On Secrecy Outage Capacity of Fading Channels Under Relaxed Delay Constraints

Onur Gungor, Can Emre Koksal, Hesham El Gamal
Department of Electrical and Computer Engineering
The Ohio State University, Columbus, 43210

Abstract—**We consider information theoretic secrecy over flat fading channels under relaxed delay constraints. More specifically, we extend the definition of outage secrecy capacity for single-input single-output single-eavesdropper case (SISOSE) to account for relaxed delay constraints, and study the fundamental limits under two different assumptions on the transmitter CSI (channel state information). First, we provide bounds on secrecy outage capacity with $k+1$ block delay constraint. We show that the bounds are tight for several special cases. We also provide a weaker lower bound that is easier to compute, and show that under low SNR, delay constraint has significant impact on secrecy outage capacity. The analysis serves as an important step towards complete characterization of information theoretic security with delay and outage constraints.**

I. Introduction

Most of the recent work on information theoretic secrecy is, arguably, inspired by Wyner's wiretap channel [2]. In this setup, a passive eavesdropper which has infinite computational resources, listens to the communication between two legitimate nodes over a separate communication channel. Wyner defined **secrecy capacity** as the maximum achievable rate subject to zero mutual information rate between the transmitted message and the signal received by the eavesdropper. In the additive Gaussian noise scenario [3], secrecy capacity turned out to be the difference between the capacities of the legitimate and eavesdropper channels. Therefore, if the eavesdropper channel has a higher channel gain, information theoretic secure communication is not possible over the main channel. Recent works have shown how to exploit multipath fading to avoid this limitation by opportunistically exploiting the instants when the main channel enjoys a higher gain than the eavesdropper channel [4], [5], [7]. This opportunistic secrecy approach achieves non-zero **ergodic secrecy capacity** even when **on average** the eavesdropper channel has favorable conditions over the legitimate channel, or when the eavesdropper channel state information is not available at the legitimate nodes [4].

The ergodic result in [4] applies only to delay tolerant traffic, e.g., file downloads. Early attempts at characterizing the secrecy capacity under strict delay limitations drew the negative conclusion that non-zero delay limited secrecy rates are not achievable for fading channels due to **secrecy outage** events corresponding to the instants when the eavesdropper channel gain is larger than the main one [6], [8]. Later, it was shown in [11] that a non-zero delay limited secrecy rate could be achieved by introducing **private key queues** at both the transmitter and the receiver. These queues are used to store private key bits that are shared **opportunistically** between the legitimate nodes when the main channel is more favorable than the one seen by the eavesdropper. These key bits are used later to secure the delay sensitive data using the Vernam one time pad approach [1]. Hence, secrecy outages are avoided by simply storing the secrecy generated previously, in the form of key bits, and using them whenever the channel conditions are more advantageous for the eavesdropper. The technique is further developed in [12] to obtain sharp characterizations of the outage secrecy capacity under strict delay, and ϵ probability of secrecy outage. The optimal power allocation in order to achieve the secrecy outage capacity turned out to be a time-sharing of secure waterfilling power policy, which maximizes the ergodic secret key generation rate without any delay constraint, and channel inversion policy, which achieves the delay limited rate. Due to the use of channel inversion power control, which does not maximize the ergodic secrecy rate, outage secrecy capacity is smaller than ergodic secrecy capacity under an average power constraint. It was shown that, under high SNR, the constraining effect of delay diminishes, hence the gap between ergodic secrecy capacity, and outage secrecy capacity narrows down. However, under low SNR, there is a significant gap between the two.

In this work, we attempt to bridge the gap between ergodic secrecy capacity with no delay limitations, and outage secrecy capacity with strict delay limitations. More specifically, we consider SISOSE setting under block fading channels, and provide bounds for the outage secrecy capacity under delay constraint of $k+1$ blocks and ϵ probability of outage, where (i) perfect knowledge about the main and eavesdropper channels are available *causally* at the transmitter, and (ii) only the main channel state information (CSI) is available at the transmitter. The achievable scheme involves use of $k+1$ data queues as well as secret key queues at the transmitter and the legitimate receiver. Then, we investigate several special cases, including relaxed delay ($k = \infty$), strict delay ($k = 1$), and zero outage probability ($\epsilon = 0$), with our focus on rate and power allocation policies. We show that the achievable scheme simplifies for these cases. Using the intuition gained, we provide weaker capacity bounds for the general case that are easier to compute, and numerically evaluate them. We conclude that delay constraints have significant impact on secrecy outage capacity under low SNR. Due to space limitations, the proofs

This work is supported in part by QNRF under grants NPRP 5-559-2-227, and by NSF under grants CNS-1054738, CNS-0831919, CCF-0916664.

of results are omitted.

