Secrecy Outage Capacity of Fading Channels

Onur Gungor, Jian Tan, Can Emre Koksal, Hesham El-Gamal, Ness B. Shroff
Department of Electrical and Computer Engineering
The Ohio State University, Columbus, 43210

***Abstract*—This paper considers point to point secure communication over flat fading channels under an outage constraint. More specifically, we extend the definition of outage capacity to account for the secrecy constraint and obtain sharp characterizations of the corresponding fundamental limits under two different assumptions on the transmitter CSI (Channel state information). First, we find the outage secrecy capacity assuming that the transmitter has perfect knowledge of the legitimate and eavesdropper channel gains. In this scenario, the capacity achieving scheme relies on opportunistically exchanging private keys between the legitimate nodes. These keys are stored in a key buffer and later used to secure delay sensitive data using the Vernam's one time pad technique. We then extend our results to the more practical scenario where the transmitter is assumed to know only the legitimate channel gain. Here, our achievability arguments rely on privacy amplification techniques to generate secret key bits. In the two cases, we also characterize the optimal power control policies which, interestingly, turn out to be a judicious combination of channel inversion and the optimal ergodic strategy. Finally, we analyze the effect of key buffer overflow on the overall outage probability.**

I. Introduction

Secure communication is a topic that is becoming increasingly important thanks to the proliferation of wireless devices. Over the years, several secrecy protocols have been developed and incorporated in several wireless standards; e.g., the IEEE 802.11 specifications for Wi-Fi. However, as new schemes are being developed, methods to counter the specific techniques also appear. Breaking this cycle is critically dependent on the design of protocols that offer provable secrecy guarantees. The information theoretic secrecy paradigm adopted here, allows for a systematic approach for the design of low complexity and provable secrecy protocols that fully exploit the intrinsic properties of the wireless medium.

Most of the recent work on information theoretic secrecy is, arguably, inspired by Wyner's wiretap channel [2]. In this setup, a passive eavesdropper listens to the communication between two legitimate nodes over a separate communication channel. While attempting to decipher the message, no limit is imposed on the computational resources available to the eavesdropper. This assumption led to defining **perfect 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], the perfect 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 [4], [5], [7]. The basic idea is to opportunistically exploit the instants when the main channel observes a higher gain than the eavesdropper channel to exchange secure messages. This opportunistic secrecy approach was shown to achieve non-zero **ergodic secrecy capacity** even when **on average** the eavesdropper channel has favorable conditions over the legitimate channel. Remarkably, this result still holds even when the instantaneous channel state information of the eavesdropper channel is not available at the legitimate nodes.

The ergodic result in [4] applies only to delay tolerant traffic, e.g., file downloads. Early attempts at characterizing the delay limited secrecy capacity drew the negative conclusion that non-zero delay limited secrecy rates are not achievable, over almost all channel distributions, 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 [12] that, interestingly, 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. A following work studied the key queue dynamics and power control strategies for this system [13]. However, these works stopped short of proving sharp capacity results or deriving the corresponding optimal power control policies. To that end, in this paper we study the secrecy outage capacity characterization of the block fading wiretap channel. We first consider the scenario where perfect knowledge about the main and eavesdropper channels are available *a-priori* at the transmitter. The outage secrecy capacity and corresponding optimal power control policy are obtained and then the results are generalized to the more practical scenario where only the instantaneous main channel state information (CSI) is available at the transmitter. Finally, the impact of the *private key queue* overflow on secrecy outage probability is studied. Overall, our results reveal interesting structural insights on the optimal encoding and power control schemes as well as sharp characterizations of the fundamental limits on secure communication of delay sensitive traffic over fading channels. Note that, we provide some intuition and very brief sketches

of the proofs of our theorems. Full proofs can be found in [14].

II. System Model

We study a point-to-point wireless communication link, in which a transmitter is trying to send information to a legitimate receiver, under the presence of a passive eavesdropper. We divide time into discrete slots, where blocks are formed by N channel uses, and B blocks combine to form a super-block. Let the communication period consist of S super-blocks. We use the notation (s,b) to denote the b^{th} block in the s^{th} super-block. 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. Within each block (s,b), the observed signals at the receiver and at the eavesdropper are:

