Average Secrecy Capacity of the Weibull Fading Channel

Xian Liu

***Abstract*: In this paper, the information-theoretic secrecy of Weibull fading channels is investigated. The present work is a generalization of the analysis on Rayleigh fading. This paper focuses on the scenario that the channel state information is available to the legitimate transmitter. The cases of single and multiple eavesdroppers are discussed. Several formulas of the average secrecy capacity are derived. Profile examples are illustrated and discussed.**

Keywords: Information-theoretic secrecy, secrecy capacity, Weibull fading.

I. INTRODUCTION

Recently, there was an ever increasing interest of exploring the *secrecy capacity* (SC) in digital communications over fading channels ([1] and the references therein). The studies on Nakagami-m SC, log-normal SC, and Rician SC have been reported ([2] and the references therein). However, to the author's best knowledge, the Weibull SC has not been well addressed in the literature, except a recent paper [3].

In wireless communications, the Weibull model has been used to describe the fading induced by multipath propagations, usually for indoor radio systems and sometimes also for outdoor radio systems. Extensive experiments and simulations have been reported in the literature. In this paper, we investigate the *average secrecy capacity* (ASC) of the system subject to the Weibull fading.

II. SYSTEM MODEL AND SECRECY CAPACITY

The concept of SC is based on the notion of *information-theoretic secrecy* (ITS) [4-6]. In the context of SC analysis, the communication system is usually abstracted by three entities: a legitimate transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper. When Alice sends information to Bob, the eavesdropper can intercept the information (Fig. 1).

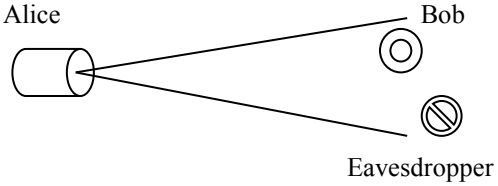

Figure 1. System model 1.

X. Liu is with the Department of Systems Engineering, University of Arkansas at Little Rock, AR 72204, USA.

In the present work, we assume that the *channel state information* (CSI) of the eavesdropper is available to Alice. This paradigm could happen if Alice is in charge of the registrations and link maintenance for all receivers in a specific region. The paradigm that the CSI of Weibull fading is not available to Alice has been discussed in a companion paper [3]. Consider the path *signal-to-noise ratio* (SNR) per symbol. Let the instantaneous SNR of Bob and the eavesdropper be U and W, respectively.

In the case of Weibull fading, the *probability density function* (PDF) of U takes the following form [7, eq. (2.29)]:

$$f_U(u) = \frac{a}{2}\left[\frac{1}{u_0}\Gamma\left(1+\frac{2}{a}\right)\right]^{\frac{a}{2}} u^{(a/2)-1}\exp\left(-\left[\frac{u}{u_0}\Gamma\left(1+\frac{2}{a}\right)\right]^{\frac{a}{2}}\right), \quad (u \ge 0,\ a > 0) \qquad (1)$$

where a is the fading factor of the main channel, $u_0 = E(U)$ is the mean of U, and $\Gamma(\bullet)$ is the gamma function, defined as:

$$\Gamma(x) = \int_0^\infty t^{x-1}\exp(-t)dt.$$

In general, the fading gets severer as the factor a decreases [7, Sec. 2.2.1.5]. Note that, when $a = 2$, the Weibull distribution reduces to the well-known exponential distribution. Similarly, for the eavesdropper channel, the PDF of W is:

$$f_W(w) = \frac{b}{2}\left[\frac{1}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{\frac{b}{2}} w^{(b/2)-1}\exp\left(-\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{\frac{b}{2}}\right), \quad (w \ge 0,\ b > 0) \qquad (2)$$

where b is the fading factor of the eavesdropper channel and $w_0 = E(W)$ is the mean of W. Corresponding to (1) and (2), the *cumulative probability functions* (CDFs) take the following form:

$$F_U(u) = 1 - \exp\left(-\left[\frac{u}{u_0}\Gamma\left(1+\frac{2}{a}\right)\right]^{a/2}\right), \qquad (3)$$

$$F_W(w) = 1 - \exp\left(-\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{b/2}\right). \qquad (4)$$