II. System Model

We adopt a block fading channel model, in which the channel is assumed to be constant over a block, and changes randomly from one block to the next. The communication period consists of B blocks, where blocks are formed of N channel uses[1]. Within each block b, the observed signals at the receiver and at the eavesdropper are:

$$\mathbf{Y}(b) = G_m(b)\mathbf{X}(b) + \mathbf{W}_m(b)$$
$$\mathbf{Z}(b) = G_e(b)\mathbf{X}(b) + \mathbf{W}_e(b),$$

respectively, where $\mathbf{X}(b) \in \mathbb{C}^N$ is the transmitted signal, $\mathbf{Y}(b), \mathbf{Z}(b) \in \mathbb{C}^N$ are received signals by the legitimate receiver and the eavesdropper respectively, and $\{\mathbf{W}_m(b)\}_{b=1}^B$ and $\{\mathbf{W}_e(b)\}_{b=1}^B$ are two mutually independent i.i.d. standard Normal vector processes that are also independent of other random variables. The power gains of the fading channels are denoted by $H_m(b) = |G_m(b)|^2$ and $H_e(b) = |G_e(b)|^2$. We use the vector notation $\mathbf{H}(\cdot) = [H_m(\cdot)\ H_e(\cdot)]$ for simplicity, and use $\mathbf{H}^b = \{\mathbf{H}(b')\}_{b'=1}^b$ to denote the set of channel gains $\mathbf{H}(b')$ observed until block b, and use backslash as relative complement operator, e.g., $\mathbf{H}^B \backslash \mathbf{H}(b)$ denotes the set of gains of all blocks except b. We use identical notation for other parameters as well, and denote the sample realization sequences with lowercase letters. We assume that the probability density function of instantaneous channel gains, denoted as $f(\mathbf{h})$, is well defined, and is known by all parties. We only consider two different cases of transmitter CSI: *Full CSI*, in which the transmitter has perfect knowledge of the **causal**[2] main and eavesdropper channel gains, and *main CSI*, in which the transmitter only knows causal main channel gains. In both cases, the eavesdropper has complete knowledge of both the main and the eavesdropper channels. Let $P(b)$ denote the power allocated at block b. We consider an average power constraint such that for some $P_{\text{avg}} > 0$,

$$\limsup_{B\to\infty} \frac{1}{B}\sum_{b=1}^{B} P(b) \le P_{\text{avg}} \tag{1}$$

For $k \ge 0$, a $k+1$ block delay system can be described as follows. Let $\{W(b)\}_{b=1}^{B-k}$ denote i.i.d. messages, each of size NR bits. Each message $W(b-k)$ becomes available to the transmitter at the beginning of block $b-k$, and needs to be securely communicated confidentially from the eavesdropper, and decoded as $\hat{W}(b-k)$ at the legitimate receiver at the end of block b. The error event at block b

$$E(b) \triangleq \big\{\hat{W}(b-k) \neq W(b-k)\big\} \cup \big\{\frac{\|\mathbf{X}(b)\|^2}{N} > P(b) + \delta\big\} \tag{2}$$

occurs either when the decoder cannot decode the message $W(b-k)$, or when the power expended is greater than $P(b)$.

