On the Secrecy Capacity of Fading Gaussian Wiretap Channel

Md. K. Hossan and S. Karmakar and A. Ghosh

Abstract—We consider the fast-fading Gaussian wiretap channel with single antenna nodes and without channel state information at the transmitter (CSIT), where the fading processes of the two links are arbitrary and independent of each other. We derive an upper bound to the secrecy capacity for this channel and an achievable rate as well. Subsequently, we identify a class of channel statistics for which the outer bound and the achievable rates are identical thereby characterizing the exact secrecy capacity of the channel. The class of channels with such channel statistics are called stochastically degraded in this paper. Many practical wireless settings including the Rayleigh fading environment fall under this stochastically degraded class. We illustrate our results by computing explicit expression for the secrecy capacity for Rayleigh distributed wiretap channels.

I. INTRODUCTION

Information-theoretic approach for secret communication first appeared in Shannon’s work [1]. In the pioneering paper on wiretap channel [2], Wyner laid out the mathematical formulation of the information-theoretic secrecy. Wyner considered a discrete memoryless wiretap channel where Eve receives a degraded version of Bob’s received signal. Csiszár and Körner [3] generalized Wyner’s result to the general discrete memoryless broadcast channel and found the secrecy capacity of the channel:

\[ C_s = \max_{V;Y,Z} \left[ I(V;Y) - I(V;Z) \right] \]

Over the years the above optimization problem has been solved for wiretap channels with both fading and time invariant channel coefficients [4]. In this paper we consider the fading wiretap channel with single antenna at each node.

The secrecy capacity of slow fading channel with single-input multiple-output (SIMO) with CSIT was characterized in [5]. In [6], secure transmission of information over fast fading channel was studied with the assumption that the legitimate receiver’s channel state information is available at the transmitter. Secrecy capacity for nodes with multiple antennas was studied in [7], [8], [9] where the legitimate receivers CSIT is necessary.

Since, channel state information (CSI) at transmitter is important to exploit the randomness of the channel to obtain physical layer security, previous works mostly focused with the assumptions that CSI is available at the transmitter. But in a fast-fading wireless channel, timely feedback of the channel measurement information by the receiver to the transmitter is a challenging task. Although there are some results for the scenario without any channel state information at the transmitter (CSIT), most of those works were carried out for specific channel state distribution. The capacity of a fast-fading Gaussian wiretap channel with general fading distribution and No-CSIT is still an open problem.

Ergodic secrecy capacity for fast fading channel without CSIT was investigated in [10], [11]. In [11], authors found some upper and lower bounds on the secrecy rate for a multiple-input single-output (MISO) wiretap channel. Achievable secrecy rate for fast Rayleigh fading channel was considered in [12]. In that paper, the legitimate channel is fixed-SNR Gaussian channel and the eavesdropper channel is a Rayleigh fading channel with no CSIT. The author showed that for that channel model, there can be a positive secrecy rate even if the legitimate channel is worse than the eavesdropper channel on the average. The strategy to achieve positive rate is to inject optimal white noise which can be computed from the statistics of the channel states. In [13] the capacity of a Rayleigh distributed fast-fading wiretap channel with multiple antennas everywhere was computed assuming the number of receive antennas at the legitimate receiver is larger or equal to that of the eavesdropper. A special case of this result characterizes the fast-Rayleigh distributed SISO wiretap channel.

To take the next step along the line of the aforementioned work, here we consider fading Gaussian wiretap channel where both the links are fast fading with arbitrary fading distribution and the instantaneous channel states are available at the receivers but not at the transmitter. This is the case in many practical wireless communication systems where channel states can only be measured by the receivers which cannot inform the transmitter of the state accurately in a timely manner due to the fast speed of variation of the channel coefficients. Besides, it is not reasonable to expect some feedback from Eve to Alice because of the malicious nature of the former user. Now, assuming that the fading statistics of the two links are arbitrary, we first derive an outer bound to the secrecy capacity of the channel and an achievable secrecy rate. We also identify a special class of channels for which the upper bound and the achievable rate are identical and therefore characterizes the exact secrecy capacity of the channel.