In the present work, the analysis is based on the notion described in [1, Lemma 1], where the SC for one realization

978-1-4673-9292-1/16/$31.00 ©2016 IEEE

of the SNR pair (U,W) of the quasi-static complex fading wiretap-channel is expressed as:

$$C_s(U,W)=\begin{cases}\log_2(1+U)-\log_2(1+W), & (U>W)\\ 0. & (U\le W)\end{cases} \quad (5)$$

Note that the SC C_s given in (5) is a random variable. Accordingly, the average secrecy capacity (ASC) of the channel can be defined as follows:

$$E(C_s)=\int_0^\infty\int_w^\infty \log_2\left(\frac{1+u}{1+w}\right)f_U(u)f_W(w)dudw. \quad (6)$$

ASC is a fundamental notion in studies on ITS. As pointed out in [1], if the CSI of the eavesdropper channel is known by Alice, then with appropriate coding the ASC is achievable. Substituting (1) and (2) into (6), we have:

$$E(C_s)=\frac{ab}{4}\left[\frac{1}{u_0}\Gamma\left(1+\frac{2}{a}\right)\right]^{a/2}\left[\frac{1}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{b/2}$$
$$\times\int_0^\infty\int_w^\infty \log_2\left(\frac{1+u}{1+w}\right)u^{(a/2)-1}\exp\left(-\left[\frac{u}{u_0}\Gamma\left(1+\frac{2}{a}\right)\right]^{\frac{a}{2}}\right)$$
$$\times w^{(b/2)-1}\exp\left(-\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{\frac{b}{2}}\right)dudw. \quad (7)$$

For general a and b, a closed-form expression of (7) does not seem to exist. Thus a numerical implementation is needed. However, it is inconvenient to directly implement (7) since it involves a double integral with infinite bounds. It is desirable to convert (7) into a single integral with finite bounds. This is possible under some conditions. For example, with $b=a$ we have:

$$E(C_s)=\frac{2}{a}\log_2\left(1+\frac{u_0^{a/2}}{w_0^{a/2}}\right)$$
$$-\int_0^1\log_2\left(1+\frac{2\Gamma(2/a)\left\{[1+(u_0/w_0)^{a/2}]^{2/a}-1\right\}}{2\Gamma(2/a)+au_0(-\ln t)^{2/a}}\right)dt. \quad (8)$$

The proof of (8) is omitted due to the space limit. In the present work, however, we are more interested in the asymptotic performance of ASC in the regime of high SNR $(U>>1, W>>1)$. Further analysis is presented in following two sections.

III. The Average Secrecy Capacity in the Regime of High SNR, Single Eavesdropper

In the regime of high SNR $(U>>1, W>>1)$, eq. (5) becomes:

$$C_s(U,W)=\begin{cases}\log_2 U-\log_2 W, & (U>W)\\ 0. & (U\le W)\end{cases} \quad (9)$$

Accordingly, eq. (7) becomes:

$$E(C_s)=\frac{ab}{4}\left[\frac{1}{u_0}\Gamma\left(1+\frac{2}{a}\right)\right]^{a/2}\left[\frac{1}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{b/2}$$
$$\times\int_0^\infty\int_w^\infty \log_2\left(\frac{u}{w}\right)u^{(a/2)-1}\exp\left(-\left[\frac{u}{u_0}\Gamma\left(1+\frac{2}{a}\right)\right]^{\frac{a}{2}}\right)$$
$$\times w^{(b/2)-1}\exp\left(-\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{\frac{b}{2}}\right)dudw. \quad (10)$$