We consider weak secrecy, as defined by Wyner [2], in which the equivocation rate of the message conditioned on eavesdropper's observations has to be arbitrarily close to message rate. Although the messages $\{W(b)\}_{b=1}^B$ are mutually independent, they may be dependent conditioned on eavesdroppers' received signal $\mathbf{Z}^B$, therefore equivocation expression for a given message includes conditioning on all other messages. We say that equivocation outage occurs at block b if the equivocation rate of the message $W(b-k)$ conditioned on complete received signal by the eavesdropper, available eavesdropper CSI, and messages to be communicated in all blocks except $W(b-k)$ is below $R-\delta$

$$\mathcal{O}_{\text{eq}}(b) = \left\{\frac{1}{N}H\big(W(b-k)|\mathbf{Z}^B, W^B\backslash W(b-k), \mathbf{h}^B\big) < R-\delta\right\} \tag{3}$$

Let us define information outage at block b as the event where communicated information about $W(b-k)$ by the end of block b remains below its entropy

$$\mathcal{O}_{\text{inf}}(b) = \left\{\frac{1}{N}I\left(W(b-k);\mathbf{Y}^b\right) < R-\delta\right\}. \tag{4}$$

Then, secrecy outage at block b is defined as,

$$\mathcal{O}_{\text{sec}}(b) = \mathcal{O}_{\text{eq}}(b) \cup \mathcal{O}_{\text{inf}}(b) \tag{5}$$

Let $\bar{\mathcal{O}}_x(\cdot)$ denote the complement of an event $\mathcal{O}_x(\cdot)$.

Definition 1: Rate R is an ϵ-achievable secrecy rate with $k+1$ block delay if for any fixed $\delta > 0$, there exist $N > 0$, $B' > 0$ such that for any $B > B'$, the conditions

$$\mathbb{P}(E(b)|\bar{\mathcal{O}}_{\text{sec}}(b)) < \delta \tag{6}$$
$$\mathbb{P}(\mathcal{O}_{\text{sec}}(b)) < \epsilon + \delta \tag{7}$$

are satisfied for all b, where $B' < b \le B$.
The ϵ-achievable secrecy capacity under $k+1$ block delay is equal to the supremum of such rates R, and is denoted as $C_F(\epsilon, k+1)$ for full CSI and $C_M(\epsilon, k+1)$ for main CSI. Note that the equivocation expressions are based on the realization $\mathbf{h}^B$ of all the channel gains, and the probability expressions are over $\mathbf{H}(b)$. Also note that the security constraints are not imposed on the first B' blocks, which could be referred to as an initialization phase to generate common randomness between the legitimate nodes. Note that this phase only needs to appear *once* in the communication lifetime of that link [12].

III. Capacity Bounds

Define[3]

$$R_m(b) \triangleq \log(1 + P(b)H_m(b)) \tag{8}$$
$$R_s(b) \triangleq [\log(1 + P(b)H_m(b)) - \log(1 + P(b)H_e(b))]^+ \tag{9}$$

where $R_m(b)$ is the supremum of achievable main channel rates at block b without any secrecy constraint [10], and $R_s(b)$ is the non-negative difference between main and eavesdropper

[1] Note that in [12], two dimensional slots are used to describe the discrete time. It can be shown that the two models are equivalent.

[2] At the beginning of block b, $\mathbf{H}(b)$ becomes available at the transmitter, yet $\mathbf{H}(b+1)$ is not available.

[3] $[\cdot]^+ = \max(\cdot, 0)$.

channel's supremum achievable rates. Since $R_s(b)$ depends on b through $P(b)$ and $\mathbf{H}(b)$, we will interchangeably use the notation $R_s(b) \equiv R_s(\mathbf{H}(b), P(b))$ and for simplicity, drop the index b such that $R_s(\mathbf{H}(b), P(b)) \equiv R_s(\mathbf{H}, P)$. We will use similar notation for other signals as well.

A. Lower Bound

We develop a scheme, and show that it achieves the lower bound presented in Theorem 1 provided at the end of this part. Our scheme, depicted in Figure 1, utilizes $k+1$ data queues, named $(Q_1, \ldots, Q_{k+1})$ at the transmitter and the receiver, where Q_i, $i \in \{1, \ldots k+1\}$ holds the message whose deadline is i blocks away. Bits pulled from data queues are secured with the keys pulled from the secret key queue Q_{key}, through Vernam's one-time pad, and sent to the encoder for transmission. Every B' blocks, key bits are generated from previous transmissions through privacy amplification.