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

respectively, where $\mathbf{X}(s,b) \in \mathbb{C}^N$ is the transmitted signal, $\mathbf{Y}(s,b) \in \mathbb{C}^N$ is the received signal by the legitimate receiver, and $\mathbf{Z}(s,b) \in \mathbb{C}^N$ is the received signal by the eavesdropper. $\mathbf{W}_m(s,b)$ and $\mathbf{W}_e(s,b)$ are independent noise vectors, whose elements are drawn from standard complex normal distribution. We assume that the channel gains of the main channel $G_m(s,b)$ and the eavesdropper channel $G_e(s,b)$ are i.i.d. complex random variables. The power gains of the fading channels are denoted by $H_m(s,b) = |G_m(s,b)|^2$ and $H_e(s,b) = |G_e(s,b)|^2$. We sometimes use the vector notation $\mathbf{H}(\cdot) = [H_m(\cdot)\ H_e(\cdot)]$ for simplicity, and also use the notation $\mathbf{H}^{s,b} = \{\mathbf{H}\}_{s'=1,b'=1}^{s,b}$ to denote the set of channel gains $\mathbf{H}(s',b')$ observed until block (s,b). We use similar notation for other signals 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 define channel state information (CSI) as one's knowledge of the instantaneous channel gains. We define *full transmitter CSI* as the case in which the transmitter has full causal knowledge of the main and eavesdropper channel gains. We define *main transmitter CSI* as the case in which that the transmitter only knows the CSI of the legitimate receiver. In both cases, the eavesdropper has complete knowledge of both the main and the eavesdropper channels. Let $P(s,b)$ denote the power allocated at block (s,b). We consider a long term power constraint (or average power constraint) such that,

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

for some $P_{\text{avg}} > 0$.

Let $\{W(s,b)\}_{s=1,b=1}^{S,B}$ denote the set of messages to be transmitted with a delay constraint. $W(s,b)$ becomes available at the transmitter at the beginning of block (s,b), and needs to be securely communicated to the legitimate receiver at the end of that particular block. We consider the problem of constructing $(2^{NR}, N)$ codes to communicate message packets $W(s,b) \in \{1,\cdots,2^{NR}\}$ of equal size, which consists of:

1) A stochastic encoder that maps $(w(s,b),\ \mathbf{x}^{s,b-1})$ to $\mathbf{x}(s,b)$ based on the available CSI, where $\mathbf{x}^{s,b-1}$ summarizes the previously transmitted signals[1], and
2) A decoding function that maps $\mathbf{y}^{s,b}$ to $\hat{w}(s,b)$ at the legitimate receiver.

Note that we consider the current block $\mathbf{x}(s,b)$ to be a function of the past blocks $\mathbf{x}^{s,b-1}$ as well. This kind of generality allows us to store shared randomness to be exploited in the future to increase the achievable secrecy rate.

Define the error event with parameter δ at block (s,b) as

$$E(s,b,\delta) = \left\{\hat{W}(s,b) \neq W(s,b)\right\} \cup \left\{\frac{1}{N}\|\mathbf{X}(s,b)\|^2 > P(s,b) + \delta\right\},$$

which occurs either when the decoder makes an error, or when the power expended is greater than $P(s,b)+\delta$. The equivocation rate at the eavesdropper is defined as the entropy rate of the message at block (s,b), conditioned on the received signal by the eavesdropper during the transmission period, and available eavesdropper CSI, which is equal to $\frac{1}{N}H(W(s,b)|\mathbf{Z}^{SB},\mathbf{h}^{SB})$. The secrecy outage event at rate R with parameter δ at block (s,b) is defined as

$$\mathcal{O}_{\text{sec}}(s,b,R,\delta) = \mathcal{O}_{\text{eq}}(s,b,R,\delta) \cup \mathcal{O}_{\text{ch}}(s,b,R) \tag{2}$$

where the equivocation outage

$$\mathcal{O}_{\text{eq}}(s,b,R,\delta) = \left\{\frac{1}{N}H(W(s,b)|\mathbf{Z}^{SB},\mathbf{h}^{SB}) < R-\delta\right\}$$

occurs if the equivocation rate at block (s,b) is less than $R-\delta$, and channel outage

$$\mathcal{O}_{\text{ch}}(s,b,R) = \left\{\frac{1}{N}I\left(\mathbf{X}(s,b);\mathbf{Y}(s,b)\right) < R\right\}$$

occurs if channel at block (s,b) is unsuitable for reliable transmission at rate R. Defining $\bar{\mathcal{O}}_{\text{sec}}(\cdot)$ as the complement of the event $\mathcal{O}_{\text{sec}}(\cdot)$, we now characterize the notion of ϵ-achievable secrecy capacity.

