Accepted in IEEE Int. Workshop on Selected Topics in Wireless and Mobile Computing (STWiMob), 2015

Performance Analysis of Physical Layer Security of Chaos-based Modulation Schemes

Long Kong, Georges Kaddoum
Department of Electrical Engineering, LaCIME Laboratory
University of Quebec, ETS
Montreal, Canada
Email: long.kong.1@ens.etsmtl.ca, georges.kaddoum@etsmtl.ca

Mostafa Taha
Department of Electrical Engineering
Assiut University
Assiut, Egypt
Email: mtaha@aun.edu.eg

***Abstract*—Chaos-shift-keying (CSK) and differential CSK (DCSK) are the two popular coherent and non-coherent modulation schemes for ultra wide-band (UWB) communications. However, security of these schemes has never been studied formally from the information-theoretic perspective. In this paper, we investigate the physical layer security of CSK and DCSK modulation schemes over AWGN and Rayleigh fading channels from the information-theoretic manner. For this aim, the average secrecy capacity and outage probability are computed and analyzed by considering the variation of bit energy E_b coming from the use of chaotic signal to convey information. Our results show that CSK has better or close secrecy capacity and outage probability compared with DCSK and the conventional spread-spectrum modulation. Additionally, these metrics favor Rayleigh fading channels over AWGN channels. Finally, we conclude that the non-constant bit energy is useful to enhance the physical layer security.**

***Index Terms*—CSK, DCSK, Secrecy capacity, Outage probability, Bit energy.**

I. Introduction

Information security became an increasingly challenging issue since the widespread deployment of wireless communication in our daily life, such as e-banking, e-commerce and medical information exchange [1]. Due to the open access of the wireless transmission medium, physical layer security suffers vulnerability from both active and passive attackers. Many countermeasures are proposed in order to ensure secure information transmission. The conventional attempt is to combine authentication and encryption at the upper layers of the protocol stack. This solution is practical and mostly successful, however, it adds computational complexity to the whole communication system. Different from the cryptography approach, information-theoretic security operates directly at the physical layer by taking advantage of the characteristics of wireless channels, such as noise, interference, path-loss and fading via signaling and channel coding [2]. The first work to information-theoretic security was firstly proposed and proved by Shannon in 1949 [3], where the wiretap channel is described. Afterwards, Wyner introduced a more general noisy wiretap channel and uncovered the fact that information-theoretic secure communication can be achieved without using any secret keys, by keeping the eavesdropper ignorant of the secure message [4]. Since then, plenty of attentions both from academia and industry was attracted to study secrecy performance from information-theoretic perspective. In [5], the secrecy capacity over additive white Gaussian noise (AWGN) channel was given and proved. The average secrecy capacity and closed-form expressions of outage probability for physical layer security over Rayleigh and Nakagami fading channels [2, 6]. Also, the authors of [7, 8] presented the physical layer secrecy of single-input single-output (SISO) system over AWGN/Rayleigh channels, Rayleigh/Rician and Rician/Rician fading channels, respectively, where the main channel and wiretap channel hold different fading assumptions.

On the other hand, there exist plenty of research focusing on digital communication systems using chaos-based signal as carrier due to their advantageous wideband characteristics [9–11]. Dating back to the application of chaos in wireless communication systems, one can easily find that chaos-based modulation schemes are suitable for spread-spectrum (SS) systems [9]. Chaotic modulations have similar advantages to all other spread-spectrum modulations, including the mitigation of fading channels and jamming resistance. Furthermore, the low probability of interception (LPI) [12] and excellent correlation properties [13] allow them to be one of the natural candidates for military communication scenarios. Among numerous chaos-based communication schemes, CSK and DCSK are widely studied from theory to implementation [9]. In [14], it was proved that CSK can provide a secure communication link while requiring chaotic synchronization. Fortunately, DCSK system can perform well without relying on the reproduction of the transmitted chaotic signal at the receiver and also shows strong resistance against multipath fading [15]. Although some security properties of CSK and DCSK were proposed in [14] and [15, 16], security of these schemes were never studied formally from the information-theoretic perspective, where comes our contribution.