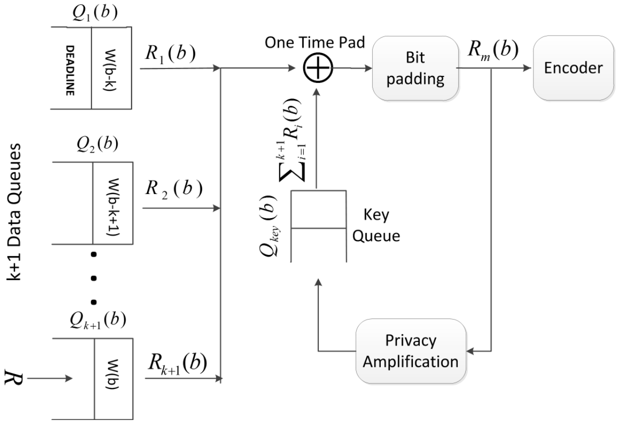

Fig. 1. The achievable scheme: transmitter

Information Transmission: Consider transmission at rate R. At each block b, message $W(b)$ of size R bits[4] becomes available at the transmitter's data queue Q_{k+1} for transmission, and message $W(b-k)$ at queue Q_1 needs to be communicated by that block. At block b, $R_i(b)$ bits are pulled from data queue Q_i for secure transmission. Therefore, the data queue dynamics satisfy

$$Q_i(b+1) = [Q_{i+1}(b) - R_i(b)]^+, \ \forall i < k+1 \tag{10}$$
$$Q_{k+1}(b+1) = [R - R_{k+1}(b)]^+ \tag{11}$$

for any b. Therefore, $\sum_{i=1}^{k+1} R_i(b)$ bits are pulled from the data queues at block b. These message bits are secured using Vernam's one time pad; by xor'ing with the key bits pulled from the secret key queues of the legitimate nodes. The amount of key bits required is equal to the number of message bits [1], therefore

$$Q_{\text{key}}(b+1) = \big(Q_{\text{key}}(b) - \sum_{i=1}^{k+1} R_i(b)\big)^+, \ b \neq mB', \ m \in \mathbb{N}$$

where $Q_{\text{key}}(b)$ as the amount of key bits stored at block b. The secured message bits (after one-time pad) is of size $\sum_{i=1}^{k+1} R_i(b)$ bits. From random coding arguments, it can be shown that at most $R_m(b)$ bits can be transmitted reliably at block b [10]. We pad randomly and uniformly generated bits of size $R_m(b) - \sum_{i=1}^{k+1} R_i(b) - \delta$, and transmit the bit stream of size $R_m(b) - \delta$ bits over the wireless channel after random encoding.

Privacy Amplification: At blocks $b = mB'$, $m \in \mathbb{N}$, secret key bits are generated from signals transmitted in the previous B' blocks through privacy amplification. It can be shown that, both under full CSI and main CSI, $\sum_{b=(m-1)B'+1}^{mB'} R_s(b)$ secure key bits can be generated at the end of block mB' [9], [12], for large enough B'. Therefore,

$$Q_{\text{key}}(mB'+1) = \left(Q_{\text{key}}(mB') + \sum_{b=(m-1)B'+1}^{mB'} R_s(b) - \sum_{i=1}^{k+1} R_i(mB')\right)^+$$

Secrecy Outage Analysis : Let us define $\mathbf{Q}(b) = [Q_1(b) \ldots Q_{k+1}(b)]$. We will consider the set

$$\mathcal{V}_F(R) = \left\{ \left[\{R_i(\mathbf{Q}, \mathbf{H})\}_{i=1}^{k+1}, P(\mathbf{Q}, \mathbf{H}) \right] \right\}$$

of rate and power allocation functions that depend on the instantaneous queue states $\mathbf{Q}$ and channel gains $\mathbf{H}$, and satisfy the conditions (10), (11), and

$$\lim_{b \to \infty} Q_i(b) \overset{d}{=} Q_i, \ w.p. \ 1, \ \forall i \tag{12}$$
$$\mathbb{P}(Q_1 > 0) = \epsilon \tag{13}$$
$$\sum_{i=1}^{k+1} R_i(\mathbf{Q}, \mathbf{H}) \leq R_m(\mathbf{H}, P), \ w.p. \ 1 \tag{14}$$
$$\mathbb{E}[P(\mathbf{Q}, \mathbf{H})] \leq P_{\text{avg}} \tag{15}$$

