Towards Achieving Full Secrecy Rate and Low Delays in Wireless Networks

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

C. 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*—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: (1) 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; (2) 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 have 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 queueing-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. In the first one, the objective is to maximize a long-term average utility, which is a function of the number of secure packets transmitted in each time slot. In the second problem, the objective is to maximize the long term admitted data rate under an average power constraint, while keeping data queue stable. In both problems, it is desirable to securely send as much data as possible at all times. Thus, 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 cross-layer solution, composed of three con-

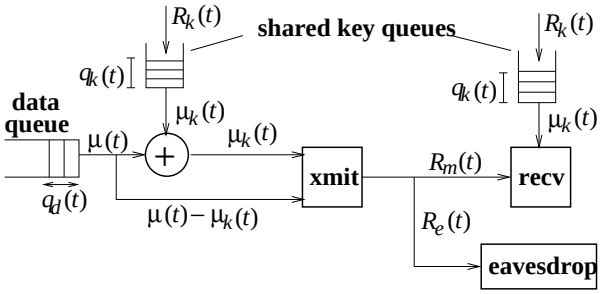

Fig. 1. System model

trollers, working at different layers. The transmission controller chooses the key generation (and transmission) rate along with the secure data transmission rate in each time slot. The admission controller 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. The power controller allocates the power such that the secrecy rate is maximized under the average power constraint. All 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 queueing 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 $\vec{h}_m = \{h_m(0), h_m(1), \ldots, h_m(T-1), \ldots\}$ and $\vec{h}_e = \{h_e(0), h_e(1), \ldots, h_e(T-1), \ldots\}$, 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 $R_m(t) = \log\big(1 + P(t)h_m(t)\big)$ and $R_e(t) = \log\big(1 + P(t)h_e(t)\big)$, 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 $R_s(t) = \big(R_m(t) - R_e(t)\big)^+$, $\forall t \geq 0$, 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 $0 \leq \mu(t) \leq \min[q_k(t) + R_s(t), R_m(t)]$, $0 \leq \mu_k(t) \leq \min[\mu(t), R_e(t)]$, and $\big(\mu(t) - \mu_k(t)\big) + R_k(t) = R_s(t)$.

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 queueing 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:

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

$$\text{s.t.} \qquad q_k(t+1) = q_k(t) + R_s(t) - \mu(t), \tag{1}$$

$$0 \leq \mu(t) \leq \min\big[q_k(t) + R_s(t), R_m(t)\big], \tag{2}$$

$$0 \leq \mu_k(t) \leq \min\big[\mu(t), R_e(t)\big], \tag{3}$$

$$\big(\mu(t) - \mu_k(t)\big) + R_k(t) = R_s(t), \tag{4}$$

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

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.

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

s.t.

$$q_d(t+1) = \big(q_d(t)-\mu(t)\big)^+ + R(t), \tag{5}$$

$$q_k(t+1) = q_k(t) + R_s(t) - \mu(t), \tag{6}$$

$$0 \le R(t) \le A(t), \tag{7}$$

$$0 \le \mu(t) \le \min\big[q_k(t)+R_s(t), R_m(t)\big], \tag{8}$$

$$\limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} q_d(t) < \infty, \tag{9}$$

$$0 \le \mu_k(t) \le \min\big[\mu(t), R_e(t)\big], \tag{10}$$

$$\big(\mu(t)-\mu_k(t)\big) + R_k(t) = R_s(t), \tag{11}$$

$$R_s(t) = \big(R_m(t)-R_e(t)\big)^+, \tag{12}$$

$$R_m(t) = \log\big(1+P(t)h_m(t)\big), \tag{13}$$

$$R_e(t) = \log\big(1+P(t)h_e(t)\big), \tag{14}$$

$$\limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} P(t) \le P_{avg}, \tag{15}$$

$$0 \le P(t) \le P_{peak}. \tag{16}$$

Note that, the maximum achievable average secrecy rate, which happens to be the objective function here, is upper bounded by the average secrecy capacity $\bar{R}_s$. 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, $\bar{R}_s$ 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 outage 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:

$$\tilde{q}_k(t+1) = \big((\tilde{q}_k(t)-\epsilon)^+ + \mu(t) - R_s(t) + I_o(t)\big)^+, \tag{17}$$

where $\epsilon > 0$ can be chosen arbitrarily, and

$$I_o(t) = \mathbf{1}_{\textit{key queue hits zero state from higher states in slot } t} = \begin{cases} 0 & \text{if } \mu(t)=0 \text{ or } \mu(t) < q_k(t)+R_s(t) \\ 1 & \text{otherwise} \end{cases} \tag{18}$$

