*(1), \ldots, \mu^*(T-1), \ldots \} \), and \( R^* = \{ R^*(0), R^*(1), \ldots, R^*(T-1), \ldots \} \) are the optimal solutions to Problem (A) and (B), respectively.

The proof of Theorem 1 can be found in Appendix A. Equation (27) shows that the data queue \( q_d \) is stable and Equation (26) shows that the average power is bounded. In Equation (24) and Equation (25), the gap between the average transmission rate and secrecy rate with our algorithm and the optimal average transmission rate and secrecy rate can be made arbitrarily small by choosing parameter \( V \) large. Similarly, by Equation (29), the admission rate can be close to optimum with large \( V \), and the optimal admission rate is actually bounded by the optimal secrecy rate. As a tradeoff, the data queue length increases as \( V \) increases. Note that the how to control the transmission rate does not really influence the optimality of the solution for Problem (B). From Equation (28), we observe that, if we plug the rates allocated by our algorithm in the utility function, it still remains close to the utility achieved by the optimal solution of Problem (B). This implies that, \( AC \) and \( TC \) allocate rates smoothly over time, as opposed to the case without a key queue. Based on this observation, combined with Equation (24), we expect the queuing delay to be smaller with a key queue. We will verify this in the following numerical example.

\[^1\text{For instance, } U(1+R) = \log(1+R).\]
C. Sample-path Delay Optimal Policy for Admissible Arrivals

Given any general time varying rates of the main and eavesdroppers channel $\tilde{R}_m = \{R_m(0), R_m(1), \ldots, R_m(T-1), \ldots\}$ and $\tilde{R}_e = \{R_e(0), R_e(1), \ldots, R_e(T-1), \ldots\}$, an arrival sample $A = \{A(0), A(1), \ldots, A(T-1), \ldots\}$ is admissible if there exists a transmission and key management policy such that the resulting average queue length is stable, i.e., $\limsup_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} q(t) < \infty$. In this section, we focus on the delay performance for admissible arrivals given sample path of secrecy rate, and only consider policies that admits all the arrivals. Our objective is that given any sample path $\tilde{R}_m$, $\tilde{R}_e$ and admissible $A$ corresponding to $\tilde{R}_m$ and $\tilde{R}_e$, to find a policy that gives the minimum average queueing delay $\limsup_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} q(t)$. Such a policy is called sample path queueing delay optimal policy.

Work conserving policy $\mu$ for single link communication:

$$\mu(t) = \min(\lambda(t) + A(t), R(t), R_{\text{max}}(t));$$

$$\mu_k(t) = \begin{cases} 0, & \text{if } \mu(t) \leq R(t) \\ \mu(t) - R(t), & \text{otherwise} \end{cases}$$

$$R_k(t) = \begin{cases} 0, & \text{if } \mu(t) > R(t) \\ R(t) - \mu(t), & \text{otherwise} \end{cases}$$

This policy satisfies all the constraints of the equivalent model characterized in Lemma 1, and $R_k(t)$ and $\mu_k(t)$ can be calculated with $\mu(t)$. The work conserving policy transmits as much data as possible in the data queue until the data queue is empty. Once the data queue is empty, the key bits will be stored in the key queue rather than being used to transmit idle packets. Such a policy keeps the remaining packets in the queue as less as possible, and at the same time does not waste any key bits. It is natural to expect this policy is sample path delay optimal.

**Proposition 1**: The above work conserving policy is sample path queueing delay optimal.

**Proof**: It is sufficient to show that $\forall t \geq 0$, the policy $\mu$ gives the smallest queue length among all policies, i.e., $q^\mu_d(t) \leq q_g^\mu_d(t)$, $\forall t \geq 0$ for any policy $\gamma$, where $q^\mu_d$ and $q_g^\mu_d$ are the resulting queue backlogs under policy $\mu$ and $\gamma$, respectively. We show this by induction. Without loss of generality, let $q^\mu_d(0) = q_g^\mu_d(0) = 0$.