where $\overset{d}{=}$ denotes equality in distribution. Here, (12) implies that the queue processes $\mathbf{Q}(b)$ converge almost surely to a random vector $\mathbf{Q}$, (14) is required for reliable communication, and (15) is due to the average power constraint. Also, it is easy to see from Figure 1 that information outage is closely tied to Q_1, since when $W(b-k)$ cannot be communicated by the end of block b, $\mathcal{O}_{\text{inf}}(b) = \{Q_1(b+1) > 0\}$, and $Q_1(b+1)$ bits are discarded at block $b+1$. Therefore, we also impose (13).

Now, we show that rate $R < \mathbb{E}[R_s(\mathbf{H}, P) + Q_1]$ satisfies the secrecy outage constraint in (7). If at any block b, $Q_{\text{key}}(b) - \sum_{i=1}^{k+1} R_i(b) < 0$, then there are not enough keys to secure the messages at blocks $(b-k, \ldots, b)$, hence key outage occurs at these blocks, which leads to equivocation outages. Let us denote this event as $\mathcal{O}_{\text{key}}(b)$. Roughly speaking, $\mathbb{E}[\sum_{i=1}^{k+1} R_i(\mathbf{Q}, \mathbf{H})]$ message bits are communicated on average. Also, $\mathbb{E}[R - Q_1]$ bits are pulled from data queue, since on average $\mathbb{E}[Q_1]$ bits are discarded due to information outages. For $\mathbb{E}[R - Q_1] \leq \mathbb{E}[R_s(\mathbf{H}, P)]$, the key queue process $Q_{\text{key}}(b)$ has a positive expected drift, therefore

[4] Assuming perfect compression, each message is of NR bits. To simplify queue analysis, we scale all queues by $1/N$.

$\lim_{b\to\infty}\mathbb{P}(\mathcal{O}_{\text{key}}(b)) = 0$. Therefore, for a given $\delta > 0$, we find B' large enough such that for any $b > B'$,

$$\mathbb{P}(\mathcal{O}_{\text{sec}}(b)) \leq \sum_{i=b-k}^{b} \mathbb{P}(\mathcal{O}_{\text{key}}(i)) + \mathbb{P}(\mathcal{O}_{\text{inf}}(b)) \tag{16}$$

$$\leq \delta + \mathbb{P}(Q_1 > 0) = \delta + \epsilon \tag{17}$$

where (16) follows due to union bound, and the fact that having no key outages in all the blocks $b-k,\dots,b$ is sufficient to avoid secrecy outage, and (17) follows due to (13), which leads to the following result.

Theorem 1: For full CSI,

$$C_F(\epsilon,k+1) \geq L_F(\epsilon,k+1) \triangleq \max_{[\{R_i(\mathbf{Q},\mathbf{H})\}_{i=1}^{k+1},P(\mathbf{Q},\mathbf{H})]\in\mathcal{V}_F(L_F(\epsilon,k+1))} \mathbb{E}[R_s(\mathbf{H},P)+Q_1] \tag{18}$$

Similarly, for main CSI

$$C_M(\epsilon,k+1) \geq L_M(\epsilon,k+1) \triangleq \max_{[\{R_i(\mathbf{Q},H_m)\}_{i=1}^{k+1},P(\mathbf{Q},H_m)]\in\mathcal{V}_M(L_M(\epsilon,k+1))} \mathbb{E}[R_s(\mathbf{H},P)+Q_1] \tag{19}$$

where $\mathcal{V}_M$ is in the same form as $\mathcal{V}_F$, except $\mathbf{H}$ is replaced by H_m due to lack of eavesdropper CSI at the transmitter.