Up to this point, the analysis has been conducted in the two dimensional space. However, with a new variable $Z=U/W\ \ (0\le Z<\infty)$, eq. (10) can be converted to a one-dimensional problem:

$$E(C_s)=\int_1^\infty \log_2(z)f_Z(z)dz, \quad (11)$$

where $f_Z(z)$ is the PDF of Z. Note that the lower bound of integral in (11) is unit due to (9). According to probability theory, we have:

$$f_Z(z)=\int_0^\infty wf_U(wz)f_W(w)dw. \quad (12)$$

Accordingly, the CDF of Z can be formulated as follows:

$$F_Z(z)=\int_0^z f_Z(t)dt=\int_0^z\int_0^\infty wf_U(wt)f_W(w)dwdt$$
$$=\int_0^\infty f_W(w)\left[\int_0^{wz}f_U(y)dy\right]dw=\int_0^\infty f_W(w)F_U(wz)dw. \quad (13)$$

Substituting (2) and (3) into (13), with several transformations, we obtain:

$$F_Z(z)=\frac{b}{2}(H_1-H_2), \quad (14)$$

where

$$H_1=\int_0^\infty w^{(b/2)-1}\left[\frac{1}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{\frac{b}{2}}$$
$$\times\exp\left(-\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{\frac{b}{2}}\right)dw=\frac{2}{b}, \quad (15)$$

$$H_2 = \int_0^\infty w^{(b/2)-1}\left[\exp\left(-\left[\frac{wz}{u_0}\Gamma\left(1+\frac{2}{a}\right)\right]^{\frac{a}{2}}\right)\right]$$
$$\times\left[\frac{1}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{\frac{b}{2}}\exp\left(-\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{\frac{b}{2}}\right)dw$$
$$=\left(\frac{2}{b}\right)\int_0^\infty \exp\left[-t-\left(\frac{b\Gamma(2/a)z}{a\Gamma(2/b)r}\right)^{\frac{a}{2}}t^{a/b}\right]dt, \qquad (16)$$

and

$$r = u_0 / w_0. \qquad (17)$$

Note that, in the derivation of (16), the following identity was incorporated:

$$\Gamma(x+1) = x\Gamma(x). \qquad (18)$$

Substituting (15) and (16) into (14), we have:

$$F_Z(z) = 1 - \int_0^\infty \exp\left[-t-\left(\frac{b\Gamma(2/a)z}{a\Gamma(2/b)r}\right)^{\frac{a}{2}}t^{a/b}\right]dt. \qquad (19)$$

As a general formula, eq. (19) can be used to evaluate the ASC for a realization of U and W with arbitrary fading parameters a and b. In the following, we focus on the case of $a = b$. In this case, eq. (19) becomes

$$F_Z(z) = 1 - \int_0^\infty \exp\left[-t-\left(\frac{z}{r}\right)^{\frac{a}{2}}t\right]dt = 1 - \frac{1}{1+(z/r)^{a/2}}. \qquad (20)$$

Accordingly, we have:

$$E(C_s) = \int_1^\infty \log_2(z) f_Z(z)dz = \frac{1}{\ln 2}\int_1^\infty \frac{dz}{z[1+(z/r)^{a/2}]}. \qquad (21)$$

The solution for the type of integral in (21) is not directly available in standard handbooks. In fact, we can easily prove:

$$E(C_s) = \frac{2}{a}\log_2\left(1+r^{a/2}\right) \qquad (22)$$

Note that the case of $a = 2$ corresponds to the Rayleigh fading regarding signal envelope:

$$E(C_s) = \log_2(1+r). \qquad (23)$$

Two sets of normalized profiles of (22) and (8) are shown in Figs. 2 and 3, where the normalization is done with respect to the Shannon capacity with SNR equal to u_0. Recall that u_0 and w_0 are the mean SNR of the main channel and eavesdropper channel, respectively. It is observed that the deviations between the asymptotic and exact curves become invisible as w_0 increases. Thus (22) is fairly applicable to the high SNR regime. Note that the profiles with $a = 2$ (Fig. 2) are consistent with the results presented in [1, Fig. 3], where only the Rayleigh case was investigated.