In this paper, we propose a novel insight in the physical layer security of chaos-based modulation schemes. We derive and analyze the secrecy capacity and outage probability, with respect to the bit energy, for CSK and DCSK modulation schemes over AWGN and Rayleigh channels. The analytical results are solved with numerical approach as the probability density function (PDF) of bit energy follows a non-standard function. In addition, these secrecy metrics are compared to the conventional SS system. Our results show that CSK performs

better or close to the conventional and DCSK modulation schemes in terms of secrecy capacity and outage probability. To the best knowledge of the authors, there is no previous work that studied the physical layer security while considering chaos-based modulations from the information-theoretic perspective.

The remaining of this paper is organized as follows. Section II covers some preliminary work including the chaotic sequence generator and the chaos-based modulation schemes: CSK and DCSK. Section III proposes our derivation and analysis of the two performance metrics of physical layer security, namely the average secrecy capacity and the outage probability. Section IV gives numerical results. The conclusion is given in section V.

II. Chaos-based modulations

In this section, we will briefly describe the CSK and DCSK modulation schemes.

A. Chaotic generators

In this paper, we use a second-order Chebyshev polynomial function (CPF) which is given by

$$c_{k+1} = 1 - 2c_k^2. \tag{1}$$

We selected this chaotic map for having good performance while being simple to realize. The chaotic sequences c_k are normalized, which means that $E(x_k) = 0$ and $E(x_k^2) = 1$, where $E(\bullet)$ is the expectation operator. The number of chaotic samples sent for each bit is defined by the spreading factor β.

The transmitted bit energy is defined as

$$E_b = T_c \sum_{k=1}^{\beta} c_k^2, \tag{2}$$

where T_c is the time chip. Fig. 1 shows the histogram of the bit energy after spreading by the CPF map with $\beta = 20$. This histogram was obtained using ten million chaotic samples. From these samples, energies of successive bits are calculated for the given spreading factor. Note that, if β is very low, due to the non-periodic nature of chaotic signals, the transmitted bit energy after spreading by chaotic sequences will vary from one bit to another and thus E_b cannot be assumed constant. However if β is high, E_b can be considered constant [15].

B. CSK communication system

A general CSK communication system is shown in Fig. 2. The data symbols ($b_l \in \{+1, -1\}$) with period T_s are spread by a chaotic sequence c_k with period T_c. Here, the spreading factor equals T_s/T_c. For the lth bit, the modulated waveforms $x_{l,C}(t)$ at the output of the transmitter is given by

$$x_{l,C}(t) = \sum_{k=1}^{\beta} b_l c_{l\beta+k} g\left(t - (l\beta + k) T_c\right), \tag{3}$$

where $g(t)$ is the pulse shaping filter. A rectangular pulse of unit amplitude on $[0, T_c]$ is used.

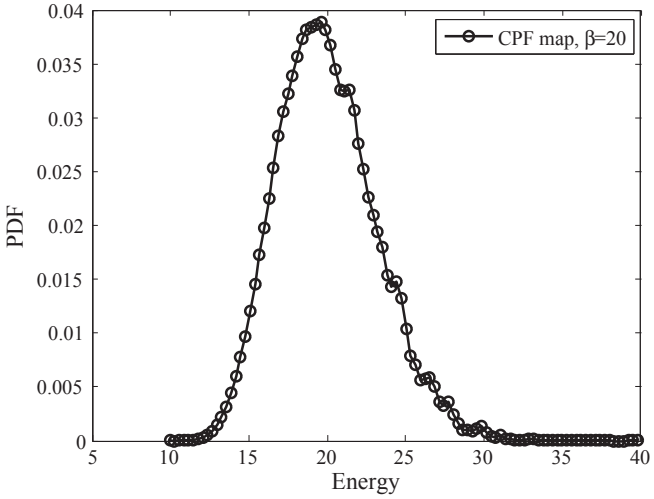

Fig. 1. Simulated distribution of bit energy for $\beta = 20$

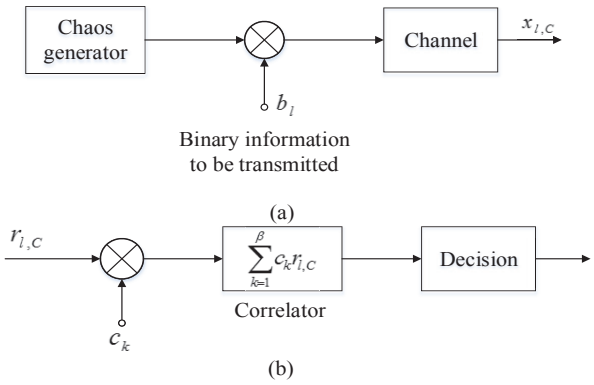

Fig. 2. Block diagram of CSK communication system. (a) Transmitter, (b) Receiver

In order to demodulate the transmitted bits, the received signal $r_{l,C}$ is first multiplied by the local synchronized chaotic sequence c_k, and then integrated over a symbol duration T_s. Finally, the transmitted bits are estimated by computing the sign of the decision variable at the output of the correlator.