B. Upper Bound

We consider the following upper bounds

$$C_F(\epsilon,k+1) \leq C_F(\epsilon,\infty),\; C_M(\epsilon,k+1) \leq C_M(\epsilon,\infty)$$

which hold since $C_F(\epsilon,k+1)$ and $C_M(\epsilon,k+1)$ are monotone increasing with respect to k. In Section IV-A, we provide $C_F(\epsilon,\infty)$ and $C_M(\epsilon,\infty)$. Further note that for any k,

$$\lim_{P_{\text{avg}}\to\infty} C_F(\epsilon,k+1) = \lim_{P_{\text{avg}}\to\infty} C_M(\epsilon,k+1) \tag{20}$$

$$= \frac{1}{1-\epsilon}\mathbb{E}\left[\log\left(\frac{H_m}{H_e}\right)^+\right] \tag{21}$$

hence the capacity gap diminishes under high SNR [4].

IV. Special Cases

A. Ergodic Secrecy Capacity with ϵ Outage, $k=\infty$

Corollary 1:

$$C_F(\epsilon,\infty) = \max_{P(\mathbf{H})} \frac{\mathbb{E}[R_s(\mathbf{H},P)]}{1-\epsilon} \tag{22}$$

$$\text{subject to: } \mathbb{E}[P(\mathbf{H})] \leq P_{\text{avg}} \tag{23}$$

Similarly, for Main CSI $C_M(\epsilon,\infty)$ is in the form (22)-(23), where $\mathbf{H}$ is replaced by H_m.

Corollary 1 is also proven in [4]. Here, we briefly explain how[5] the scheme in Theorem 1 can be modified to achieve $C_F(\epsilon,\infty)$. Consider transmission at rate $R < C_F(\epsilon,\infty)$. Instead of $k+1$ data queues $Q_1,\dots,Q_{k+1}$, we have single FIFO data queue Q_1, where arriving message is pushed to the data queue with probability $1-\epsilon$ for transmission. Let $\{U(b)\}_{b=1}^{B}$ be i.i.d. random variables, where $U(b)$~Bern$(1-\epsilon)$. If $U(b) = 0$, then $W(b)$ is pushed to the data queue for transmission. Otherwise, $W(b)$ is discarded. Then, the data queue dynamics are governed by

$$Q_1(b+1) = \min\left[\sum_{i=b-k}^{b} RU(i), Q_1(b) + RU(b) - R_m(b)\right]^+$$

Information outage at block b

$$\mathcal{O}_{\text{inf}}(b) = \left\{Q_1(b) > \sum_{i=b-k}^{b} R\mathbf{1}(U(i)=1)\right\} \cup \{U(b-k)=0\}$$

occurs either if $W(b-k)$ is not admitted to data queue, i.e., $U(b-k) = 0$, or if the deadline is not met despite the fact that $W(b-k)$ is in the data queue. It can be shown that queue overflow probability decays to 0 with increasing k since the data queue process has negative expected drift. Therefore, the power/rate allocation functions are not constrained by $Q_1(b)$, and $\mathbb{P}(\mathcal{O}_{\text{inf}}(b)) < \epsilon + \delta$ for $b > B'$, and large enough B'. The rest of the proof is similar to the proof of Theorem 1.

B. $k+1$ Block Delay, $\epsilon = 0$

Corollary 2: For full CSI,

$$C_F(0,k+1) = \max_{P(Q_1,\mathbf{H})\in\mathcal{V}'_F} \mathbb{E}[R_s(\mathbf{H},P)] \tag{24}$$

where $\mathcal{V}'_F$ is the set of $P(Q_1,\mathbf{H})$ such that the queue process

$$Q_1(b+1) = \left[Q_{i+1}(b) + C_F(0,k+1) - R_m(b)\right]^+$$

satisfies the conditions

$$\lim_{b\to\infty} Q_1(b) \overset{d}{=} Q_1,\; Q_1 \leq kC_F(0,k+1),\; w.p\ 1 \tag{25}$$

$$\mathbb{E}[P(Q_1,\mathbf{H})] \leq P_{\text{avg}} \tag{26}$$

For main CSI,

$$C_M(0,k+1) = \max_{P(Q_1,H_m)\in\mathcal{V}'_M} \mathbb{E}[R_s(\mathbf{H},P)]$$

and $\mathcal{V}'_M$ is of the form of $\mathcal{V}'_F$, where $\mathbf{H}$ is replaced by H_m. The proof is omitted. Achievability follows from concatenating $k+1$ data queues in the proof of Theorem 1 to form a single FIFO data queue Q_1. Note that, (25) is due to the fact that in a FIFO queue, message $W(b-k)$ cannot be communicated by block b if $Q_1(b) > kC_{Fs}(0,k+1)$.