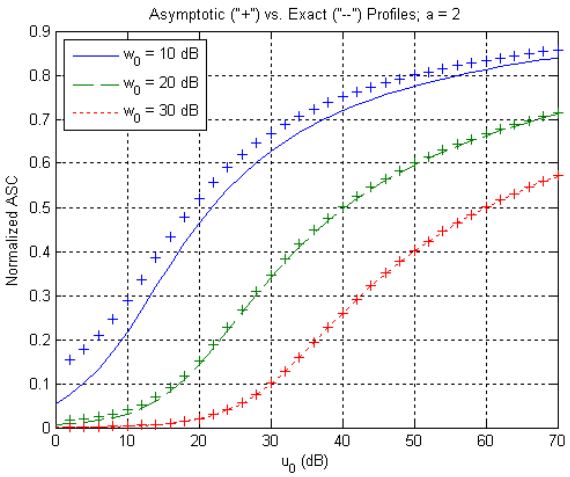

Figure 2. Comparison 1 of asymptotic to exact curves.

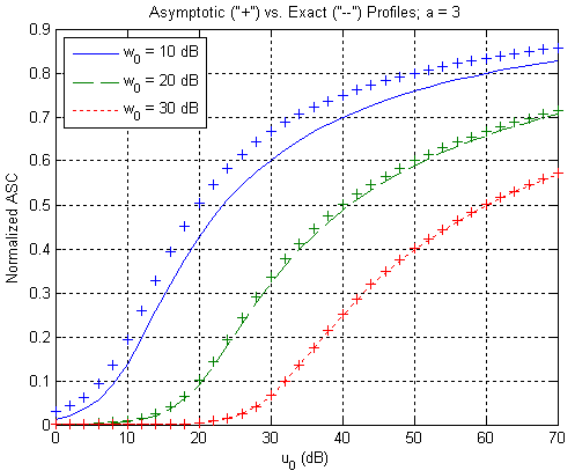

Figure 3. Comparison 2 of asymptotic to exact curves.

IV. The Average Secrecy Capacity in the Regime of High SNR, Double Eavesdroppers

In this section, we consider a generic system consisting of four entities: Alice, Bob, eavesdropper 1, and eavesdropper 2. When Alice sends messages to Bob, both eavesdroppers can intercept the information. Let the instantaneous SNR of Bob be U. In this system, the PDF and CDF of Bob are the same as given in (1) and (3), respectively. On the other hand, for eavesdroppers 1 and 2, denote their instantaneous SNRs as W_1 and W_2, respectively. The effect of two eavesdroppers can be characterized by the random variable: $W = \max(W_1, W_2)$. Then the CDF of W is:

$$F_W(w) = \Pr(W_1 \le w)\Pr(W_2 \le w) = F_{W_1}(w)F_{W_2}(w)$$
$$= 1 - 2\exp\left(-\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{b/2}\right)$$
$$+\exp\left(-2\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{b/2}\right), \qquad (24)$$

where W_1 and W_2 are supposed to be independent and identically distributed (i.i.d.). The corresponding PDF is:

$$f_W(w) = b\left[\frac{2}{bw_0}\Gamma\left(\frac{2}{b}\right)\right]^{\frac{b}{2}}\left[1-\exp\left(-\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{b/2}\right)\right] \times \exp\left(-\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{b/2}\right)w^{(b/2)-1}. \quad (25)$$

Let $a = b$. Substituting (1) and (25) into (12), we derive:

$$f_Z(z) = (rz)^{a/2}\left(\frac{a}{z}\right)\left[\frac{1}{(z^{a/2}+r^{a/2})^2}-\frac{1}{(z^{a/2}+2r^{a/2})^2}\right]. \quad (26)$$

Then, substituting (26) into (11), we obtain:

$$E(C_s) = \frac{ar^{a/2}}{\ln 2}\int_1^\infty \frac{z^{(a/2)-1}\ln z}{(z^{a/2}+r^{a/2})^2}dz - \frac{ar^{a/2}}{\ln 2}\int_1^\infty \frac{z^{(a/2)-1}\ln z}{(z^{a/2}+2r^{a/2})^2}dz = \frac{r^{a/2}}{\ln 2}(I_1 - I_2), \quad (27)$$

where

$$I_1 = a\int_1^\infty \frac{z^{(a/2)-1}\ln z}{(z^{a/2}+r^{a/2})^2}dz, \quad (28)$$

$$I_2 = a\int_1^\infty \frac{z^{(a/2)-1}\ln z}{(z^{a/2}+2r^{a/2})^2}dz. \quad (29)$$