I) When $t = 1$, it is apparent.

II) Suppose $q^\mu_d(t) \leq q_g^\mu_d(t)$ for $T \geq 1$ and any policy $\gamma$.

Note that under policy $\mu$, the queue evolution follows:

$$q^\mu_d(t+1) = q^\mu_d(t) - \mu(t) + A(t);$$

and for policy $\gamma$, the queue evolution follows:

$$q^\mu_d(t+1) = q^\mu_d(t) - \gamma(t) + A(t);$$

Thus, we have

$$q^\mu_d(t) = \sum_{t=0}^{T-1} A(t) - \sum_{t=0}^{T-1} \mu(t);$$

which implies

$$q^\mu_d(T) + R(T) = \sum_{t=0}^{T} A(t) + \sum_{t=0}^{T} q^\mu_d(t) + A(T).$$

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

$$\mu(T) = \min(\lambda(T) + A(T), R(T), R_{\text{max}}(T));$$

$$\gamma(T) = \min(\lambda(T) + A(T), R(T), R_{\text{max}}(T));$$

and we also have

$$q^\mu_d(T) + R(T) \leq q_g^\mu_d(T) + q_g^\mu_d(T) + A(T).$$

then combine with Equation (31) and (32), we have

$$q^\mu_d(T) + q^\mu_d(T) + \gamma(T) \leq \gamma(T) + A(T).$$

(1.1) When $q^\gamma_d(T) + R_d(T) \leq R_{\text{max}}(T)$ and $q^\mu_d(T) + R_d(T) \leq R_{\text{max}}(T)$, then continue from Equation (34), we have

$$q^\mu_d(T+1) - q^\mu_d(T+1) \leq q^\gamma_d(T) + q^\gamma_d(T) + R_d(T) - \mu(T);$$

and

$$q^\mu_d(T) - q^\mu_d(T) = 0.$$

(1.2) When $q^\gamma_d(T) + R_d(T) \leq R_{\text{max}}(T)$ and $q^\mu_d(T) + R_d(T) \geq R_{\text{max}}(T)$, then continue from Equation (33), we have

$$q^\mu_d(T+1) - q^\mu_d(T+1) \leq q^\gamma_d(T) + q^\gamma_d(T) + R_d(T) - \mu(T);$$

and

$$q^\mu_d(T) - q^\mu_d(T) = 0.$$

by the hypothesis,

(i.3) when $q^\gamma_d(T) + R_d(T) > R_{\text{max}}(T)$ and $q^\mu_d(T) + R_d(T) \leq R_{\text{max}}(T)$, then continue from Equation (32), we have

$$q^\mu_d(T+1) - q^\mu_d(T+1) \leq q^\gamma_d(T) + q^\gamma_d(T) + R_d(T) - \mu(T);$$

and

$$q^\mu_d(T) - q^\mu_d(T) = 0.$$
\( R_m(T) \), then continue from Equation (34), we have

\[
q_d^m(T + 1) = q_d^m(T + 1) \\
\leq q_d^m(T) + 2q_b^m(T) + R_m(T) - \mu(T) \\
\leq q_d^m(T) - R_s(T) + q_b^m(T) + R_s(T) - \mu(T) \\
= q_d^m(T) - q_b^m(T) + R_s(T) = R_s(T) = 0.
\]

(i.4) when \( q_b^m(T) + R_s(T) > R_m(T) \) and \( q_d^m(T) + R_s(T) > R_m(T) \), then continue from Equation (33), we have

\[
q_d^m(T + 1) = q_d^m(T) + 1 \\
\leq q_d^m(T) + 2q_b^m(T) + R_m(T) - \mu(T) \\
\leq q_d^m(T) - R_s(T) + q_b^m(T) + R_s(T) - \mu(T) \\
= q_d^m(T) - q_b^m(T) + R_s(T) = R_s(T) = 0.
\]

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

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

\[
\mu(T) = \min\{q_d^m(T) + A(T), R_m(T)\}, \\
\gamma(T) = \min\{q_b^m(T) + \mu(T), R_m(T), R_m(T)\}.
\]