II. CHANNEL MODEL AND SOME PRELIMINARIES

We consider a 2-user Fast fading wiretap channel as shown in Fig 1. The input output model of the channel can be written as
mean and unit variance. For a fading channel where the fading
channel is memoryless and changing independently at each
symbol time, we can omit the time index for simpler notation.

When either of the legitimate or eavesdropper channel is in
state $s$, the receiver observes an output identically distributed
as
\[
Y^{(s)} := \sqrt{s} X + U,
\]
where $U \sim \mathcal{N}(0, 1)$, which is a normal distribution with zero
mean and unit variance. For a fading channel where the fading
state is a random process $S$, the ergodic capacity of the point-
to-point fading channel (7) with unit transmit power is
\[
C_e(S) := \frac{1}{2} E_S \left[ \log(1+s) \right] = \frac{1}{2} \int_0^\infty f_S(s) \log(1+s) ds, \tag{8}
\]
and the capacity is achieved with Gaussian input [14][15].

III. MAIN RESULT

Here, we state the main results about the characterization of the
secrecy capacity of the fading Gaussian wiretap channel
defined by (4) and (5). Denoting the complementary Cumulative
Distribution Function (CDF) of a random variable $S$ as by
$\bar{F}_S(s)$, i.e., $\bar{F}_S(s) = P[S \geq s]$ we have the following result.

Theorem 1: If $R_s$ represents an achievable secrecy rate,
on the fast fading Gaussian wiretap channel defined in the
previous section, then
\[
R_s \leq \log e \int_{J_1} (\bar{F}_{S_1}(s) - \bar{F}_{S_2}(s)) \frac{1}{1+s} ds, \tag{9}
\]
where $J_1 := \{ s \geq 0 | \bar{F}_{S_1}(s) > \bar{F}_{S_2}(s) \}$.

While it is not clear if a single coding scheme can achieve
the secrecy capacity of the channel for all possible channel
statistics, in what follows, we identify one class of channel
statistics for which the above upper bound can be achieved.
As a result for these class of channels we have exact secrecy
capacity characterization. To the best of our knowledge, this
is the first capacity result on Ergodic fading wiretap channel.

Definition 1 (Stochastically degraded channel): We call a
fast fading wiretap channel described by equations (4) and (5)
a stochastically degraded channel if $\bar{F}_{S_1}(s) \geq \bar{F}_{S_2}(s), \ \forall s \geq 0$.
In what follows, we shall use the notation $S_1 \geq_{st} S_2$ to
denote a stochastically degraded wiretap channel.

Theorem 2 below provides the secrecy capacity for this class
of channels.

Theorem 2: The secrecy capacity of the stochastically
degraded fading Gaussian wiretap channel of figure 1 is given
by
\[
C_s = \log e \int_0^\infty (\bar{F}_{S_1}(s) - \bar{F}_{S_2}(s)) \frac{1}{1+s} ds. \tag{10}
\]
In the following two subsections we shall prove these two
theorems.

A. Upper bound to the secrecy capacity

Lemma 1 (Lemma 2 in [16]): The fading Gaussian wiretap
channel $(S_1, S_2)$ satisfying $S_1 \geq_{st} S_2$ is a degraded wiretap
channel.

Now, if we define
\[
\bar{F}_{\bar{S}}(s) = \max [\bar{F}_{S_1}(s), \bar{F}_{S_2}(s)]. \tag{11}
\]
then by the above lemma we can say that the Gaussian wiretap
channel $(\bar{S}_1, \bar{S}_2)$ is a degraded wiretap channel. Also, from
the definition of $\bar{S}$ it is clear that if $R_s$ is a secrecy rate achievable
on the $(S_1, S_2)$ wiretap channel then it is also achievable on
the $(\bar{S}_1, \bar{S}_2)$ channel. As a result it is upper bounded by the
secrecy capacity of the $(\bar{S}_1, \bar{S}_2)$ channel.