C. DCSK communication system

Fig. 3 shows the block diagram of DCSK communication system. In this scheme, every transmitted bit is represented by two consecutive chaotic signal samples. The first part serves as the reference sample while the second one carries the data (data sample). With respect to different information bits b_l to be transmitted, the data sample carries the same or inverted versions of the reference sample. Here, the symbol duration and the bit energy are doubled,

$$T_s = 2\beta T_c, E_{b,D} = 2T_c \sum_{k=1}^{\beta} c_k^2.$$

Fig. 3 (a) shows a DCSK transmitter, while Fig. 3 (b) shows a sample frame.

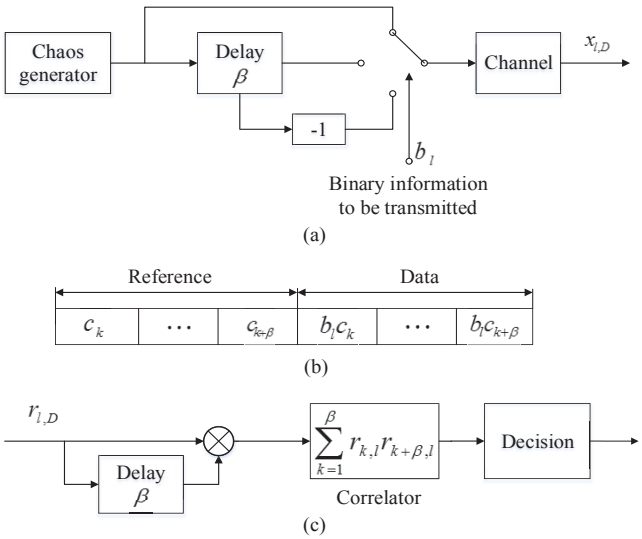

Fig. 3. Block diagram of DCSK communication system. (a) The DCSK transmitter. (b) The DCSK frame. (c) The DCSK receiver.

For the lth symbol,we have

$$x_{l,D}(t) = \begin{cases} \sum_{k=1}^{\beta} c_{l\beta+k} g\left(t-(l\beta+k)T_c\right), \\ \sum_{k=\beta}^{2\beta} b_l c_{l\beta+k} g\left(t-(l\beta+k)T_c\right). \end{cases} \tag{4}$$

Fig. 3. (c) shows the DCSK non-coherent demodulator. The received signal is correlated to its delayed version, then summed over the bit duration T_s. Finally, the received bits are estimated by computing the sign of the correlator output. If it is greater than '0', '1' is detected, otherwise, '-1' is detected.

III. System Model

A three-node classic model shown in Fig. 4, is used in this paper to illustrate a wireless network with potential eavesdropper. Herein, a legitimate transmitter (Alice) wishes to send the secret messages to an intended receiver (Bob) in the presence of an eavesdropper (Eve). The communication channel between Alice and Bob is called the main channel, while the one between Alice and Eve is named as wiretap channel. The secrecy performance is evaluated with consideration of two cases: (i) real-valued AWGN channel; (ii) flat quasi-static Rayleigh fading channel characterized by the fading coefficients h_m and h_w, respectively. Herein, $G_m = |h_m|^2$ and $G_w = |h_w|^2$ are called fading gain.

The relationship between Alice and Bob in the presence of the Eve can be described as follows

$$r_{Bob}(t) = h_m x(t) + n_m(t), \tag{5}$$

$$r_{Eve}(t) = h_w x(t) + n_w(t), \tag{6}$$

where $r_{Bob}(t)$ and $r_{Eve}(t)$ are the received signal at Bob's and Eve's receiver, respectively. $x(t)$ is the CSK or DCSK modulated transmitted signal by Alice, following equations (3) and (4). $n_m(t)$ and $n_w(t)$ are the zero-mean complex additive white Gaussian noise, respectively.

