A Closed-Form Expression for Outage Secrecy Capacity in Wireless Information-Theoretic Security

Theofilos Chrysikos, Tasos Dagiuklas, and Stavros Kotsopoulos

Wireless Telecommunications Laboratory
Department of Electrical & Computer Engineering
University of Patras – 26500 Greece
{txrysiko,ntan,kotsop}@ece.upatras.gr

Abstract. This paper provides a closed-form expression for Outage Secrecy Capacity in Wireless Information-Theoretic Security. This is accomplished on the basis of an approximation of the exponential function via a first-order Taylor series. The error of this method is calculated for two different channel cases, and the resulting precision confirms the correctness of this approach. Thus, the Outage Secrecy Capacity can be calculated for a given Outage Probability and for a given propagation environment (path loss exponent, average main channel SNR), allowing us to estimate with increased precision the boundaries of secure communications.

Keywords: Wireless Information-Theoretic Security; quasi-static Rayleigh fading; Outage Secrecy Capacity; Taylor approximation; path loss exponent.

1 Introduction

Security remains an issue of utmost importance in wireless communications. For all the advances and breakthrough progress in both industry and academia, security still provides a fertile ground for extensive research and innovative solutions. It is imperative to begin with a brief overview of background work in the field of wireless security from an information-theoretic standpoint.

1.1 Background Work

Based on Shannon's definition of *perfect secrecy* [1], innovative research was carried out in the latter half of the 1970s, investigating the impact of the wireless channel on the boundaries of secure communications [2]-[4]. Both the main and the wiretap channel were considered to be Gaussian. This proved to be the first major setback in the ongoing research, due to the limitation that the average SNR of the main (legitimate) channel had to be greater than the average SNR of the wiretap channel (eavesdropper's channel) so that secure communication over the wireless interface would be guaranteed. To make matters worse, the lack of channel coding schemes at the time prevented researchers from coming up with a flexible and reliable solution to the situation at hand. Information-theoretic solutions for wireless security were seemingly brought to a quick ending, and the interest of public research was drawn towards

Q. Gu, W. Zang, and M. Yu (Eds.): SEWCN 2009, LNICST 42, pp. 3–12, 2010.

higher layer, more sophisticated schemes that paved the way for the transition from "weak" to "strong" secrecy, incorporating cryptography schemes [5]-[8].

Recent work, however, has re-approached the issue of physical layer-based security for wireless communication under a new light by developing the concept of Wireless Information-Theoretic Security.

1.2 Wireless Information-Theoretic Security

In [9],[10] Bloch, Barros, Rodrigues and McLaughlin suggest that the wireless communication between a transmitter and a (legitimate) receiver in the presence of a malicious user (eavesdropper) can be secure even when the SNR of the main channel is lower than the SNR of the eavesdropper. This is possible when quasi-static Rayleigh fading channels are considered, instead of the classic Gaussian scenario.

The outage probability for a given Secrecy Rate $R_s > 0$ (defined as the probability that the Secrecy Capacity will be smaller than a non-zero secrecy rate) is calculated as an expression of the average main and wiretap channel SNR, $\overline{\gamma}_M$ and $\overline{\gamma}_W$ respectively:

$$P_{out}\left(C_s < R_s\right) = P_{out}(R_s) = 1 - \frac{\overline{\gamma}_M}{\overline{\gamma}_M + 2^{R_s}\,\overline{\gamma}_W} e^{\left(-\frac{2^{R_s}-1}{\overline{\gamma}_M}\right)} \qquad (1)$$

The practical implementation of this information-theoretic scheme can be achieved via the use of LDPC channel coding as shown in [11],[12].

1.3 Impact of the Propagation Environment

In [9],[10] the intrinsic characteristics of the propagation environment were examined by assigning a value of n=3 to the path loss exponent [13]. Thus the Outage Probability is calculated by:

$$P_{out}\left(C_s < R_s\right) = P_{out}\left(R_s\right) = 1 - \frac{e^{\left(-\frac{2^{R_s}-1}{\overline{\gamma}_M}\right)}}{1 + 2^{R_s}\left(\frac{d_M}{d_W}\right)^n} \qquad (2)$$

This however does not correspond to realistic cases where the path loss exponent can assume a wide range of values [14], from n=1.8 (indoor LOS cases) up to n=3.8 and even n=4 (indoor complex NLOS topology, outdoor urban shadowed dense area). In [15], the impact of this channel-dependent variation of path loss exponent on the non-zero probability of Secrecy Capacity and the Outage Probability was examined.

In all published works so far, however, another important parameter, the Outage Secrecy Capacity, has not been properly and thoroughly investigated.