Fig. 1: Fading Gaussian wiretap channel.

\[
Y(t) = \sqrt{S_1} e^{j\theta_1(t)} X(t) + U_1(t), \tag{2}
\]
\[
Z(t) = \sqrt{S_2} e^{j\theta_2(t)} X(t) + U_2(t), \tag{3}
\]
where $X(t), Y(t), Z(t)$ are the signals transmitted by Alice
and those received by Bob and Eve, respectively at time $t$.
$(S_1(t), \theta_1(t))$ and $(S_2(t), \theta_2(t))$ denotes the channel gains
and phases of the legitimate and eavesdropper channel respec-
tively, which are mutually independent and i.i.d. across time.
$U_1(t)$ and $U_2(t)$ are mutually independent circular symmetric
complex Gaussian (CSCG) noises with unit variance which are
also assumed to be i.i.d. across time. Since, our wiretap
channel is memoryless and changing independently at each
symbol time, we can omit the time index for simpler notation.
Hence our channel model becomes
\[
Y = \sqrt{S_1} e^{j\theta_1} X + U_1, \tag{4}
\]
\[
Z = \sqrt{S_2} e^{j\theta_2} X + U_2. \tag{5}
\]
The complex channel can be treated as a pair of identical
real channels independent of each other. If we compute the
achievable rate for one channel, same can be achieved for
the other channel. Hereafter, we shall consider only the real-
valued Gaussian wiretap channel. The capacity of the original
complex Gaussian wiretap channel is just double of the
capacity we get for the real-valued channel. Hence our final
channel model becomes,
\[
Y = \sqrt{S_1} X + U_1, Z = \sqrt{S_2} X + U_2, \tag{6}
\]
where $X$ is the transmitted signal by Alice with unit power
constraint, i.e., $E(X^2) \leq 1$. In the sequel, we shall refer to the
channel in equation (6) as the fading Gaussian wiretap channel
$(S_1, S_2)$.

When either of the legitimate or eavesdropper channel is in
state $s$, the receiver observes an output identically distributed
as
\[
Y^{(s)} := \sqrt{s} X + U, \tag{7}
\]
the secrecy capacity expression for a degraded wiretap channel available in [3], we get

\[ R_s \leq \max \left[ I(X; Y, \tilde{S}_1) - I(X; Z, S_2) \right] \]  \hspace{1cm} (12)

\[ = \max \left[ I(X; \tilde{S}_1) + I(X; Y|\tilde{S}_1) - I(X; Z, S_2) \right] \]  \hspace{1cm} (13)

\[ = \max \left[ I(X; Y|\tilde{S}_1) - I(X; Z|S_2) \right] \]  \hspace{1cm} (14)

\[ = \max \left[ h(Y|\tilde{S}_1) - h(Y|X, \tilde{S}_1) - h(Z|S_2) + h(Z|X, S_2) \right] \]  \hspace{1cm} (15)

\[ = \max \left[ h(Y|\tilde{S}_1) - h(U_1) - h(Z|S_2) + h(U_2) \right] \]  \hspace{1cm} (16)

(13) follows from the chain rule of mutual information. Since, we assume no CSI at transmitter, hence the input and channel states are independent to each other. Therefore, the mutual information between input and channel state is zero and we have (14). Since, \( U_1, U_2 \sim \mathcal{N}(0,1) \), their differential entropies are same and cancel each other resulting (16). Using (7), we derive the average differential entropy in (17).

Let us define

\[ \bar{F}_d(s) := \bar{F}_{S_1}(s) - \bar{F}_{S_2}(s). \]  \hspace{1cm} (20)

Differentiating (20), we get

\[ \frac{d}{ds} F_d(s) = \frac{d}{ds} \left( \bar{F}_{S_1}(s) - \bar{F}_{S_2}(s) \right) \]  \hspace{1cm} (21)

\[ = -f_{S_1}(s) + f_{S_2}(s). \]  \hspace{1cm} (22)

By denoting, \( f_d(s) := -\frac{d}{ds} F_d(s) \), we can write (22) as

\[ f_d(s) = f_{S_1}(s) - f_{S_2}(s). \]  \hspace{1cm} (23)