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

(ii.2) when \( q_d^m(T) + A(T) > R_m(T) \), then

\[
q_d^m(T + 1) = q_d^m(T) + 1 \\
\leq q_d^m(T) + 2q_b^m(T) + R_m(T) - \mu(T) \\
< \sum_{t=0}^{\infty} R_s(t) = R_s(T) = 0.
\]

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

\[\text{V. Numerical Example}\]

In this section we simulate our algorithms and numerically compare them with the optimal performance. In the simulation, the number of time slots is \( T = 10^6 \). We use the utility function \( \frac{1}{T} + \frac{1}{x} \) for each slot. The main channel gain is uniformly distributed over \([0, 45]\) and the eavesdropper channel gain is uniformly distributed over \([0, 5]\). We use rate power function \( R_m = 10 \times \log(1 + g_m P) \) and \( R_e = 10 \times \log(1 + g_e P) \) for each slot. The average power upper bound is 1 and the peak power is 2. We also set the virtual key queue parameter \( \epsilon = 0.01 \). As shown in Figure 2 (a), the power controller achieves the optimal average secrecy rate \( R_s = 28.3 \) as increasing \( V \).

![Fig. 2. Performance Evaluation of PC, AC, and TC with respect to the solutions of Problem (A) and (B) under Poisson Arrivals: (a) Control Parameter \( V \) vs. Average Secrecy Rate; (b) Control Parameter \( V \) vs. Average Admissibility Rate; (c) Control Parameter \( V \) vs. Average Utility of Transmission Rate; (d) Throughput vs. Delay Curve]

Figure 2 illustrates the same scenario, with a more bursty arrival process. This time, \( A(t) = 0 \) w.p. \( \frac{1}{2} \) and \( A(t) = 50 \) w.p. \( \frac{1}{2} \) independently for each time slot. Consequently, \( \tilde{A} = 25 < \tilde{R}_s \). Similar observations to the previous case can be made with this arrival process, but the delay performance with a key queue is now much better than that without a key queue, for bursty arrivals. Furthermore, in this case, the arrivals are admissible, we also plotted the optimal delay curve in Figure 2 (c) and (d) given the output secrecy sample of the power controller.

\[\text{VI. Conclusion}\]

In this paper, we considered a single-user secure data communication system and addressed two separate problems, in order to achieve optimal secrecy rate and admitted arrival rate, and small queueing delay, under an average power constraint. We proposed a transmission controller, a power controller and an admission controller based on simple index policies that do not rely on any prior statistical information on the data arrival process. We showed that our controller pair has a provably efficient performance. Also, we illustrated via simulations that the use of a key queue reduces the queueing 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. When the arrival is admissible given sample path secrecy rate, we provide a rate allocation policy that is sample path queueing delay optimal.

REFERENCES


APPENDIX

A. Proof of Theorem 1

Proof of Equation (27): Equation (27) directly follows from the following lemma:

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

\[ q_d(t) \leq \frac{\beta V}{2}, \quad q_k(t) \leq \frac{\beta V}{2}, \quad q_p(t) \leq \frac{V}{2}. \]

Proof: Since \( U(\cdot) \) is concave on \( R^+ \cup \{0\} \), we have \( U(\mu(t)) \leq U(0) + \beta \mu(t) \), \( \forall t \geq 0 \), where \( 0 \leq \beta = U'(0) < \infty \). Then, \( \frac{\beta V}{2} U(\mu(t)) - \tilde{q}_k(t) \mu(t) \leq \frac{\beta V}{2} U(0) + \frac{\beta V}{2} \mu(t) - \tilde{q}_k(t) \mu(t) \) 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 \( \frac{\beta V}{2} U(\mu(t)) - \tilde{q}_k(t) \mu(t) \leq \frac{\beta V}{2} U(0) \). However, TC chooses \( \mu(t) \) that maximizes \( \frac{\beta V}{2} U(\mu(t)) - \tilde{q}_k(t) \mu(t) \), which means \( \frac{\beta V}{2} U(\mu(t)) - \tilde{q}_k(t) \mu(t) \geq \frac{\beta V}{2} U(0) \) since \( 0 \in \Pi(t) \). Then, we must have \( \beta V \mu(t) - \tilde{q}_k(t) \mu(t) \geq 0 \), i.e.,

\[ \tilde{q}_k(t) \mu(t) \leq \frac{\beta V}{2} \mu(t). \]  