2 Outage Secrecy Capacity

Outage Secrecy Capacity is defined as the maximum secrecy rate $R_s\{\max\} = C_{out}$ such that the Outage Probability is less than a certain value, i.e. *p*:

$$P_{out}\left(C_{out}(p)\right) = p \tag{3}$$

2.1 The Need for a Closed-Form Expression

A closed-form expression for Outage Secrecy Capacity will provide us with knowledge of the largest secrecy rate for a given Outage Probability, intrinsic channel characteristics (path loss exponent) and average main channel SNR, namely the exact value of the secrecy rate that will serve as a threshold for Secrecy Capacity.

2.2 Closed-Form Expression via Taylor Approximation

The approximation of the exponential function via a first-order Taylor series in its generalized expression is provided by [16]:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \ldots \tag{4}$$

In our case, the approximation via a first-order Taylor series is achieved as such:

$$e^{\left(-\frac{2^{R_s}-1}{\overline{\gamma}_M}\right)} \approx 1 - \left(\frac{2^{R_s}-1}{\overline{\gamma}_M}\right) \tag{5}$$

Thus, the Outage Probability is provided by:

$$P_{out}\left(R_s\right) = 1 - \frac{1-\left(\dfrac{2^{R_s}-1}{\overline{\gamma}_M}\right)}{1+2^{R_s}\left(\dfrac{d_M}{d_W}\right)^n} \tag{6}$$

The closed-form expression for Outage Secrecy Capacity for a given Outage Probability *p* is given by:

$$C_{out}(p) = \log_2\left(\frac{\overline{\gamma}_M p + 1}{\overline{\gamma}_W\left(1-p\right)+1}\right) \tag{7}$$

$$C_{out}(p) = \log_2\left(\frac{p+\frac{1}{\overline{\gamma}_M}}{\left(\frac{d_M}{d_W}\right)^n(1-p)+\frac{1}{\overline{\gamma}_M}}\right) \tag{8}$$

Naturally, a certain error lies within this approach. Even though the parameters in Eq. 5 are such (target Secrecy Rate, average main channel SNR) that their value range allows for the approximation to take place, it is imperative to evaluate the precise error for realistic values of these parameters, that is for realistic schemes that we will be compelled to resolve in actual scenarios of information-theoretic security. In the following section, the exact calculation of this error for two different channel cases is accomplished and the findings, based on computation of Outage Probability, are discussed.

3 Error Calculation Based on Outage Probability

Two channel cases will be examined, corresponding to two very frequently met scenarios in wireless communications: (a) The pass loss exponent is assigned a value of n=2. This corresponds to the Free Space Model and describes a "good" channel case where the attenuation of the average signal strength follows the inverse-square law [17], and (b) the pass loss exponent is assigned a value of n=3.8 that stands for a "bad" channel case with heavy attenuation of the average signal strength. This corresponds to urban shadowed outdoor propagation or obstructed indoor propagation (corridors, complex topologies).

The average main channel SNR is assigned a value of 10 dB for the first case. For the n=3.8 case, the average main channel SNR is set to 0 dB.

3.1 Error Calculation for "Good" Channel Case

The following tables provide an analytical presentation of the error of our approximation for different distance ratios and for various realistic values of the target Secrecy Rate. It is interesting to note that for values of the Secrecy Rate above 3.5 bits per second, the Taylor approximation gives an Outage Probability of 1, whereas the original formula gives also very high values of Outage Probability. It is therefore a common assumption, despite some minor error deviation present (especially for the distance ratio scheme of dw=5dm) that for the given channel characteristics the Secrecy Rate should not exceed 3.5 bits per second otherwise the communication is compromised in terms of information-theoretic security.

The error is quite small for realistic values of the Secrecy Rate. For Rs< 1 bit/s, the mean error is below 1%. The curves confirm the correctness of our approach, while demonstrating that the Taylor approximation is more linear and faster than the original formula containing the exponential function.

