

Introduction

- 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.
- In the classical wiretap setting, it is well known that information theoretic secrecy at a constant bit rate is not possible at an arbitrarily low probability of outage, i.e., the *delay limited secrecy capacity* is 0.
- We utilize the wiretap channel 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.
- The outage probability can be made arbitrarily close to 0 by jointly controlling the key buffer with the transmit power.

System Model

- There is one transmitter, receiver and eavesdropper.
- In each time slot, a block of data is transmitted over N channel uses.

Problem Description

Our **goal** is to find,

- What is the maximum achievable constant (delay-limited) rate b^* achievable, subject to a given upper bound α on the outage probability and a given average power constraint \bar{P} ?

$$b^* = \max_{P(\text{outage}) \leq \alpha, \mathbb{E}[P(\mathbf{h})] \leq \bar{P}} b. \quad (1)$$

- What is the optimal power allocation to achieve b^* ?
- What is the key queue workload distribution when achieving b^* ?

There are two types of outages.

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.

We resort to a sub-optimal scheme that can approximate the original problem by two sub-problems, using which we decouple the issues of power allocation and queue control.

- The transmitted signal is corrupted by circularly symmetric complex Gaussian Noise.
- Block fading is assumed, such that the power gains of the main and eavesdropper channels at block t are denoted by $h_m(t)$ and $h_e(t)$ respectively. We further assume that channel gains are i.i.d.