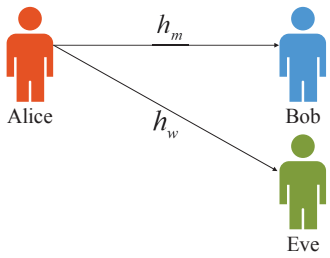

Fig. 4. Wireless wiretap system model

Therefore, the instantaneous signal-to-noise ratio (SNRs) over Rayleigh fading channels for CSK ($\gamma_{m,C}$) and DCSK ($\gamma_{m,D}$) modulations at Bob's receiver side are

$$\gamma_{m,C} = \frac{E_{b,C}|h_m|^2}{N_{m,C}}, \gamma_{m,D} = \frac{E_{b,D}|h_m|^2}{N_{m,D}}.$$

While the average SNRs at Bob's receiver side are

$$\overline{\gamma}_{m,C} = \frac{E_{b,C}E(|h_m|^2)}{N_{m,C}}, \overline{\gamma}_{m,D} = \frac{E_{b,D}E(|h_m|^2)}{N_{m,D}}.$$

Similarly, the received instantaneous SNRs at Eve for CSK ($\gamma_{w,C}$) and DCSK ($\gamma_{w,D}$) modulations are

$$\gamma_{w,C} = \frac{E_{b,C}|h_w|^2}{N_{w,C}}, \gamma_{w,D} = \frac{E_{b,D}|h_w|^2}{N_{w,D}}.$$

The received average SNRs at Eve are

$$\overline{\gamma}_{w,C} = \frac{E_{b,C}E(|h_w|^2)}{N_{w,C}}, \overline{\gamma}_{w,D} = \frac{E_{b,D}E(|h_w|^2)}{N_{w,D}},$$

where $N_{m,C}$ and $N_{m,D}$ are the noise power of the main channel for CSK and DCSK modulations. Similarly, $N_{w,C}$ and $N_{w,D}$ are the noise power of the wiretap channel for CSK and DCSK modulations.

In the following two subsections, the average secrecy capacity and outage probability for CSK and DCSK modulation schemes over AWGN channel and Rayleigh fading channel are derived.

A. Average Secrecy Capacity

The secrecy capacity is defined similarly to the standard capacity, which is the maximum achievable secrecy rate, given as follows [2]

$$C_s = C_m - C_w, \tag{7}$$

where C_m and C_w are the capacity of main channel and wiretap channel, respectively.

First, we start by recalling the channel capacity of AWGN channel (C_A) and Rayleigh fading channel (C_R) with consideration of date rate given by [17]

$$C_A = \frac{1}{2}\log_2\left(1+\frac{RE_b}{N_0}\right), \tag{8}$$

$$C_R = \log_2\left(1+\frac{RE_b|h|^2}{N_0}\right), \tag{9}$$

where R is the transmission rate of the system in bps, N_0 is the one-sided noise power spectral density, h is the Rayleigh fading coefficient.

In the case of real-valued Gaussian noise (AWGN) channel and for constant bit energy E_b, the secrecy capacity of CSK ($C_{s,C,A}$) and DCSK ($C_{s,D,A}$) can be given as follows based on (7) and (8)

$$C_{s,C,A}=\left[\frac{1}{2}\log_2\left(1+\frac{R_C E_{b,C}}{N_{m,C}}\right)-\frac{1}{2}\log_2\left(1+\frac{R_C E_{b,C}}{N_{w,C}}\right)\right]^+, \tag{10}$$

$$C_{s,D,A}=\left[\frac{1}{2}\log_2\left(1+\frac{R_D E_{b,D}}{N_{m,D}}\right)-\frac{1}{2}\log_2\left(1+\frac{R_D E_{b,D}}{N_{w,D}}\right)\right]^+, \tag{11}$$

where $[x]^+ = \max\{0, x\}$, R_C and R_D are the data rate of CSK and DCSK modulations for constant bit energy, respectively. Similarly, the received SNRs at Bob and Eve over AWGN channel of CSK and DCSK modulation schemes can be written as: $\gamma_{m,C,A} = E_{b,C}/N_m$, $\gamma_{w,C,A} = E_{b,C}/N_w$, $\gamma_{m,D,A} = E_{b,D}/N_m$ and $\gamma_{w,D,A} = E_{b,D}/N_w$. Since E_b is assumed constant, in this case, equation (10) is equivalent to the secrecy capacity of conventional coherent SS BPSK system with the same data rate R_C.