Table 1. Comparative Calculation of Outage Probability for n=2 and avg. SNR=10 dB

Rs	dw = 5 dm		dw = 2 dm		dm = dw		dm = 2 dw	
	Exp.	Taylor	Exp.	Taylor	Exp.	Taylor	Exp.	Taylor
0,01	0,039	0,039	0,202	0,202	0,502	0,502	0,801	0,801
0,5	0,092	0,093	0,291	0,292	0,603	0,603	0,856	0,856
1	0,162	0,167	0,397	0,4	0,698	0,7	0,9	0,9
1,5	0,252	0,266	0,512	0,521	0,782	0,787	0,932	0,934
2	0,361	0,397	0,630	0,65	0,852	0,86	0,956	0,956
2,5	0,488	0,564	0,74	0,779	0,906	0,92	0,973	0,977
3	0,624	0,773	0,835	0,9	0,945	0,967	0,985	0,991
3,5	0,755	1	0,906	1	0,971	1	0,992	1
4	0,864	1	0,955	1	0,987	1	0,997	1
4,5	0,940	1	0,983	1	0,995	1	0,999	1
5	0,980	1	0,995	1	0,998	1	0,999	1

Table 2. Mean Error (%) for the Taylor Approximation for n=2 and avg. SNR=10 dB

Rs (bits/s)	dw=5dm	dw=2dm	dm=dw	dm=2dw
0< Rs ≤ 5	10,47	3,31	0,96	0,25
0< Rs ≤ 3	8,35	2,73	0,81	0,21
0< Rs ≤ 1	1,21	0,34	0,10	0,02

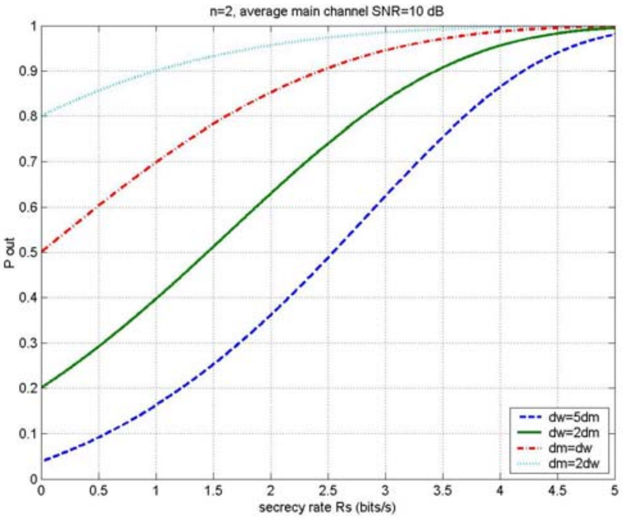

Fig. 1. Outage Probability versus Secrecy Rate for n=2 and avg. SNR=10 dB

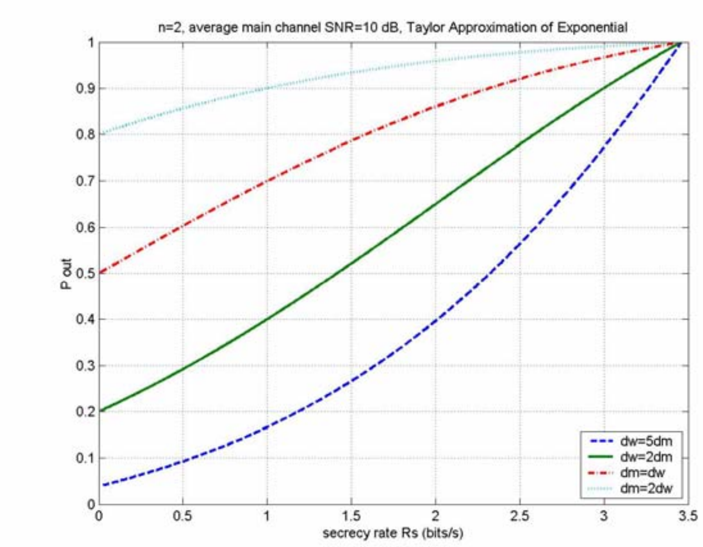

Fig. 2. Outage Probability versus Secrecy Rate for n=2 and avg. SNR=10 dB (Taylor approx.)

3.2 Error Calculation for "Bad" Channel Case

Table 3. Comparative Calculation of Outage Probability for n=3.8 and avg. SNR=0 dB

Rs	dw = 5 dm		dw = 2 dm		dm = dw		dm = 2 dw	
	Exp.	Taylor	Exp.	Taylor	Exp.	Taylor	Exp.	Taylor
0,01	0,009	0,009	0,074	0,074	0,505	0,505	0,934	0,934
0,5	0,341	0,416	0,400	0,468	0,726	0,757	0,968	0,972
1	0,634	1	0,678	1	0,877	1	0,987	1
1,5	0,840	1	0,867	1	0,958	1	0,996	1
2	0,951	1	0,961	1	0,99	1	0,999	1
2,5	0991	1	0,993	1	0,998	1	0,999	1

Table 4. Mean Error (%) for the Taylor Approximation for n=3.8 and avg. SNR=0 dB

Rs (bits/s)	dw=5dm	dw=2dm	dm=dw	dm=2dw
0< Rs ≤ 3	13,12	7,69	2,16	0,20
0< Rs ≤ 0,5	10,96	8,51	2,14	0,19
Rs=0.01	0	0	0	0