Substituting (23) in (19), we get

\[ R_s \leq \max \left[ \int_0^\infty f_d(s)h(Y(s))ds \right]. \]  \hspace{1cm} (24)

Using integration by parts, we get

\[ \int_0^\infty f_d(s)h(Y(s))ds = \left[ h(Y(s)) \int f_d(s)ds \right]_0^\infty \]

\[ - \int_0^\infty \left[ \frac{d}{ds}h(Y(s)) \int f_d(s)ds \right]ds \]  \hspace{1cm} (25)

\[ = \bar{F}_d(0)h(U) - \bar{F}_d(\infty)h(\infty X + U) \]

\[ + \int_0^\infty \bar{F}_d(s) \frac{d}{ds}h(Y(s))ds \]  \hspace{1cm} (26)

\[ = \int_0^\infty \bar{F}_d(s) \frac{d}{ds}h(Y(s))ds. \]  \hspace{1cm} (27)

From the definition of \( \bar{F}_d(s) \) in (20), we have \( \bar{F}_d(0) = \bar{F}_{S_1}(0) - \bar{F}_{S_2}(0) = 1 - 1 = 0 \) and \( \bar{F}_d(\infty) = \bar{F}_{S_1}(\infty) - \bar{F}_{S_2}(\infty) = 0 - 0 = 0 \) which results (27). Consider the term \( \bar{F}_d(h(\infty X + U)) \) in (26), where the CCDF is a decreasing function of its argument and the differential entropy increases logarithmically with variance of the RV. The rate of decrease of the CCDF is faster than the rate of increase of the differential entropy. Hence the combined term results zero.

Substituting (27) in (24), we get

\[ R_s \leq \max \left[ \int_0^\infty \bar{F}_d(s) \frac{d}{ds}h(Y(s))ds \right]. \]  \hspace{1cm} (28)

Since \( I(X; Y(s)) = h(Y(s)) - h(U) \), we have

\[ \frac{d}{ds} I(X; Y(s)) = \frac{d}{ds} h(Y(s)). \]  \hspace{1cm} (29)

Substituting this in (28) we get

\[ R_s \leq \max \left[ \int_0^\infty \bar{F}_d(s) \frac{d}{ds} I(X; Y(s)) ds \right]. \]  \hspace{1cm} (30)

It was shown in [17] that

\[ \frac{d}{ds} I(X; Y(s)) = \log e \text{mmse}(s), \]  \hspace{1cm} (31)

where minimum mean square error (mmse) is given by

\[ \text{mmse}(s) := E \left[ \left( X - E[X|Y(s)] \right)^2 \right]. \]  \hspace{1cm} (32)

Furthermore, we have an upper bound for mmse [16], which is given by

\[ \text{mmse}(s) \leq \frac{1}{1 + s}. \]  \hspace{1cm} (33)

We define

\[ \tilde{I}_1 := \{ s \geq 0 | \bar{F}_d(s) > 0 \}. \]  \hspace{1cm} (34)

Hence, our upper bound becomes

\[ R_s \leq \frac{\log e}{2} \int_{\tilde{I}_1} \bar{F}_d(s) \frac{1}{1 + s} ds. \]  \hspace{1cm} (35)

If we consider signaling for both in-phase and quadrature component channels, the final upper-bound can be written as

\[ R_s \leq \log e \int_{\tilde{I}_1} \left( \bar{F}_{S_1}(s) - \bar{F}_{S_2}(s) \right) \frac{1}{1 + s} ds. \]  \hspace{1cm} (36)

1) Special Case: Upper-bound for a Degraded Channel:

Clearly, for a stochastically degraded wiretap channel, the partition of channel states would not be required. As was stated in Lemma 1, for a stochastically degraded wiretap channel, \( \bar{F}_{S_1}(s) \geq \bar{F}_{S_2}(s), \forall s \). Hence the partition of SNR \( \tilde{I}_1 = \{ s \geq 0 \} \) for a for a stochastically degraded fading Gaussian wiretap channel, the secrecy rate upper-bound is given by

\[ R_{sd} \leq \log e \int_0^\infty \left( \bar{F}_{S_1}(s) - \bar{F}_{S_2}(s) \right) \frac{1}{1 + s} ds. \]  \hspace{1cm} (37)
B. Fading Gaussian Wiretap Channel: Achievability