Definition 1: Rate R is achievable with at most ϵ probability of secrecy outage if, for any fixed $\delta > 0$, there exist S, B and N large enough such that the conditions

$$\mathbb{P}(E(s,b,\delta)|\bar{\mathcal{O}}_{\text{sec}}(s,b,R,\delta)) < \delta \tag{3}$$
$$\mathbb{P}(\mathcal{O}_{\text{sec}}(s,b,R,\delta)) < \epsilon + \delta \tag{4}$$

are satisfied for all (s,b), $s \neq 1$.

We call such R an ϵ-achievable secrecy rate. Note that the security constraints are not imposed on the first super-block.

Definition 2: The ϵ-achievable secrecy capacity is the supremum of ϵ-achievable secrecy rates R.

Remark 1: The notion of secrecy outage was previous defined and used in [6], [8]. However, those works did not

[1]An exception is for $b = 1$, in which case the previous signals are summarized by $\mathbf{x}^{s-1,B}$.

consider the technique of storing shared randomness for future use, and in that case, secrecy outage depends only on the instantaneous channel states. In our case, secrecy outage depends on previous channel states as well. Note that we do not impose a secrecy outage constraint on the first superblock ($s = 1$). We refer to the first superblock as an initialization phase used to generate initial common randomness between the legitimate nodes. Note that this phase only needs to appear *once* in the communication lifetime of that link. In other words, when a session (which consists of S superblocks) between the associated nodes is over, they will not need to go through the initialization step again before the subsequent sessions.

III. Capacity Results

In this section, we investigate this capacity under two different cases; full CSI and main CSI at the transmitter. Before giving the capacity results, we define the following quantities. For a given power allocation function $P(s,b)$, let $R_m(s,b)$ and $R_s(s,b)$ be as follows,

$$R_m(s,b) \triangleq \log(1 + P(s,b)H_m(s,b)) \tag{5}$$

$$R_s(s,b) \triangleq [\log(1 + P(s,b)H_m(s,b)) - \log(1 + P(s,b)H_e(s,b))]^+, \tag{6}$$

where $[\cdot]^+ = \max(\cdot, 0)$. Note that, $R_m(\cdot)$ is the supremum of achievable main channel rates, without the secrecy constraint. Also, $R_s(\cdot)$ is the non-negative difference between main channel and eavesdropper channel's supremum achievable rates. We define memoryless power allocation strategy as a mapping from the available instantaneous CSI to $\mathbb{R}^+$. We consider [2] the set of memoryless power allocation strategies $\mathcal{P}$. For **full CSI**, a memoryless power allocation policy is a function of $\mathbf{h}(s,b) = [h_m(s,b)\ h_e(s,b)]$. For simplicity, we drop the block index (s,b), and use the notation $P(\mathbf{h})$ for a memoryless power allocation policy. Similarly, with **main CSI** memoryless power allocation policies are functions of $h_m(s,b)$ only, and we use the notation $P(h_m)$ for the stationary power allocation policy. In both cases, since the secrecy rate $R_s(s,b)$, and the main channel rate $R_m(s,b)$ are completely determined by the power allocation functions $P(\cdot)$ and channel gains $\mathbf{h}$, we will interchangeably use the notations $R_s(s,b) \equiv R_s(\mathbf{h}, P)$ and $R_m(s,b) \equiv R_m(\mathbf{h}, P)$.

A. Full CSI

Theorem 1: Let the transmitter have full CSI. Then, for any ϵ, $0 \leq \epsilon < 1$, the ϵ-achievable secrecy capacity is identical to

$$C_F^\epsilon = \max_{P(\mathbf{h}) \in \mathcal{P}'} \frac{\mathbb{E}[R_s(\mathbf{H}, P)]}{1 - \epsilon}, \tag{7}$$

where the set $\mathcal{P}' \subseteq \mathcal{P}$ consists of power control policies $P(\mathbf{h})$ that satisfies the following conditions.