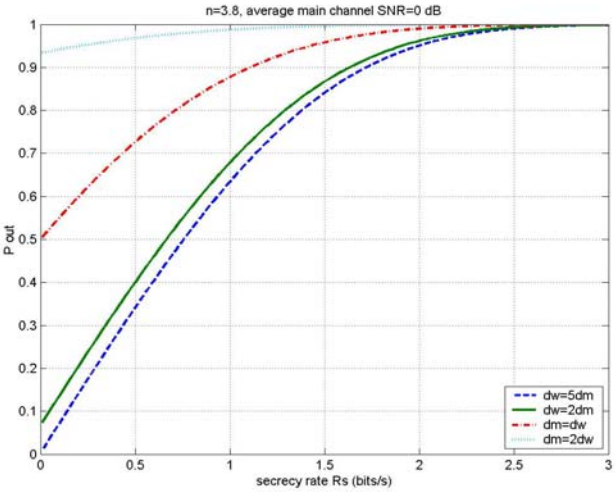

Fig. 3. Outage Probability versus Secrecy Rate for n=3.8 and avg. SNR=0 dB

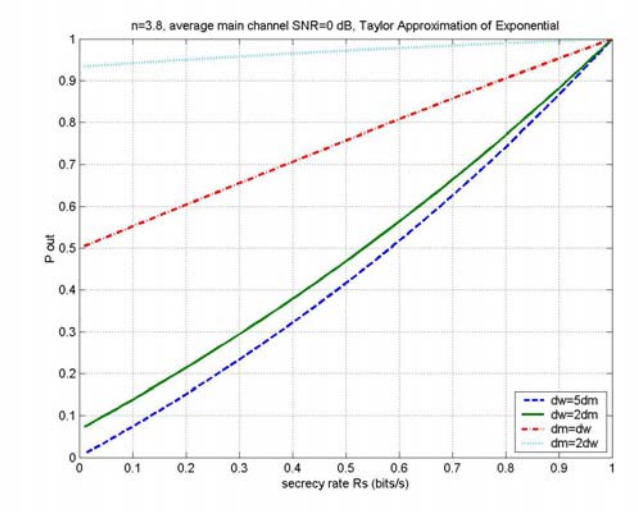

Fig. 4. Outage Probability versus Secrecy Rate for n=3.8 and avg. SNR=0 dB (Taylor approx.)

4 Behavior of the Closed-Form Expression

We shall examine, for the two aforementioned channel cases, the behavior of the Outage Secrecy Capacity that determines the threshold of secure communications for the information-theoretic scheme:

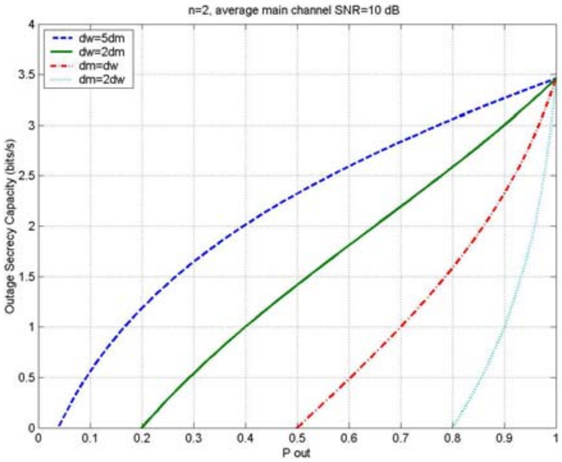

Fig. 5. Outage Secrecy Capacity for n=2, avg. SNR=10 dB and various distance ratio schemes

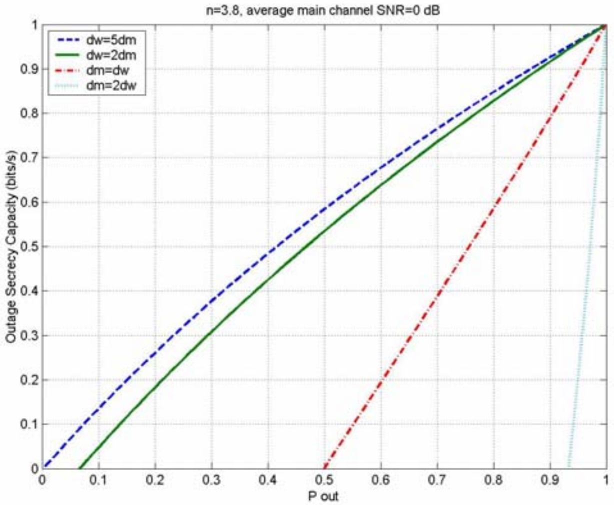

Fig. 6. Outage Secrecy Capacity for n=3.8, avg. SNR=0 dB and various distance ratio schemes