Our achievability scheme for fading Gaussian wiretap channel follows a different approach than that of the layered case. We cannot use the layered decoding argument for Gaussian case, because we cannot just dictate the eavesdropper to obey the decoding rule as we instruct. The eavesdropper can have arbitrary decoding technique, hence the layered achievability argument for Gaussian case fails.

Instead, we shall derive the achievable scheme directly from the capacity expression for some familiar input distributions which have the potential to be the optimal. Then, we compare those achievable rates to the upper-bound (36) to see how close they are.

We have capacity expression for a discrete memoryless wire-tap channel which is given by (1). We are restating the expression here.

\[ C_s = \max_{X \to Y; Z} \left[ I(V; Y) - I(V; Z) \right] \tag{38} \]

\( C_s \) is maximum secrecy rate where the maximization is taken over all possible joint distributions of \( P_{V,X}(v, x) \). Instead of looking for the optimal \( V, X \) that gives the maximum secrecy rate we choose some specific distributions of \( V, X \). The rate we get for that specific distribution is an achievable rate and (38) serves as an upper-bound for all achievable rates. We carefully choose \( V, X \) that have potential to be optimal. Since for most of the channel, Gaussian input is optimal, we shall choose \( V, X \) both to be Gaussian in our achievable scheme.

1) Achievable Rate with \( V = X \sim \mathcal{N}(0,1) \): We shall evaluate the achievable rate for input with Gaussian distribution and set the auxiliary random variable \( V \) equal to the input. In this setting, we have \( V = X = X^G \) where \( X^G \sim \mathcal{N}(0,1) \). We denote this achievable secrecy rate as \( R_s^G \).

From (38), we have

\[ R_s^G = I(X^G; Y | S_1) - I(X^G; Z | S_2) \tag{39} \]

\[ = E_{S_1} \left[ \log(1 + s_1) \right] - E_{S_2} \left[ \log(1 + s_2) \right]. \tag{40} \]

In (40), we have used the ergodic rate of point-to-point fading channel with Gaussian input as given by (8) for a complex channel.

We can simplify

\[ E_{S_1} \left[ \log(1 + s_1) \right] = \int_0^\infty f_{S_1}(s) \log(1 + s) ds \tag{41} \]

\[ = \left\{ \log(1 + s) \int_0^\infty f_{S_1}(s) ds \right\} \bigg|_{0}^{\infty} - \int_0^\infty \frac{df_{S_1}(s)}{ds} \log(1 + s) \int f_{S_1}(s) ds \bigg|_{0}^{\infty} ds \tag{42} \]

\[ = - \log(1) F_{S_1}(0) + \log(\infty) F_{S_1}(\infty) \]

\[ - \log e \int_0^\infty \left[ -\frac{1}{1 + s} \right] F_{S_1}(s) ds \tag{43} \]

\[ = \log e \int_0^\infty \frac{1}{1 + s} \bar{F}_S(s) ds. \tag{44} \]

Please note that for continuous RV \( S \), \( \bar{F}_S(s) = 1 - F_S(s) \) where \( F_S(s) \) is the CDF of \( S \). By differentiating we get \( \frac{d}{ds} \bar{F}_S(s) = -f_S(s) \) and further integrating we get \( \int f_S ds = -\bar{F}_S(s) \). Substituting this fact in (42) resulted (43).