$$\mathbb{P}\left(R_m(\mathbf{H}, P) < \frac{\mathbb{E}[R_s(\mathbf{H}, P)]}{1 - \epsilon} \right) \leq \epsilon \tag{8}$$

$$\mathbb{E}[P(\mathbf{H})] \leq P_{\text{avg}}. \tag{9}$$

Here, we give a brief intuition on the result. For a given $P(\mathbf{h})$, $R_s(\mathbf{h}, P)$ the supremum of the secret key generation rates within a block that experiences channel gains $\mathbf{h}$ [3]. This implies that the expected achievable secrecy rate [4] is $\mathbb{E}[R_s(\mathbf{H}, P)]$ without the outage constraint. With the outage constraint, the fluctuations of $R_s(\mathbf{H}, P)$ due to fading are unacceptable, since $R_s(\mathbf{H}, P)$ can go below the desired rate when the channel conditions are unfavorable (e.g., when $H_m < H_e$, $R_s(\mathbf{H}, P) = 0$). Hence, we utilize the system illustrated in Figure 1 to address this issue. In our system, secret key buffers smoothen out these fluctuations to provide secrecy rate of $\mathbb{E}[R_s(\mathbf{H}, P)]$ at each block. The generated secret key bits are stored in secret key buffers of both the transmitter and receiver, and they are utilized to secure data of same size using Vernam's one-time pad technique. With the allowable amount of secrecy outages, the secrecy rate goes up to $\mathbb{E}[R_s(\mathbf{H}, P)]/(1 - \epsilon)$. Equation (8) on the other hand, ensures that channel outage probability is at most ϵ, hence it is a necessary condition to satisfy the secrecy outage constraint in (4) due to (2).

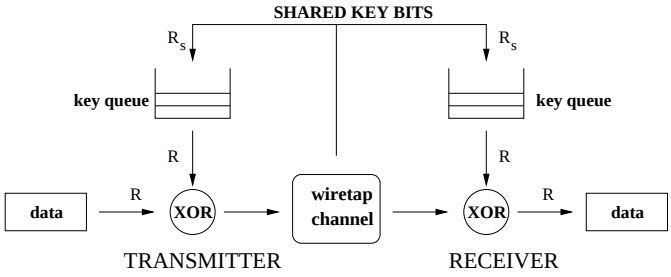

Fig. 1. The private key queues at the transmitter and the receiver.

Example 1: Consider a four state system, where H_m and H_e takes values from the set $\{1, 10\}$ and the joint probabilities are as given in Table I. Let the average power constraint be $P_{\text{avg}} = 0.5$, and there is no power control, i.e., $P(\mathbf{h}) = P_{\text{avg}}$ $\forall \mathbf{h}$. The achievable instantaneous secrecy rate at each state is given in Table II. According to the pessimistic result in [6,8], any non-zero rate cannot be achieved with a secrecy outage probability $\epsilon < 0.6$ in this case. However, according to Theorem 1, for any $\epsilon > 0$, rate $R = \frac{0.8}{1-\epsilon}$ can be achieved with ϵ secrecy outage probability[3], since $\mathbb{E}[R_s(\mathbf{H}, P_{\text{avg}})] = 0.8$. In Figure 2, we study the performance of two strategies with the goal of achieving secrecy rate of $R = 1$. In strategy 1, the available instantaneous secrecy rate is used greedily, hence in block 2, secrecy outage occurs when $R_s = 0$. Strategy 2 is our achievable scheme in Theorem 1. We can see that with this

[2]Note that, it is shown in [14] that a memoryless power allocation strategy achieves the ϵ achievable secrecy capacity.

[3]Although Theorem 1 is stated for the case where random vector $\mathbf{H}$ is continuous, the result similarly applies to discrete $\mathbf{H}$ as well.

strategy, excess secrecy in block 1 are stored in the form of secret key bits, and they are used to secure the data in block 2, hence secrecy outage is avoided.

TABLE I
$\mathbb{P}(\mathbf{h})$

$\downarrow h_m \setminus h_e \rightarrow$	1	10
1	0.1	0.1
10	0.4	0.4

TABLE II
$R_s(\mathbf{h}, P_{\text{AVG}})$

$\downarrow h_m \setminus h_e \rightarrow$	1	10
1	0	0
10	2	0

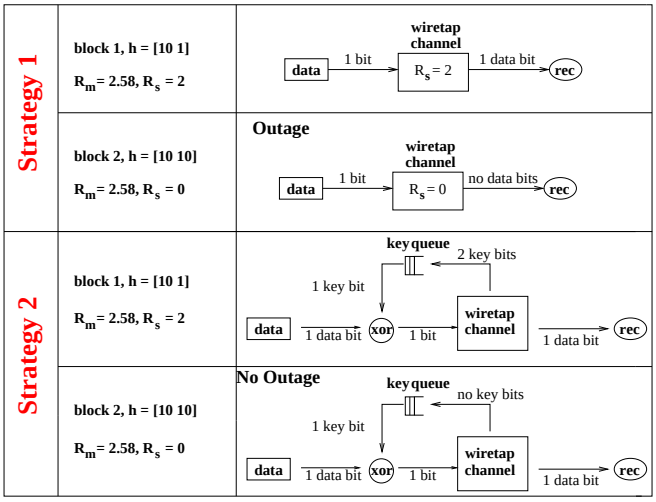

Fig. 2. A sample path. With strategy 2, secrecy outage can be avoided for block $t = 2$ via the use of key bits.