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:

$$\tilde{q}_p(t+1) = \big(\tilde{q}_p(t) - P_{avg}\big)^+ + P(t). \tag{19}$$

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 $V \in \Re^+$ to be the control parameter of our algorithm. In slot t, the controller solves the following optimization problem and transmits with the calculated rate:

$$\max_{\mu(t)\in\Pi(t)} \frac{V}{2}U\big(\mu(t)\big) - \tilde{q}_k(t)\mu(t), \tag{20}$$

where $\Pi(t) = \{\mu(t) : 0 \le \mu(t) \le \min[q_k(t)+R_s(t), R_m(t)]\}$ is a compact and nonempty set. Furthermore, key generation and usage rates $(R_k(t), \mu_k(t))$ are chosen as follows: If $\mu(t) > R_s(t)$, then $R_k(t) = 0$ and $\mu_k(t) = \mu(t) - R_s(t)$; if $\mu(t) \le R_s(t)$, then $\mu_k(t) = 0$ and $R_k(t) = R_s(t) - \mu(t)$. This ensures that constraint $\big(\mu(t)-\mu_k(t)\big) + R_k(t) = R_s(t)$ is satisfied. It is not surprising that $\mu_k(t)R_k(t) = 0$, since any solution with $\mu_k(t) > 0$ 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. Note that $R_s(t) = \big(R_m(t)-R_e(t)\big)^+ \ge R_m(t)-R_e(t)$, then for $\mu(t) > R_s(t)$, we have $\mu_k(t) = \mu(t) - R_s(t) \le R_m(t) - R_s(t) \le R_e(t)$. This leads to constraint $0 \le \mu_k(t) \le \min[\mu(t), R_e(t)]$ 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:

$$\max_{0\le R(t)\le A(t)} \frac{V}{2}U\big(R(t)\big) - q_d(t)R(t). \tag{21}$$

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

$$\max_{0\le P(t)\le P_{peak}} \frac{V}{2}\left(\log\left(\frac{1+P(t)h_m(t)}{1+P(t)h_e(t)}\right)\right)^+ - \tilde{q}_p(t)P(t). \tag{22}$$

Note that, when $h_m(t) < h_e(t)$, i.e., the power gain of the eavesdropper is larger, $P(t) = 0$ is the solution of Equation (22). On the other hand, when $h_m(t) \ge h_e(t)$, we have

$$\left(\log\left(\frac{1+P(t)h_m(t)}{1+P(t)h_e(t)}\right)\right)^+ = \log\left(\frac{1+P(t)h_m(t)}{1+P(t)h_e(t)}\right)$$
$$= \log\left(\frac{h_m(t)}{h_e(t)} - \frac{\frac{h_m(t)}{h_e(t)}-1}{1+P(t)h_e(t)}\right), \tag{23}$$

which is concave in $P(t)$. Thus, 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 $\Re^+\bigcup\{0\}$, and its slope at 0 satisfies[1] $0 \le \beta = U'(0) < \infty$,

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

then *TC* achieves:

$$\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(\mu(t)) \ge \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(\mu^*(t)) - O(\frac{1}{V}), \tag{24}$$

PC achieves:

$$\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R_s\big(P(t)\big) \ge \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R_s\big(P^*(t)\big) - O(\frac{1}{V}), \tag{25}$$

$$\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}P(t) \le P_{avg}, \tag{26}$$

and *AC* achieves:

$$q_d(t) \le \beta\frac{V}{2}, \quad \forall\ t \ge 0 \tag{27}$$

$$\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(R(t)) \ge \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(R^*(t)) - O(\frac{1}{V}), \tag{28}$$

$$\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R(t) \to \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R^*(t)\ as\ V\to\infty, \tag{29}$$

where $\vec{\mu}^* = \{\mu^*(0), \mu^*(1), \ldots, \mu^*(T-1), \ldots\}$, and $\vec{R}^* = \{R^*(0), R^*(1), \ldots, R^*(T-1), \ldots\}$ 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 queueing delay to be smaller with a key queue. We will verify this in the following numerical example.