C. Secrecy Outage Capacity with Strict Delay, $k = 0$

Corollary 3: (Theorem 1, [12]) For Full CSI,

$$C_F(\epsilon,1) = \max_{P(\mathbf{H})\in\mathcal{V}'_F} \frac{\mathbb{E}[R_s(\mathbf{H},P)]}{1-\epsilon} \tag{27}$$

$$\mathcal{V}'_F = \left\{P(\mathbf{H}) :\ \mathbb{P}\left(R_m < \frac{\mathbb{E}[R_s]}{1-\epsilon}\right) \leq \epsilon \right. \tag{28}$$

$$\left. \mathbb{E}[P(\mathbf{H})] \leq P_{\text{avg}} \right\} \tag{29}$$

Similarly for Main CSI, $\mathbf{H}$ is replaced by H_m.

[5] Note that $C_F(\epsilon,\infty)$ can also be achieved without the use of key queues.

Note that, an achievable scheme is a special case of Theorem 1, where we do not need a data queue. When message $W(b)$ arrives at the transmitter at the beginning of block b, it is either transmitted entirely at that block, or the message is skipped, and information outage occurs.

Power allocation function that solves $C_F(\epsilon, 1)$ is a time-sharing of channel inversion power policy

$$P_{\text{inv}}(\mathbf{H}, R) = \frac{2^R - 1}{H_m} \tag{30}$$

which delivers *minimum* required power to maintain main channel rate of R, and secure waterfilling

$$P_{\text{wf}}(\mathbf{H}, \lambda) = \frac{1}{2}\Bigg[\sqrt{\left(\frac{1}{H_e} - \frac{1}{H_m}\right)^2 + \frac{4}{\lambda}\left(\frac{1}{H_e} - \frac{1}{H_m}\right)} - \left(\frac{1}{H_e} + \frac{1}{H_m}\right)\Bigg]^+, \tag{31}$$

that maximizes ergodic secrecy rate, where $\lambda > 0$ is a constant that depends on the average power constraint.

V. Numerical Evaluations

In this section, we numerically evaluate the capacity bounds using Monte Carlo simulations. Note that, it may not be feasible to evaluate (18)-(15) since optimization is jointly over $k+1$ rate allocation and one power allocation function. Instead, we focus on a worse lower bound that is easier to evaluate: Inspired by the 0-outage case, we consider a single FIFO data queue Q_1, and inspired by optimal power allocation function of strict delay ($k = 0$), we use the following power allocation

$$\begin{aligned} P^*(\mathbf{H}, Q_1) =& P_{\text{wf}}(\mathbf{H}, \lambda^*) + \mathbf{1}\left(\mathbf{H} \in \mathcal{G}(\lambda^*, c^*)\right) \\ & \Big(P_{\text{inv}}\left(\mathbf{H}, [Q_1 - L'_F(\epsilon, k+1)]^+\right) - P_{\text{wf}}(\mathbf{H}, \lambda^*)\Big)^+ \end{aligned} \tag{32}$$

$$\text{subject to: } c^* \leq 0,\ \ \lambda^* > 0$$

$$L'_F(\epsilon, k+1) = \mathbb{E}[R_s(\mathbf{H}, P^*) + Q_1] \tag{33}$$

$$\begin{aligned} Q_1(b+1) = \min\big(&kL'_F(\epsilon, k+1), \\ &[Q_1(b) + L'_F(\epsilon, k+1) - R_m(b)]^+\big) \end{aligned}$$

$$\mathbb{P}\big(R_m(\mathbf{H}, P^*) < Q_1 - (k-1)L'_F(\epsilon, k+1)\big) = \epsilon \tag{34}$$

$$\mathbb{E}[P^*(\mathbf{H}, Q_1)] = P_{\text{avg}} \tag{35}$$

for full CSI, where the time sharing region is defined as

$$\mathcal{G}(\lambda, c) = \Big\{\mathbf{h} : [R_s(\mathbf{h}, P_{\text{inv}}) - R_s(\mathbf{h}, P_{\text{wf}})]^+ - \lambda\left[P_{\text{inv}}(\mathbf{h}, R) - P_{\text{wf}}(\mathbf{h}, \lambda)\right]^+ \geq c\Big\} \tag{36}$$