Following the rule of integration by parts, we have:

$$I_1 = \frac{2\ln z}{z^{a/2}+r^{a/2}}\Big|_\infty^1 - 2\int_\infty^1 \frac{1}{z(z^{a/2}+r^{a/2})}dz = \frac{2}{r^{a/2}}\int_1^\infty \frac{1}{z[1+(z/r)^{a/2}]}dz. \quad (30)$$

Note that the integral on the right-hand side of (30) is the same as that in (21). Therefore, according to (22),

$$I_1 = \frac{4}{ar^{a/2}}\ln\left(1+r^{a/2}\right) \quad (31)$$

Moreover, due to the resemblance between (28) and (29), we have:

$$I_2 = \frac{2}{ar^{a/2}}\ln\left(1+2r^{a/2}\right) \quad (32)$$

Finally, substituting (31) and (32) into (27), we obtain:

$$E(C_s) = \frac{4}{a}\log_2\left(\frac{1+r^{a/2}}{\sqrt{1+2r^{a/2}}}\right). \quad (33)$$

V. REMARKS

Several important insights can be gained. First, the ASC is favored by increasing r, the ratio of $E(U)$ to $E(W)$. Secondly, the ASC is favored with the descending values of a, the common fading factor of both main and eavesdropper channels. Thirdly, the presence of a second eavesdropper makes a significant impact on ASC. Finally, we remark that the approach presented in the preceding section can be extended to the system encountered N $(N>2)$ eavesdroppers. In this general situation, eq. (24) becomes the following expression:

$$F_W(w) = \prod_{k=1}^N \Pr(W_k \le w) = \prod_{k=1}^N F_{W_k}(w) = \left\{1-\exp\left(-\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{b/2}\right)\right\}^N. \quad (34)$$

By the binomial theorem, we have:

$$F_W(w) = \sum_{k=0}^N \binom{N}{k}(-1)^k \exp\left(-k\left[\frac{w}{w_0}\Gamma\left(1+\frac{2}{b}\right)\right]^{b/2}\right). \quad (35)$$

Accordingly, the PDF takes the following form:

$$f_W(w) = \left[\frac{\Gamma(2/b)}{w_0}\right]^{b/2}\left(\frac{2}{b}\right)^{(b/2)-1} \times \sum_{k=0}^N \binom{N}{k}k(-1)^{k+1}\exp\left(-k\left[\frac{2w\Gamma(2/b)}{bw_0}\right]^{b/2}\right)w^{(b/2)-1}. \quad (36)$$

Note that eq. (18) is incorporated in the derivation of (36). Substituting (1) and (36) into (12), we can conduct an analysis similar to that for the case of two eavesdroppers. The details are omitted here due to the space limit.

VI. CONCLUSION

The Weibull distribution characterizes the fading induced by multipath propagations occurred in the mobile radio systems. In the fields of information-theoretic secrecy (ITS), the average secrecy capacity (ASC) is an important benchmark. In the regime of high SNR, we derive a general formula. Then it is refined to the closed-form expressions for several special cases.

REFERENCES

[1] M. Bloch, J. Barros, M.R.D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security", *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, 2008.

[2] X. Liu, "Probability of strictly positive secrecy capacity of the Rician-Rician fading channel", *IEEE Wireless Communications Letters,* vol. 2, no. 1, pp. 50-53, 2013.

[3] X. Liu, "Probability of strictly positive secrecy capacity of the Weibull fading channel", *Proc. of IEEE Globecom 2013.*

[4] C. E. Shannon, "Communication theory of secrecy systems", *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, 1949.

[5] A. D. Wyner, "The wire-tap channel", *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1387, 1975.

[6] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel", *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451-456, 1978.

[7] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels,* Hoboken, NJ: Wiley-Interscience, 2005.