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 (17). Otherwise, \( \mu(t) \neq 0 \), and by Equation (35), we have \( \tilde{q}_k(t) \leq \frac{\beta V}{2} \mu(t) \).

We have \( q_d(t) \leq \frac{\beta V}{2} \) can be obtained using the same argument.
Since
\[
\left( \log \left( \frac{1 + P(t)h_m(t)}{1 + P(t)h_e(t)} \right) \right)^+ = \left( \log \left( 1 + \frac{P(t)[h_m(t) - h_e(t)]}{1 + P(t)h_e(t)} \right) \right)^+ \leq \left( \log \left( 1 + \frac{P(t)[h_m(t) - h_e(t)]}{1 + P(t)h_e(t)} \right) \right)^+ = \log \left( 1 + \frac{P(t)[h_m(t) - h_e(t)]}{1 + P(t)h_e(t)} \right) \leq \frac{P(t)[h_m(t) - h_e(t)]}{1 + P(t)h_e(t)}, \quad \forall t \geq 0.
\]
Similarly, we have \( {\tilde{q}}_p(t) \leq h_m(t) \leq h_M < \infty \), where \( h_M = \max_{t>0} h_m(t) \).

**Proof of Equation (24):** We define the Lyapunov function \( L(\tilde{q}_k(t)) = (\tilde{q}_k(t))^2 \), and \( \Delta(\tilde{q}_k(t)) = L(\tilde{q}_k(t+1)) - L(\tilde{q}_k(t)) \). From Equation (17), we have
\[
(\tilde{q}_k(t+1))^2 \leq (\tilde{q}_k(t) - \epsilon)^2 + (\mu(t) - R_s(t) + I_0(t))^2 + 2(\tilde{q}_k(t) - \epsilon)^+ (\mu(t) - R_s(t) + I_0(t)) \leq (\tilde{q}_k(t))^2 + \epsilon^2 + (1 + R_{max})^2 + 2\epsilon R_{max} + 2\tilde{q}_k(t)I_0(t) + 2\tilde{q}_k(t)\mu(t) - 2\tilde{q}_k(t)R_s(t),
\]
then
\[
\Delta(\tilde{q}_k(t)) \leq VU(\mu(t)) - VU(\mu(t)) + \epsilon^2 + (1 + R_{max})^2 + 2\epsilon R_{max} + 2\tilde{q}_k(t)I_0(t) + 2\tilde{q}_k(t)\mu(t) - 2\tilde{q}_k(t)R_s(t).
\]

\[\Delta = \Delta(\tilde{q}_k(t)) \leq VU(\mu(t)) - VU(\mu(t)) + \epsilon^2 + (1 + R_{max})^2 + 2\epsilon R_{max} + 2\tilde{q}_k(t)I_0(t) + 2\tilde{q}_k(t)\mu(t) - 2\tilde{q}_k(t)R_s(t).
\]

It is apparent that \( TC \) is trying to maximize the value of the term \( \left[ \frac{1}{2}VU(\mu(t)) - \tilde{q}_k(t)\mu(t) \right] \). Since the optimal solution for Problem (A) may not be unique, we let \( \mu^* \) be the optimal solution set and \( \mu^* \in U^* \) be any optimal solution, for Problem (A) given any sample path. Since the constraint set \( II(t) \) is queue dynamic related, it is possible that \( \mu^*(t) \notin II(t) \).