Here, $L'_F(\epsilon, k+1)$ is achievable. The proof, and the power allocation used for main CSI to achieve $L'_M(\epsilon, k+1)$ are omitted due to space constraints. We assume that H_m and H_e follow chi square distribution of degree 1, and means 2 and 1, respectively. In Figure 2, for $\epsilon = 0.05$, we plot $L'_F(\epsilon, k+1)$ for $k = \{1, 2\}$, $C_F(\epsilon, 1)$ and $C_F(\epsilon, \infty)$, along with the main CSI equivalents. We can clearly see the impact of delay over secrecy capacity under low SNR, whereas under high SNR, they all converge to the same value.

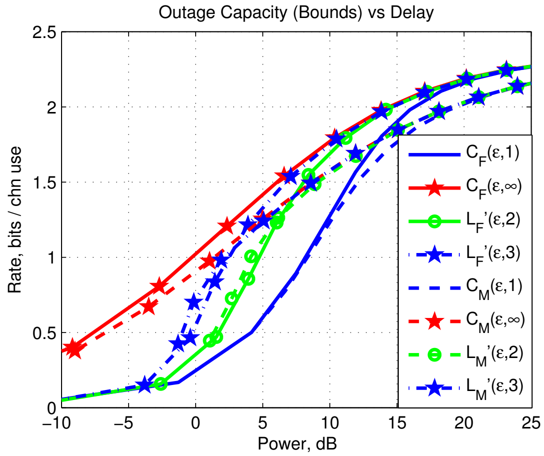

Fig. 2. Capacity bounds for different delay parameters, $\epsilon = 0.05$

VI. Conclusion and Future Work

We characterized ϵ-achievable secrecy capacity with $k+1$ block delay under Full CSI and Main CSI. We showed that the bounds simplify for special cases such as no delay constraint, and 0-outage constraint. We have provided an approach to numerically evaluate an upper bound on the gap between ergodic secrecy capacity, and secrecy capacity with $k+1$ delay, for any k. We illustrated that the gap is significant for low SNR. Our current investigations are focused on 1) Finding analytical bounds for secrecy capacity gap, and 2) Complete characterization of the outage secrecy capacity with ϵ outage, $k+1$ block delay under correlated message sets.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *The Bell System Technical Journal*, vol. 28, pp. 656-715, October 1949.

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

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Transactions on Information Theory* , vol.24, no.4, pp. 451-456, Jul 1978.

[4] 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.

[5] Y. Abdallah, M. A. Latif, M. Youssef, A. Sultan and H. El-Gamal, "Keys through ARQ: Theory and Practice," *arXiv:1005.5063v2 [cs.IT]*, May 2010.

[6] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory*, vol.54, pp. 2515-2534, 2008.

[7] A. Khisti, A. Tchamkerten and G.W. Wornell ,"Secure Broadcasting Over Fading Channels," *IEEE Transactions on Information Theory*, vol.54, no.6, pp. 2453-2469, June 2008.

[8] Y. Liang, H.V. Poor and S. Shamai, "Secure Communication Over Fading Channels," *IEEE Transactions on Information Theory*, vol.54, no.6, pp. 2470-2492, June 2008.

[9] C.H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer, "Generalized Privacy Amplification," *IEEE Transactions on Information Theory* , vol.41, no.6, pp. 1915-1923, Nov 1995.

[10] T. Cover and J. Thomas, "Elements of Information Theory,". *John Wiley & Sons*, 1991.

[11] K. Khalil, M. Youssef, O. O. Koyluoglu, and H. El-Gamal, "Opportunistic Secrecy with a Strict Delay Constraint," *arXiv:0907.3341v1 [cs.IT]*, Jul 2009.

[12] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal and N. B. Shroff, "Secrecy Outage Capacity of Fading Channels", http://arxiv.org/abs/1112.2791v1.