It can be observed that for n=2 and a main channel SNR=10 dB, the largest possible Secrecy Rate is smaller than 3.5 bits per second, whereas for an acceptable value of Outage Probability the largest Secrecy Rate should not exceed 1.5 bits per second. Of course the actual optimal value of the largest Secrecy Rate, namely the Outage Secrecy Capacity, depends on the specific value of the distance ratio as well, thus demonstrating the importance of the users' location.

For n=3.8 and SNR=0 dB (main channel), the largest possible Secrecy Rate is well below 1 bit per second, whereas for an acceptable value of Outage Probability, the Secrecy Rate should not exceed 0.5 bits per second, again depending on the actual user location in the topology in question.

5 Conclusions

A closed-form expression for Outage Secrecy Capacity was provided in this work, based on an approximation of the exponential function in the original formula of Outage Probability via Taylor series (first-order). The mean error was calculated for certain regions of the Secrecy Rate and the precision was evaluated as satisfactory for realistic scenarios. Therefore the closed-form expression and the subsequent curves are able to predict the behavior of the Outage Secrecy Capacity in reliable and practical manner.

The above curves provide an essentially significant standpoint for the precise estimation of the required threshold for a given Outage Probability when the propagation characteristics of the topology at hand and the location of the users therein play an important role in the reliability of information-theoretic security schemes.

Acknowledgments. The authors wish to acknowledge the support of the ICT European Research Programme and all the partners in PEACE: PDMF&C, Instituto de Telecomunicaes, FhG Fokus, University of Patras, Thales, Telefonica, CeBit.

References

1. Shannon, C.E.: Communication theory of secrecy systems. Bell Tech. J. 29, 656–715 (1949)
2. Wyner, A.D.: The wire-tap channel. Bell Tech. J. 54, 1355–1387 (1975)
3. Csiszar, I., Korner, J.: Broadcast channels with confidential messages. IEEE Trans. Inf. Th. 24(3), 339–348 (1978)
4. Leung-Yan-Cheong, S.K., Hellman, M.E.: The Gaussian wiretap channel. IEEE Trans. Inf. Th. 24(4), 451–456 (1978)
5. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE Trans. Inf. Th. 39(3), 733–742 (1993)
6. Maurer, U.M.: Information-theoretically secure secret-key agreement by NOT authenticated public discussion. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 209–225. Springer, Heidelberg (1997)
7. Maurer, U.M., Wolf, S.: Information-theoretic key agreement: from weak to strong secrecy for free. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 351–368. Springer, Heidelberg (2000)
8. Maurer, U.M., Wolf, S.: Secret-key agreement over unauthenticated public channels Part I: Definitions and a completeness result. IEEE Trans. Inf. Th. 49(4), 822–831 (2003)
9. Barros, J., Rodrigues, M.R.D.: Secrecy capacity of wireless channels. In: 2006 IEEE International Symposium on Information Theory, pp. 356–360. IEEE Press, New York (2006)
10. Bloch, M., Barros, J., Rodrigues, M.R.D., McLaughlin, S.W.: Wireless Information-Theoretic Security. IEEE Trans. Inf. Th. 54(6), 2515–2534 (2008)
11. Bloch, M., Thangaraj, A., McLaughlin, S.W., Merolla, J.M.: LDPC-based Gaussian key reconciliation. In: 2006 IEEE Information Theory Workshop, pp. 116–120. IEEE Press, New York (2006)
12. Richardson, T.J., Shokrollahi, M.A., Urbanke, R.L.: Design of capacity-approaching irregular low-density parity-check codes. IEEE Trans. Inf. Th. 47(2), 619–637 (2001)

13. Rappaport, T.: Wireless Communications: Principles and Practice. Prentice Hall, Upper Saddle River (2001)
14. Seybold, J.: Introduction to RF Propagation. Wiley Interscience, Hoboken (2005)
15. Chrysikos, T., Kotsopoulos, S.: Impact of channel-dependent variation of path loss exponent on Wireless Information-Theoretic Security. In: Wireless Telecommunications Symposium 2009, April 22-24, pp. 1–7. IEEE Press, New York (2009)
16. Abramowitz, M., Stegun, I.: Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. Dover Publications, New York (1970)
17. Kotsopoulos, S., Karagiannidis, G.: Mobile Communication. Papasotiriou SA Publication, Athens (1997)