As shown in Fig. 1, the bit energy of the CSK and DCSK is varying. Therefore, equations (10) and (11) can be further computed by integrating the secrecy capacity expression over all values of bit energy as following forms

$$\overline{C}_{s,C,A} = \int_0^\infty \frac{1}{2}\log_2\left(\frac{N_{m,C}+R_C E_{b,C}}{N_{w,C}+R_C E_{b,C}}\cdot\frac{N_{w,C}}{N_{m,C}}\right) p\left(E_{b,C}\right) dE_{b,C}, \tag{12}$$

$$\overline{C}_{s,D,A} = \int_0^\infty \frac{1}{2}\log_2\left(\frac{N_{m,D}+R_D E_{b,D}}{N_{w,D}+R_D E_{b,D}}\cdot\frac{N_{w,D}}{N_{m,D}}\right) p\left(E_{b,D}\right) dE_{b,D}, \tag{13}$$

where $\overline{C}_{s,C,A}$ and $\overline{C}_{s,D,A}$ are the average capacity over the bit energy distribution. Since the analytical expression of the PDF of bit energy is difficult to obtain leaving the numerical integration as the solution for the integrals in equations (12) and (13).

In the case of i.i.d Rayleigh fading channel, the instantaneous secrecy capacity for CSK and DCSK modulation schemes based on (7) and (9) can be separately presented by

$$C_{s,C,R} = \left[\log_2\left(\frac{1+R_C\gamma_{m,C}}{1+R_C\gamma_{w,C}}\right)\right]^+, \quad \gamma_{m,C} > \gamma_{w,C}, \tag{14}$$

$$C_{s,D,R} = \left[\log_2\left(\frac{1+R_D\gamma_{m,D}}{1+R_D\gamma_{w,D}}\right)\right]^+, \quad \gamma_{m,D} > \gamma_{w,D}. \tag{15}$$

Obviously, the instantaneous secrecy capacity is the function of the fading coefficients (G_m and G_w) and bit energy. On one hand, if the spreading factor is high enough, the bit energy can be regarded constant, then the instantaneous SNRs at Bob and Eve, namely $\gamma_{m,C}$, $\gamma_{w,C}$, $\gamma_{m,D}$ and $\gamma_{w,D}$ are exponentially distributed, then the average secrecy capacity can be simplified to a closed form [2]. On the other hand, if β is relative low, then the bit energy will be varying. The average secrecy capacity of equations (14) and (15) of CSK ($\overline{C}_{s,C,R}$) and DCSK ($\overline{C}_{s,D,R}$) modulation schemes can be obtained by

$$\overline{C}_{s,C,R} = \int_0^\infty\int_0^\infty C_{s,C}\left(\gamma_{m,C},\gamma_{w,C}\right) p\left(\gamma_{m,C}\right) p\left(\gamma_{w,C}\right) d\gamma_{m,C} d\gamma_{w,C}, \tag{16}$$

$$\overline{C}_{s,D,R} = \int_0^\infty\int_0^\infty C_{s,D}\left(\gamma_{m,D},\gamma_{w,D}\right) p\left(\gamma_{m,D}\right) p\left(\gamma_{w,D}\right) d\gamma_{m,D} d\gamma_{w,D}, \tag{17}$$

where $\gamma_{m,C}$, $\gamma_{w,C}$, $\gamma_{m,D}$ and $\gamma_{w,D}$ are the multiply of bit energy and channel coefficients, respectively. The PDF of bit energy has no analytical expression, hence equations (16) and (17) can only be obtained numerically.

B. Secrecy Outage Probability

The outage probability of the secrecy capacity is defined as the probability that the secrecy capacity C_s falls below the target secrecy rate R_s, i.e.,

$$P_{out}\left(R_s\right) = P\left(C_s \le R_s\right). \tag{18}$$

Regarding the Rayleigh fading scenario for fixed E_b, the outage probability is given by [2]. However, for our case, CSK and DCSK are employed, the outage probability can be achieved by

$$P_{out,C}\left(R_s\right) = P\left(C_{s,C,R} \le R_s\right), \tag{19}$$

$$P_{out,D}\left(R_s\right) = P\left(C_{s,D,R} \le R_s\right), \tag{20}$$

Since the analytical expression for PDF of bit energy is not available, the outage probability are computed numerically.