B. Main CSI

Theorem 2: Let the transmitter have main CSI. Then, for any ϵ, $0 \leq \epsilon < 1$, the ϵ-achievable secrecy capacity is identical to

$$C_M^{\epsilon} = \max_{P(h_m) \in \mathcal{P}''} \frac{\mathbb{E}[R_s(\mathbf{H}, P)]}{1-\epsilon}, \tag{10}$$

where the set $\mathcal{P}'' \subseteq \mathcal{P}$ consists of power control policies $P(h_m)$ that satisfies the following conditions.

$$\mathbb{P}\left(R_m(\mathbf{H}, P) < \frac{\mathbb{E}[R_s(\mathbf{H}, P)]}{1-\epsilon}\right) \leq \epsilon \tag{11}$$

$$\mathbb{E}[P(H_m)] \leq P_{\text{avg}}. \tag{12}$$

Although the problems (7)-(9) and (10)-(12) are of the same form, due to the absence of eavesdropper CSI, the maximization in this case is over power allocation functions $\mathcal{P}''$ that depend on the instantaneous main channel state only. Hence, $C_M^{\epsilon} \leq C_F^{\epsilon}$. As in the full CSI case, our achievable scheme uses similar key buffers and Vernam's one time pad technique to secure the message. The main difference is the generation of secret key bits. Due to the lack of knowledge of $H_e(s, b)$ at the transmitter, secret key bits cannot be generated within a block. Instead, using the statistical knowledge of $H_e(s, b)$, we generate keys over a super-block. Roughly, over a superblock the receiver can reliably obtain $NB\mathbb{E}[R_m(\mathbf{H}, P)]$ bits of information, while the eavesdropper can obtain $NB\mathbb{E}[R_m(\mathbf{H}, P) - R_s(\mathbf{H}, P)]$ bits of information. From privacy amplification arguments [9], $NB\mathbb{E}[R_s(\mathbf{H}, P)]$ bits of secret key can be extracted by using a universal hash function.

In [14], we prove that

$$\lim_{P_{\text{avg}} \to \infty} C_F^{\epsilon} = \lim_{P_{\text{avg}} \to \infty} C_M^{\epsilon} = \frac{\mathbb{E}_{H_m > He} \log\left(H_m / H_e\right)}{(1-\epsilon)}. \tag{13}$$

Thus, in the high power regime, the power allocation policy has minimal impact on the achievable key rate. Our simulation results also illustrate this fact. On the other hand, when the average power is limited, the optimality of the power allocation function is of critical importance, which is the focus of the following section.

IV. Optimal Power Allocation Strategy

A. Full CSI

The optimal power control strategy, $P^*(\mathbf{h})$ is the stationary strategy that solves the optimization problem (7)-(9). In this section, we will show that $P^*(\mathbf{h})$ is a time-sharing between the channel inversion power policy, and the secure waterfilling policy. We first introduce the channel inversion power policy, $P_{\text{inv}}(\mathbf{h}, R)$, which is the *minimum* required power to maintain main channel rate of R. For $\mathbf{h} = [h_m \ h_e]$,

$$P_{\text{inv}}(\mathbf{h}, R) \triangleq \frac{2^R - 1}{h_m}. \tag{14}$$

Next we introduce $P_{\text{wf}}(\mathbf{h}, \lambda)$,

$$P_{\text{wf}}(\mathbf{h}, \lambda) \triangleq \frac{1}{2}\Bigg[\sqrt{\left(\frac{1}{h_e} - \frac{1}{h_m}\right)^2 + \frac{4}{\lambda}\left(\frac{1}{h_e} - \frac{1}{h_m}\right)} - \left(\frac{1}{h_e} + \frac{1}{h_m}\right)\Bigg]^+. \tag{15}$$

We call it the 'secure waterfilling' power policy because it maximizes the ergodic secrecy rate without any outage constraint, and resembles the traditional 'waterfilling' power control policy without secrecy. Here, the parameter λ determines the power expended on average. Now, let us define a time-sharing region

$$\mathcal{G}(\lambda, k) \triangleq \Big\{\mathbf{h} : [R_s(\mathbf{h}, P_{\text{inv}}) - R_s(\mathbf{h}, P_{\text{wf}})]^+ - \lambda\left[P_{\text{inv}}(\mathbf{h}, b) - P_{\text{wf}}(\mathbf{h}, \lambda)\right]^+ \geq k\Big\}, \tag{16}$$

which is a function of parameters λ and k.