Similarly we have

\[ E_{S_2} \left[ \log(1 + s_2) \right] = \log e \int_0^\infty \frac{1}{1 + s} \bar{F}_{S_2}(s) ds. \tag{45} \]

Substituting the results of (44) and (45) in (40), we get

\[ R_s^G = \log e \int_0^\infty \frac{1}{1 + s} \bar{F}_{S_1}(s) ds \]

\[ - \log e \int_0^\infty \frac{1}{1 + s} \bar{F}_{S_2}(s) ds \tag{46} \]

\[ = \log e \int_0^\infty \left( \bar{F}_{S_1}(s) - \bar{F}_{S_2}(s) \right) \frac{1}{1 + s} ds. \tag{47} \]

For a general wiretap channel, the difference between the upper-bound. But if the wiretap channel is a stochastically degraded wire-tap channel, we can say that Gaussian input without prefixing is optimal, i.e., the secrecy rate \( R_s^G \) for Gaussian input matches the upper bound (37).

C. Secrecy Capacity of Fading Wiretap Channel in Urban Area

In previous sections we have proved that Gaussian input can achieve the secrecy capacity for stochastically degraded wire-tap channels. There are many practical wireless communication systems where, the channels are either stochastically degraded or reversely degraded. For those class of wire-tap channels, our theorem 3 can be readily used to compute the secrecy capacities. In this section we shall consider such a practically predominant class of channels: channels with Rayleigh fading distribution. To model the wireless environment in an urban area, cellular wireless networks generally use the Rayleigh fading model to represent the random channel coefficients [18]. This is because Rayleigh fading model works better for the heavily built up urban area where there is no dominant line of sight propagation and the obstacles to wireless signals are more or less uniformly distributed between the transmitters and the receivers.

For Rayleigh fading wireless channel, the channel gain \( \sqrt{s} \) is Rayleigh distributed and hence \( s \) has an exponential distribution, \( f_S(s) = \lambda e^{-s \lambda} \), the corresponding CDF is \( F_S(s) = e^{-s \lambda} \) where the average SNR of the channel is given by \( E[s] = \frac{1}{\lambda} \).

Hence the CDF of the channel is

\[ \bar{F}_S(s) = e^{-s \lambda}. \tag{48} \]

We plot the CDF against channel strength for different values of \( \lambda \). Note that in figure 2, the CDF for lower variance remains above the higher ones for all values of channel state. Since, the Rayleigh fading model is the most accurate model for urban setting, therefore the wiretap channel in a cellular wireless network environment is either stochastically degraded or reversely degraded. For those class of channels, our general converse is tight and achievable. Hence, we can apply theorem 2 to compute the secrecy capacity.

Consider a Rayleigh fading Gaussian wiretap channel. The CDF of the legitimate channel is

\[ \bar{F}_{S_1}(s) = e^{-s \lambda_1}. \tag{49} \]
Fig. 2: CCDFs vs channel state for different values of \( \lambda \) for Rayleigh fading.

and the CCDF of the eavesdropper is

\[
F_{S_1}(s) = e^{-s\lambda_2}.
\]  
(50)

We assume \( \lambda_1 \leq \lambda_2 \). Otherwise, computing secrecy capacity is trivial because, in that case, the capacity is zero.

The secrecy capacity is given by Theorem 2

\[
C_{s,\text{urban}} = \log_e \int_0^\infty (e^{-s\lambda_1} - e^{-s\lambda_2}) \frac{1}{1+s} ds.
\]  
(51)

Fig. 3: Secrecy Capacity vs SNR of the legitimate receiver when the SNR of the eavesdropper is held constant for fading Gaussian wire-tap channel with Rayleigh fading.

Fig. 4: Secrecy Capacity vs SNR of the eavesdropper when the ratio of the SNRs is held constant for fading Gaussian wire-tap channel with Rayleigh fading.

IV. CONCLUSION

We derive an outer bound to the capacity of the fading channel where the time varying channel coefficients of both the main and eavesdropper channel can assume arbitrary statistics. We then identify a rather broad class of channels - called stochastically degraded channels here - for which we characterize the secrecy capacity of the channel. We show that a Gaussian distributed input can achieve a rate same as the upper bound giving the secrecy capacity of the channel. Moreover, the capacity for channels with exponential and rician channel state distribution has been derived. In other wireless settings, the general upper bound provides the first step towards exact capacity characterization.

REFERENCES