IV. Numerical Analysis

In this section, we will compare the average secrecy capacity and outage probability for CSK and DCSK modulations over AWGN and Rayleigh fading channels, respectively. It is assumed that Alice, Bob and Eve have perfect knowledge of the instantaneous channel coefficient, that is to say, all the three nodes in the wireless network model have full channel state information (CSI). In our simulations, the spreading factor β is set as 20, obviously the data rate for CSK R_c is double of that for DCSK R_D, $R_C = 2R_D$. In order to simplify the simulation, R_D is normalized to 1, then R_C is 2. $\gamma_{m,C,A}$, $\gamma_{w,C,A}$, $\gamma_{m,D,A}$ and $\gamma_{w,D,A}$ can be simplified as $\gamma_{m,A}$ and $\gamma_{w,A}$. Meanwhile, $\overline{\gamma}_{m,C}$, $\overline{\gamma}_{m,D}$, $\overline{\gamma}_{w,C}$ and $\overline{\gamma}_{w,D}$ are substituted by $\overline{\gamma}_m$ and $\overline{\gamma}_w$ for simplicity. The target secrecy rate R_s is set to be 1 bps.

Fig. 5 and Fig. 6 depict the average secrecy capacity versus $\gamma_{m,A}$ or $\overline{\gamma}_m$ with regard to selected $\gamma_{w,A}$ or $\overline{\gamma}_w$ over AWGN channels (equations (12) and (13)) and Rayleigh fading channels (equations (16) and (17)) with comparison to the conventional SS-BPSK modulation system with same date rate as CSK, respectively. One can observe that the average secrecy capacity for CSK modulation is higher than or equal to that of DCSK modulation. In addition, the average secrecy capacity over Rayleigh fading channel is always higher than

or equal to the secrecy capacity over AWGN channel. Based on the simulation results, CSK has better secrecy capacity compared to the conventional SS system. This outperformance compared to the conventional SS-BSPK returns to the fact that the bit energy in CSK is not constant. Strikingly, the fading property of wireless channels can be utilized to secure communication.

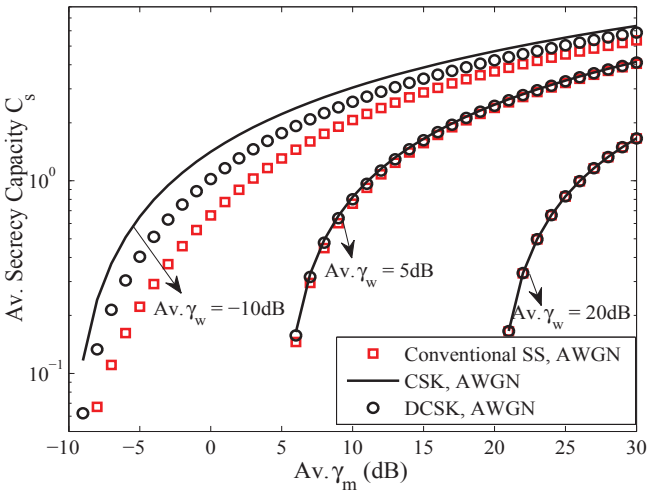

Fig. 5. Average secrecy capacity versus $\gamma_{m,A}$ over AWGN channel.

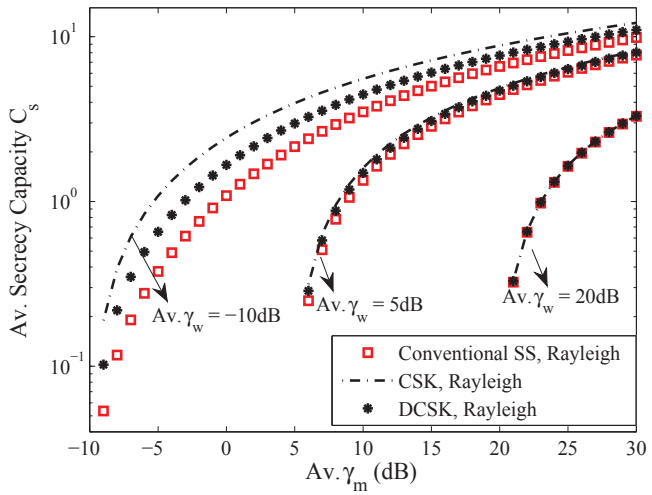

Fig. 6. Average secrecy capacity versus $\overline{\gamma}_m$ over Rayleigh fading channel.