Theorem 3: $P^*(\mathbf{h})$ is the unique solution to

$$P^*(\mathbf{h}) = P_{\text{wf}}(\mathbf{h}, \lambda^*) + \mathbf{1}\left(\mathbf{h} \in \mathcal{G}(\lambda^*, k^*)\right)\left(P_{\text{inv}}(\mathbf{h}, C_F^{\epsilon}) - P_{\text{wf}}(\mathbf{h}, \lambda^*)\right)^+ \tag{17}$$

subject to: $k^* \leq 0, \lambda^* > 0$

$$C_F^{\epsilon} = \mathbb{E}[R_s(\mathbf{H}, P^*)]/(1-\epsilon) \tag{18}$$

$$\mathbb{P}(\mathbf{H} \in \mathcal{G}(\lambda^*, k^*)) = 1 - \epsilon \tag{19}$$

$$\mathbb{E}[P^*(\mathbf{H})] = P_{\text{avg}}, \tag{20}$$

where $\mathbb{E}[R_s(\mathbf{H}, P^*)]$ is the expected secrecy rate under the power allocation policy $P^*(\mathbf{h})$.
Due to (17), the optimal power allocation function is a time-sharing between the channel allocation power allocation function and secure waterfilling; a balance between avoiding channel outages, hence secrecy outages, and maximizing the expected secrecy rate. The time sharing region $\mathcal{G}(\lambda, k)$ determines the instants $\mathbf{h}$, for which avoiding channel outages are guaranteed through the choice of $P(\mathbf{h}) = \max(P_{\text{inv}}(\mathbf{h}, R), P_{\text{wf}}(\mathbf{h}, \lambda))$. Equation (19) ensures that channel outage probability is at most ϵ, and (20) ensures that average power constraint is met with equality. (18), on the other hand, is an immediate consequence of (7).

Note that, an extreme case is $P^*(\mathbf{h}) = P_{\text{wf}}(\mathbf{h}, \lambda^*)\ \forall \mathbf{h}$, which occurs when $P_{\text{inv}}(\mathbf{h}, R) \leq P_{\text{wf}}(\mathbf{h}, \lambda^*)$ for any $\mathbf{h} \in \mathcal{G}(\lambda^*, k^*)$, which means that the secure waterfilling solution itself satisfies the channel outage probability in (8). However, that the other extreme $P^*(\mathbf{h}) = P_{\text{inv}}(\mathbf{h}, R^*)$, $\forall \mathbf{h}$ cannot occur for any non-zero ϵ due to (17). The parameter C_F^ϵ can be found graphically as shown in Figure 3, by plotting $\mathbb{E}[R_s(\mathbf{H}, P^R)]$ and and $(1-\epsilon)R$ as a function of R. The abcissa of the unique intersection point is $R = C_F^\epsilon$.