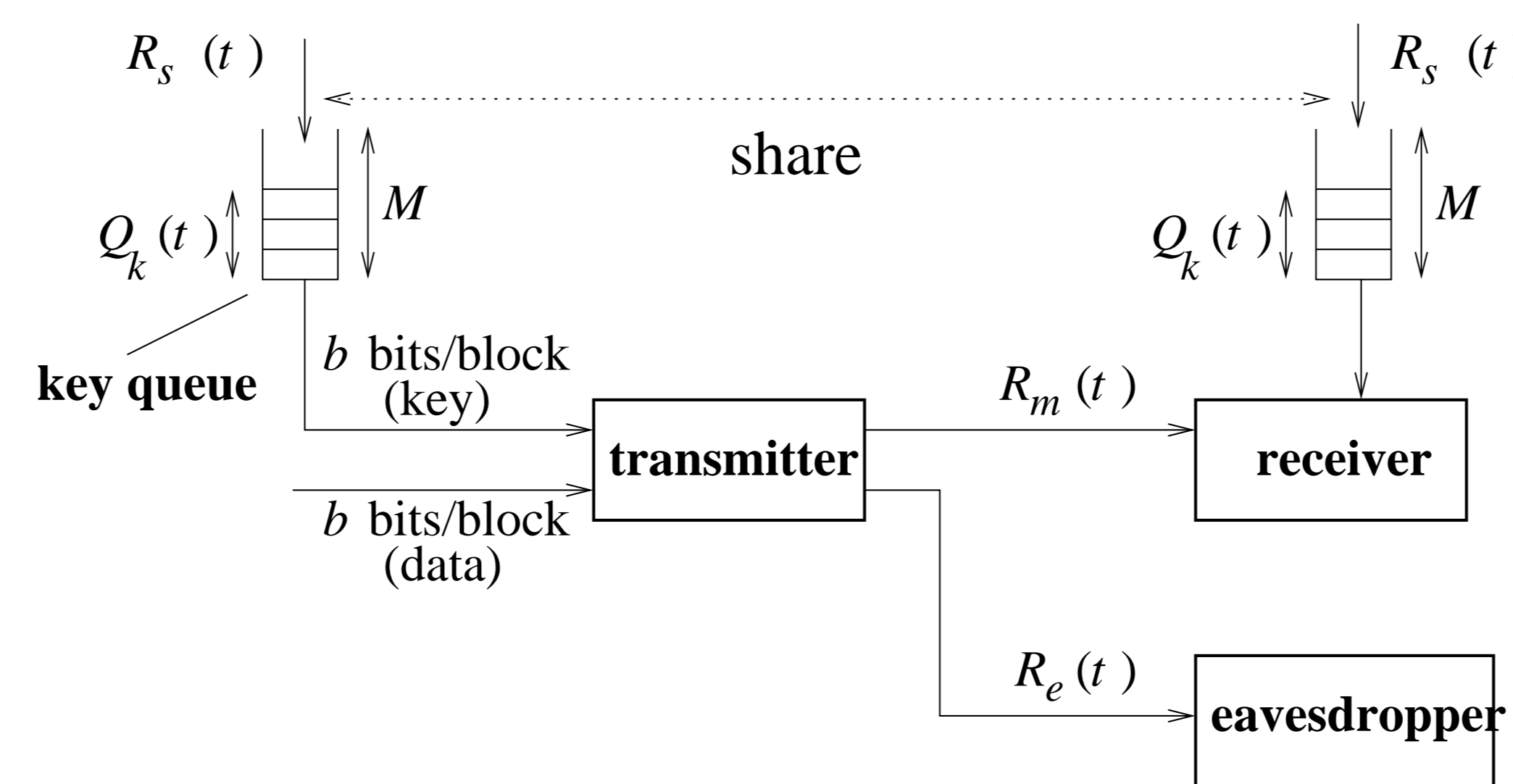


FIGURE 1: System model

Solution

1. We start with a general optimization problem that solves the maximum expected secrecy capacity $R(b, \bar{P}, \alpha_1)$ for fixed $b > 0$, α_1 and $\bar{P} > 0$,

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

subject to: $P(\mathbf{h}) \geq 0$,
 $\mathbb{E}[P(\mathbf{h})] \leq \bar{P}$,
 $\mathbb{P}[R_m^h < b] \leq \alpha_1$.

2. If

$$R(b, \bar{P}, \alpha_1) = b^*(1 - \mathbb{P}[R_m^h < b^*]), \quad (2)$$

then our system will have a zero key outage probability.

3. Find the maximum b^* that satisfies Equation (2). To this end, we develop an iterative algorithm that searches for b^* .

4. 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 unbounded as $t \rightarrow \infty$, which is untenable because in practice the key buffer size is finite. We introduce key outages to stabilize the private key queue. 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.

- Since $\{\mathbf{h}(t)\}$ is i.i.d., we drop the index t and use the notation \mathbf{h} for simplicity and let $P(\mathbf{h})$ be the power allocation function.
- We assume full channel state information (CSI).
- We define *instantaneous achievable rates* for the legitimate receiver and eavesdropper as $R_m(t)$ and $R_e(t)$ respectively. For each block t , using wiretap channel arguments, we can achieve a *secrecy rate* of

$$R_s(t) = \max\{0, [R_m(t) - R_e(t)]\}, \quad (3)$$

- Application requires a constant amount, b bits/channel use of data, which corresponds to Nb bits/block 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.