C. Sample-path Optimal Policy for Time-Averaged Queue Size

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

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

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 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. Furthermore, we assume constant transmission power. Next, we specify the *work-conserving policy*, μ, for transmission control and show that it achieves the minimum time-averaged queue length $\limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} q_d(t)$, for any sample path for the channel rates $\vec{R}_m$, $\vec{R}_e$, and any associated admissible arrival process, $\vec{A}$. Hence, the work conserving policy is the sample-path optimal policy for the average queue size.

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

$$\begin{aligned}\mu(t) &= \min\{q_d(t)+A(t), q_k(t)+R_s(t), R_m(t)\},\\ \mu_k(t) &= \begin{cases} 0, & \text{if } \mu(t) \le R_s(t)\\ \mu(t)-R_s(t), & \text{otherwise}\end{cases}\\ R_k(t) &= \begin{cases} 0, & \text{if } \mu(t) > R_s(t)\\ R_s(t)-\mu(t), & \text{otherwise}\end{cases}\end{aligned} \tag{30}$$

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 the time-averaged queue size.

Proof: The proof is provided in Appendix B.

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 $U(x) = \log_2(1+x)\ \forall x \ge 0$. 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 $R_m = 10*\log(1+g_m P)$ and $R_e = 10*\log(1+g_e P)$ 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 $\bar{R}_s = 28.3$ as increasing V.

We first use an arrival process $A(t),\ t \ge 0$, that is composed of independent Poisson random variables with mean 30 each slot. In this example, $\bar{A} > \bar{R}_s$. We run the simulation for different values of the control coefficient V and compare the results with the optimal value[2]. Figure 2(b) shows that, as V increases, the average admission rate (both with and without a key queue) also increases to the optimum, which is consistent with Equation (29). In Figure 2 (c), one can observe that, as V increases, the average utility of the transmission rate with a key queue approaches the optimal value, which is consistent with Equation (24). For the case without a key queue, the average utility is smaller but not much in the Poisson arrival scenario. As a result, the delay performance with a key queue is also only a little better as we can see in Figure 2(d) for Poisson arrivals.

[2]Note that the optimal value for Problem (A) is upper bounded by $U(\bar{R}_s)$ and for Problem (B) is $\min[\bar{A}, \bar{R}_s]$.

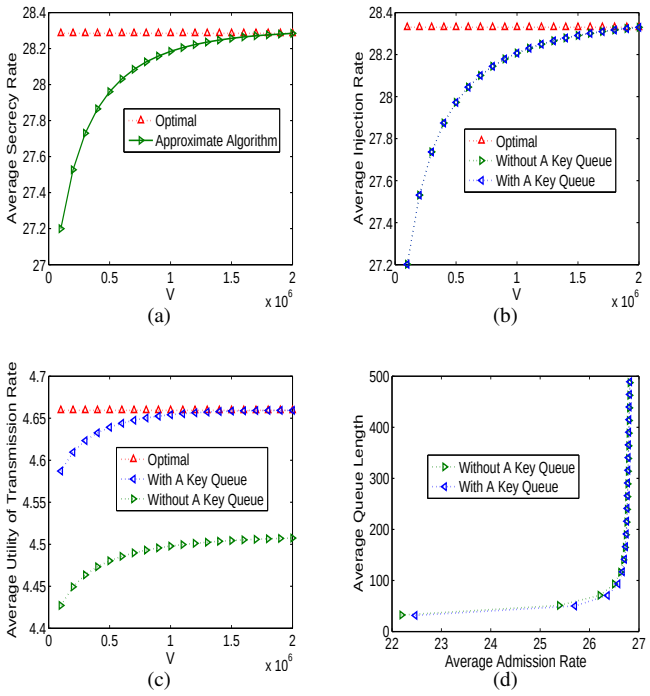

Fig. 2. Performance Evaluation of *PC*, *AC*, and *TC* with respect to the solutions of Problem (A) and (B) under Poisson Arrivals: (a) Control Parameter V vs. Average Secrecy Rate; (b) Control Parameter V vs. Average Admission Rate; (c) Control Parameter V vs. Average Utility of Transmission Rate; (d)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