**Lemma 3:** In slot \( s \), if by solving \( TC \), we get \( \frac{1}{2}VU(\mu(t)) - \tilde{q}_k(t)\mu(t) \), then \( \mu(t) < \mu^*(t) \) and \( I_0(t') = 1 \) for some \( t' \leq t \) and \( t - t' < \infty \).

**Proof:** The proof is given in [23] as well.

Let \( N = \max\{n : \forall t \geq 0, R_s(t) = 0, \forall t[t, t + n]\}. \) By using Lemma 3 and \( \mu(t), \mu^*(t) \leq R_{max}, \forall t \geq 0 \), we have \( N < \infty \) and
\[
\Delta \leq VU(\mu(t)) - VU(\mu^*(t)) + \epsilon^2 + (1 + 2R_{max})^2 + 2\epsilon R_{max} + 2\tilde{q}_k(t)\mu^*(t) - 2\tilde{q}_k(t)R_s(t).
\]

\[\text{Lemma 4:}
\]
\[
1 \quad \limsup_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} \tilde{q}_k(t)[\mu^*(t) - R_s(t)] \leq O\left( \frac{1}{\sqrt{V}} \right).
\]
\[
1 \quad \limsup_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} \tilde{q}_p(t)[P^* - P_{avg}] \leq O\left( \frac{1}{\sqrt{V}} \right).
\]

**Proof:** The proof is similar as in [23].

**Lemma 5:** If \( \tilde{q}_k(t) \leq \frac{\sqrt{V}}{2} \), then \( q_k(t) < \infty \).

**Proof:** The proof is given in [23] as well.

**Lemma 6:** If both the key queue \( q_k(t) \) and virtual key queue \( \tilde{q}_k(t) \) are strongly stable, i.e.,
\[
\limsup_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} (q_k(t) + \tilde{q}_k(t)) < \infty,
\]
then \( \limsup_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} I_o(t) \leq \epsilon \).

If the virtual power queue \( \tilde{q}_p(t) \) is strongly stable, then
\[
\limsup_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} P(t) \leq P_{avg}.
\]

**Proof:** The proof is similar as in [23].

By summing from 0 to \( T - 1 \), dividing by \( T \) and \( V \), taking \( \liminf_{T \to \infty} \) over Equation (36), combined with Lemma 2, Lemma 5, Lemma 6, and Lemma 4, we get
\[
\liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} U(\mu(t)) \geq \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} U(\mu^*(t)) - O\left( \frac{1}{\sqrt{V}} \right) - \epsilon(NU(R_{max}) + \beta).
\]

By letting \( \epsilon \to 0 \), we obtain Equation (24).

**Proof of Equation (26):** Equation (26) follows from Lemma 2 and Lemma 6.

**Proof of Equation (25):** We define \( L(\tilde{q}_p(t)) = (\tilde{q}_p(t))^2 \), and \( \Delta(\tilde{q}_p(t)) = L(\tilde{q}_p(t+1)) - L(\tilde{q}_p(t)) \). Both \( P(t) \) and \( P^* \) are within \([0, P_{peak}]\), by Equation (19), we have
\[
\Delta = \Delta(\tilde{q}_p(t)) \leq VR_s(t) - 2\left[ \frac{1}{2} \left( \log \left( \frac{1 + P(t)h_m(t)}{1 + P(t)h_e(t)} \right) \right)^+ - \tilde{q}_p(t)P(t) \right] - 2\tilde{q}_p(t)P_{avg} + P_{peak}^2 + \tilde{q}_p(t)P^*(t) - 2\tilde{q}_p(t)P_{avg} + P_{peak}^2 + P_{peak}^2.
\]

By summing from 0 to \( T - 1 \), dividing by \( T \) and \( V \), taking \( \liminf_{T \to \infty} \) over both sides, combined with Lemma 4, we get
\[
\liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} R_s(P(t)) \geq \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} R_s(P^*(t)) - O\left( \frac{1}{\sqrt{V}} \right).
\]

**Proof of Equation (28) and Equation (29):** The proof is given in [23] as well.