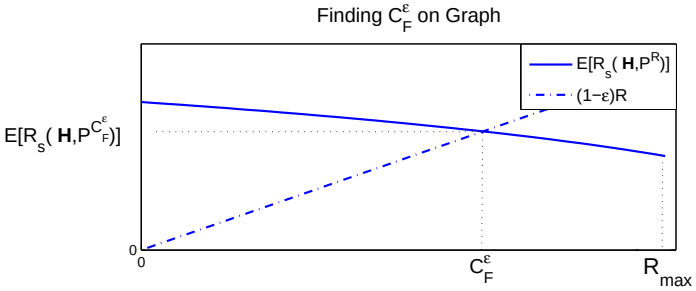

Fig. 3. Finding C_F^ϵ with graphical approach

Example 2: Consider the same system model in Example 1. We have found that for $R = \frac{0.8}{1-\epsilon}$ bits/channel use is achievable with ϵ probability of secrecy outage with no power control, i.e., $P(\mathbf{h}) = 0.5\ \forall \mathbf{h}$. Let $\epsilon = 0.2$, we will see if we can do better than $R = 1$ with power control. Solving the problem (17)-(20), we can see that[4] the time-sharing, and power expended in each state are as given in Tables III and IV. For $\mathbf{h} \equiv [h_m\ h_e] = [10\ 1]$, i.e., the legitimate channel has a better gain, secure waterfilling is used and when $\mathbf{h} = [10\ 10]$, secret key bits cannot be generated, but channel inversion is used to guarantee a main channel rate of R, which is secured by the excess keys generated during the state $\mathbf{h} = [10\ 1]$. As a result, we can see that $C_F^{0.2} = 1.26$ bits per channel use is achievable, which corresponds to 26% increase with respect to no power control.

B. Main CSI

Here, we provide the optimal power control strategy $P^*(h_m)$, which solves the optimization problem (10)-(12). Let us define $P_w(h_m, \lambda)$ as the maximum of 0, and the solution of the following equation

$$\frac{\partial \mathbb{E}[R_s(\mathbf{H}, P)]}{\partial P(h_m)} = \frac{h_m \mathbb{P}(h_e \leq h_m)}{1 + h_m P(h_m)} - \int_0^{h_m} \left(\frac{h_e}{1 + h_e P(h_m)} \right) f(h_e) dh_e - \lambda = 0$$

$P_w(h_m, \lambda)$ will replace $P_{\text{wf}}(\mathbf{h}, \lambda)$ in the full CSI case.

Theorem 4: $P^*(h_m)$ is the unique solution to

$$P^*(h_m) = P_w(h_m, \lambda^*) + \mathbf{1}(h_m \geq c) \left(P_{\text{inv}}(h_m, C_M^\epsilon) - P_w(h_m, \lambda^*)\right)^+ \quad (21)$$

subject to: $\lambda^* > 0$

$$C_M^\epsilon = \mathbb{E}[R_s(\mathbf{H}, P^*)]/(1-\epsilon) \quad (22)$$

$$\mathbb{P}(H_m \geq c) = 1 - \epsilon \quad (23)$$

$$\mathbb{E}[P^*(H_m)] = P_{\text{avg}} \quad (24)$$

where $\mathbb{E}[R_s(\mathbf{H}, P^*)]$ is the expected secrecy rate under the power allocation policy $P^*(h_m)$.
The graphical solution in Figure 3 to find C_F^ϵ also generalizes to the main CSI case.

TABLE III
TIME SHARING REGIONS

$\downarrow h_m \setminus h_e \rightarrow$	1	10
1	wf	wf
10	wf	inv

TABLE IV
$P^*(\mathbf{h})$

$\downarrow h_m \setminus h_e \rightarrow$	1	10
1	0	0
10	1.11	0.14

V. Sizing the Key Buffer

The capacity results of Section III assume availability of *infinite size* secret key buffers at the transmitter and receiver, which mitigate the effect of fluctuations in the achievable secret key bit rate due to fading. Finite-sized buffers, on the other hand will lead to a higher secrecy outage probability due to wasted key bits by the key buffer overflows. We revisit the full CSI problem, and we consider this problem at a 'packet' level, where we assume a packet is of fixed size of N bits. We provide the following result.

Theorem 5: Let $\epsilon' > \epsilon$. Let $M_{C_F^\epsilon}(\epsilon')$ be the buffer size (in terms of packets) sufficient to achieve rate C_F^ϵ with at most ϵ' probability of secrecy outage. Then,

$$\lim_{\epsilon' \searrow \epsilon} \frac{M_{C_F^\epsilon}(\epsilon')}{\eta \log(\eta)} \leq 1 \quad (25)$$

where

$$\eta = \frac{\mathbb{V}ar[R_s(\mathbf{H}, P^{C_F^\epsilon})] + (C_F^\epsilon)^2 \epsilon(1-\epsilon)}{(\epsilon' - \epsilon) C_F^\epsilon}.$$

We can interpret the result as follows. If buffer size is infinite, we can achieve rate C_F^ϵ with ϵ probability of secrecy outage. With finite buffer, we can achieve the same rate only with some $\epsilon' > \epsilon$ probability of secrecy outage. Considering this difference to be the price that we have to pay due to the finiteness of the buffer, we can see that the buffer size required scales with $\mathrm{O}\left(\frac{1}{\epsilon' - \epsilon} \log \frac{1}{\epsilon' - \epsilon}\right)$, as $\epsilon' - \epsilon \to 0$.