Figure 3 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, $\bar{A} = 25 < \bar{R}_s$. 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 3 (c) and (d) given the output secrecy sample of the power controller.

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

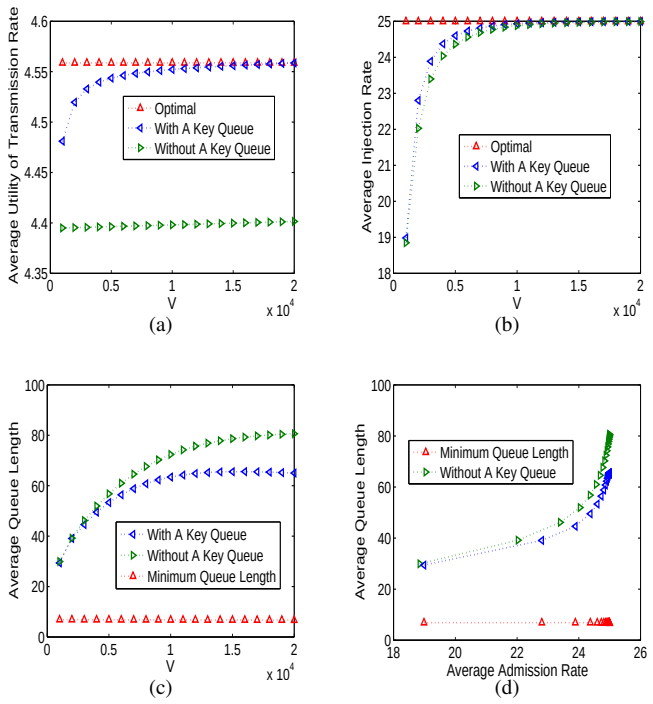

Fig. 3. Performance Evaluation of *TC* and *AC* for Problem (A) and (B) under Variable Arrivals

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 *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, 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*, 2009, to appear.

[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, to appear.

[9] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," 2010, submitted.

[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," *CoRR*, vol. abs/1101.3444, 2011.

[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, "Towards Achieving Full Secrecy Rate in Wireless Networks: A Control Theoretic Approach," San Diego, CA, ITA 2011.

[24] ——, "Near Optimal Power and Rate Control of Multi-hop Sensor Networks with Energy Replenishment: Basic Limitations with Finite Energy and Data Storage," in *IEEE Transactions on Automatic Control*, accepted.

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

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

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

$$\tilde{q}_k(t)\mu(t) \leq \frac{\beta V}{2}\mu(t). \tag{31}$$

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 $\tilde{q}_k(t)\le\tilde{q}_k(t-1)\le\frac{\beta V}{2}$ by Equation (17). Otherwise, $\mu(t)\neq 0$, and by Equation (31), we have $\tilde{q}_k(t)\le\frac{\beta V}{2}$.

$q_d(t)\le\frac{\beta V}{2}$ can be obtained using the same argument.

Since

$$\begin{aligned}&\left(\log\left(\frac{1+P(t)h_m(t)}{1+P(t)h_e(t)}\right)\right)^+\\=&\left(\log\left(1+\frac{P(t)\big(h_m(t)-h_e(t)\big)}{1+P(t)h_e(t)}\right)\right)^+\\\le&\left(\log\left(1+\frac{P(t)\big|h_m(t)-h_e(t)\big|}{1+P(t)h_e(t)}\right)\right)^+\\=&\log\left(1+\frac{P(t)\big|h_m(t)-h_e(t)\big|}{1+P(t)h_e(t)}\right)\\\le&\frac{P(t)\big|h_m(t)-h_e(t)\big|}{1+P(t)h_e(t)},\quad\forall t\ge 0.\end{aligned}$$