Simulations

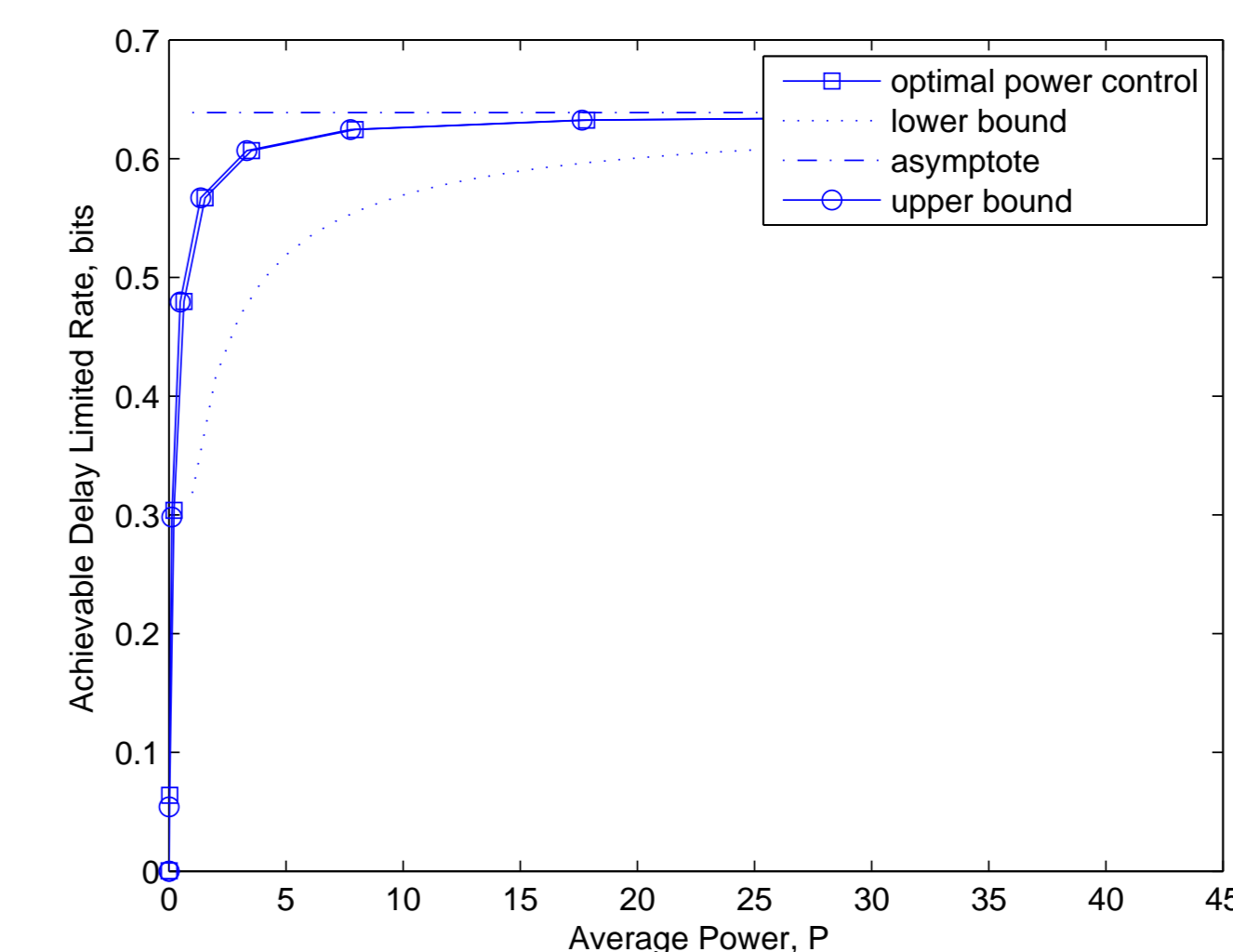


FIGURE 2: Achievable delay limited rate under optimal power control without outages for the Gaussian Channel

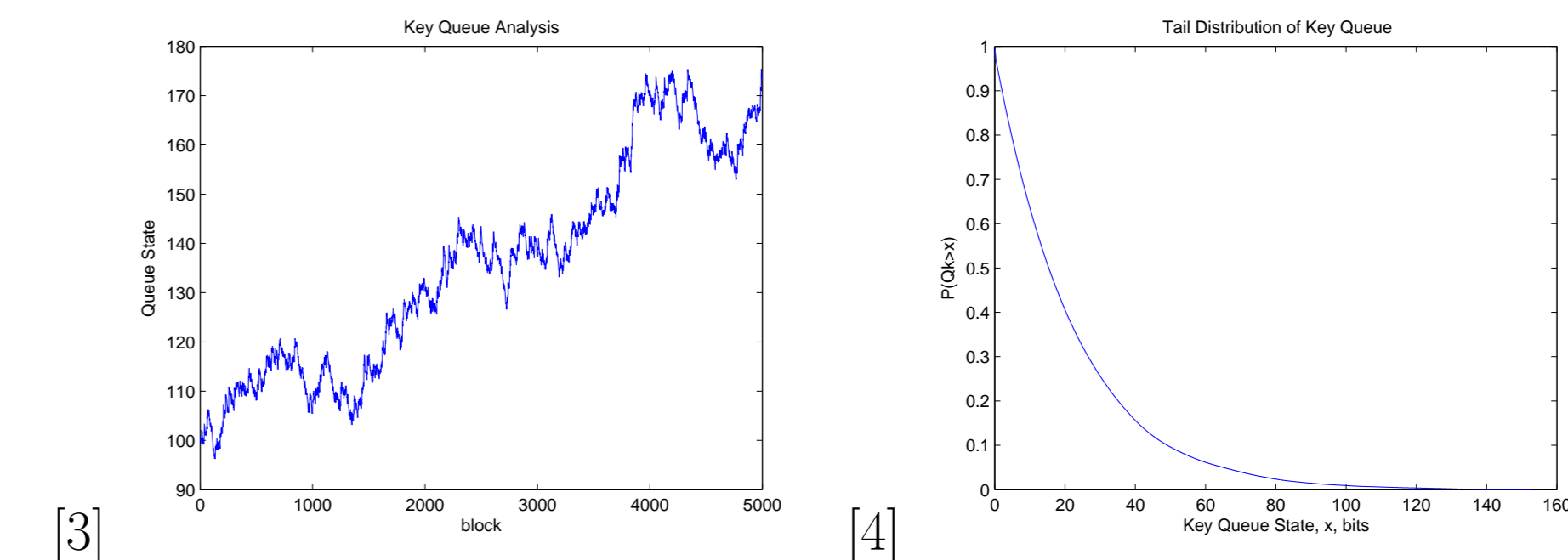


FIGURE 3: Evolution of the key queue workload under optimal control with only channel outages for Rayleigh channel

FIGURE 3: Key queue workload distribution with both channel and key outages for Rayleigh channel