[4]Although Theorem 3 assumes $\mathbf{H}$ is a continuous random vector, the results similarly hold for the discrete case as well.

VI. Numerical Results

In this section, we conduct simulations to illustrate our main results with two examples. In the first example, we analyze the relationship between the ϵ-achievable secrecy capacity and the average power. We assume that both the main channel and eavesdropper channel are characterized by Rayleigh fading, where the main channel and eavesdropper channel power gains follow an exponential distribution with a mean 2 and 1, respectively. In Figure 4, we plot the ϵ-achievable secrecy capacity as a function of the average power for secrecy outage probability $\epsilon = 0.02$, under both full CSI and main CSI cases. It can be observed that the gap between capacities under full CSI and main CSI vanishes as average power increases, which support the result (13).

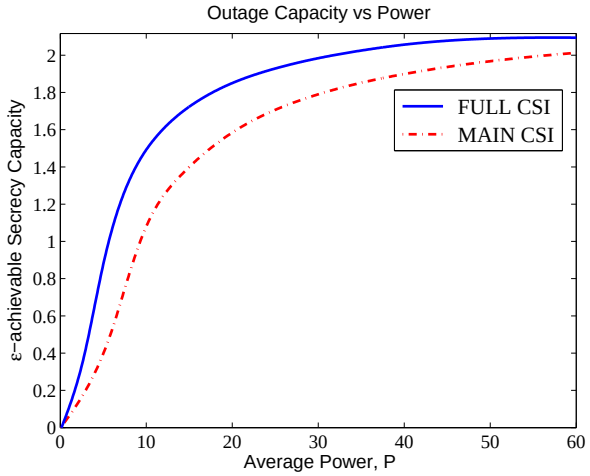

Fig. 4. The ϵ-achievable secrecy capacities as a function of average power, P_{avg}

Next, we study the relationship between the secrecy outage probability and the buffer size for a given rate. We assume that both the main and eavesdropper channel gains follow a chi-square distribution of degree 2, with a mean 2 and 1, respectively. We focus on the full CSI case. In Figure 5, we plot the secrecy outage probabilities, denoted with ϵ', as a function of buffer size M. On the same graph, we also plot our asymptotic result given in Theorem 5, which provides an upper bound on the required buffer size to achieve ϵ' outage probability for rate C_F^{ϵ}, with the assumption that (25) is met with equality for any ϵ'. We can see that, this theoretical result serves as an upper bound on the required buffer size when $\epsilon' - \epsilon$, additional secrecy outages due to key buffer overflows, is very small.

VII. Conclusions

This paper obtained sharp characterizations of the secrecy outage capacity of block flat fading channels under the assumption full and main CSI at the transmitter. In the two cases, our achievability scheme relies on opportunistically exchanging private keys between the legitimate nodes and using them later to secure the delay sensitive information.

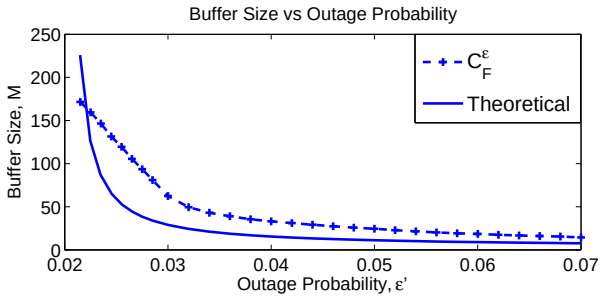

Fig. 5. Relationship between buffer size M, and outage probability ϵ'

We further derive the optimal power control policy in each scenario revealing an interesting structure based by judicious time sharing between time sharing and the optimal strategy for the ergodic. Finally, we investigate the effect of key buffer overflow on the secrecy outage probability.

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] U. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," *Advances in Cryptology - EUROCRYPT 2000, Lecture Notes in Computer Science 1807*, pp.351-368, 2000.

[11] R. G. Gallager, "A Simple Derivation of the Coding Theorem and Some Applications," *IEEE Transactions on Information Theory*, vol. IT-11, pp. 3-18, January 1965.

[12] 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.

[13] 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," *Proceedings of IEEE INFOCOM 2010*, pp.1-9, 14-19 March 2010

[14] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal and N. B. Shroff, "Secrecy Outage Capacity of Fading Channels," *arXiv:1112.2791v1 [cs.IT]*, Dec 2011