Similarly, we have $\tilde{q}_p(t)\le h_m(t)\le h_M<\infty$, where $h_M=\max_{t\ge0}h_m(t)$. ■

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

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

then

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

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

Lemma 3: In slot t, if by solving *TC*, we get $\left[\frac{V}{2}U(\mu(t))-\tilde{q}_k(t)\mu(t)\right]<\left[\frac{V}{2}U(\mu^*(t))-\tilde{q}_k(t)\mu^*(t)\right]$, then $\mu(t)<\mu^*(t)$ and $I_o(t')=1$ for some $t'\le t$ and $t-t'<\infty$.

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

Let $N=\max\{n:\ \textit{for any } t\ge0,\ R_s(\tau)=0,\ \forall\tau\in[t,t+n]\}$. By using Lemma 3 and $\mu(t),\mu^*(t)\le R_m(t)\le R_{max},\ \forall t\ge0$, we have $N<\infty$ and

$$\begin{aligned}\Delta\le&VU(\mu(t))-VU(\mu^*(t))+\epsilon^2+\big(1+R_{max}\big)^2+2\epsilon R_{max}\\&+2\tilde{q}_k(t)\Big[\mu^*(t)-R_s(t)\Big]+V(\beta+NU(R_{max}))I_o(t).\end{aligned}\tag{32}$$

Lemma 4:

$$\begin{aligned}\frac{1}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\tilde{q}_k(t)[\mu^*(t)-R_s(t)]\le&O(\frac{1}{V}),\\\frac{1}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\tilde{q}_p(t)[P^*(t)-P_{avg}]\le&O(\frac{1}{V}).\end{aligned}$$

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

Lemma 5: If $\tilde{q}_k(t)\le\frac{\beta V}{2}$, 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.,

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

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

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

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 (32), combined with Lemma 2, Lemma 5, Lemma 6, and Lemma 4, we get

$$\begin{aligned}\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(\mu(t))\ge&\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(\mu^*(t))-O(\frac{1}{V})\\&-\epsilon(NU(R_{max})+\beta).\end{aligned}$$

By letting $\epsilon\to0$, 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 $P^*(t)$ are within $[0,P_{peak}]$, by Equation (19), we have

$$\begin{aligned}\Delta=&\Delta(\tilde{q}_p(t))\\\le&VR_s(t)-2\left[\frac{V}{2}\left(\log\left(\frac{1+P(t)h_m(t)}{1+P(t)h_e(t)}\right)\right)^+-\tilde{q}_p(t)P(t)\right]\\&-2\tilde{q}_p(t)P_{avg}+P_{avg}^2+P_{peak}^2\\\le&VR_s\big(P(t)\big)-VR_s\big(P^*(t)\big)+2\tilde{q}_p(t)P^*(t)-2\tilde{q}_p(t)P_{avg}\\&+P_{avg}^2+P_{peak}^2.\end{aligned}$$

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

$$\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R_s(P(t))\ge\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R_s(P^*(t))-O(\frac{1}{V}).$$ ■

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

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

$$q_k^{\mu}(T) + R_s(T) = \sum_{t=0}^{T} R_s(t) - \sum_{t=0}^{T} A(t) + q_d^{\mu}(T) + A(T), \tag{33}$$

$$q_k^{\gamma}(T) + R_s(T) \leq \sum_{t=0}^{T} R_s(t) - \sum_{t=0}^{T} A(t) + q_d^{\gamma}(T) + A(T). \tag{34}$$

(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 (33) and (34), we have

$$\begin{aligned} & q_d^{\mu}(T+1) - q_d^{\gamma}(T+1) \\ \leq & q_d^{\mu}(T) - q_d^{\gamma}(T) + \gamma(T) - \mu(T) \qquad (35) \\ \leq & q_k^{\mu}(T) - q_k^{\gamma}(T) + \gamma(T) - \mu(T), \qquad (36) \end{aligned}$$

(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 (36), 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 (35), 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 (36), 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 (35), 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. ■