Fig. 7 compares the secrecy outage probabilities versus $\overline{\gamma}_m$ for CSK and DCSK modulations over Rayleigh fading channels for different $\overline{\gamma}_w$, respectively. Surprisingly, the higher $\overline{\gamma}_m$ the lower the outage probability, also the higher $\overline{\gamma}_w$ the higher the outage probability. It is observed that CSK has better or same secrecy outage probability than that of DCSK and conventional SS-BPSK system. Additionally, when the gap between the main channel capacity and wiretap channel capacity is gearing smaller, the difference of outage probability between CSK and DCSK is becoming less slight.

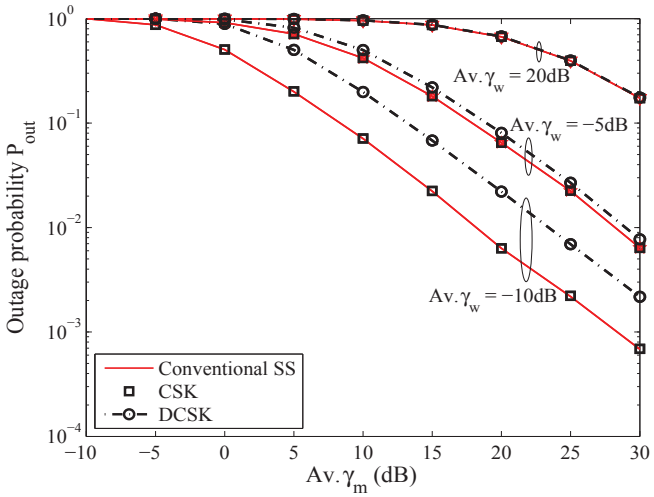

Fig. 7. Outage probability versus $\overline{\gamma}_m$, for selected values of $\overline{\gamma}_w$.

V. Conclusions

In this paper, we studied the physical layer security of chaos-based modulations, namely CSK and DCSK, over AWGN and Rayleigh fading channels. In terms of the evaluation for our case, two critical significant metrics, average secrecy capacity and outage probability are derived and numerically computed by taking account of the variation of bit energy. We conclude that CSK is a better modulation candidate for physical layer security compared with DCSK and the conventional SS-BPSK system. Furthermore, the potential of fading property of physical layer can be well employed to ensure secure communication.

Acknowledgment

This work has been supported by the ETS' research chair of physical layer security in wireless networks. The author would like to thank Prof. Matthieu Bloch for the helpful discussions.

References

[1] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal processing approaches to secure physical layer communications in multi-antenna wireless systems*. Springer-Verlag, 2013.

[2] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[3] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[5] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[6] Z. Rezki and M.-S. Alouini, "On the capacity of Nakagami-m fading channels with full channel state information at low SNR," *IEEE Wireless Commun. Lett.*, vol. 1, no. 3, pp. 253–256, Jun. 2012.

[7] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE Int. Symp. on Information Theory (ISIT)*, Jun. 2007, pp. 1296–1300.

[8] 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, February 2013.

[9] F. C. Lau and C. K. Tse, *Chaos-based digital communication systems*. Springer-Verlag, 2003.

[10] W. K. Xu, L. Wang, and G. Kolumban, "A novel differential chaos shift keying modulation scheme," *International Journal of Bifurcation and Chaos*, vol. 21, no. 03, pp. 799–814, 2011.

[11] G. Kaddoum and F. Shokraneh, "Analog network coding for multi-user multi-carrier differential chaos shift keying communication system," *IEEE Trans. Wireless Commun.*, vol. 14, no. 3, pp. 1492–1505, Mar. 2015.

[12] J. Yu and Y.-D. Yao, "Detection performance of chaotic spreading LPI waveforms," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 390–396, Mar. 2005.

[13] G. Heidari-Bateni and C. McGillem, "Chaotic sequences for spread spectrum: an alternative to PN-sequences," in *Proc. IEEE International Conference on Selected Topics in Wireless Communications*, Jun 1992, pp. 437–440.

[14] Y.-S. Lau, K. Lin, and Z. Hussain, "Space-time encoded secure chaos communications with transmit beamforming," in *IEEE Region 10 TENCON 2005*, Nov. 2005, pp. 1–5.

[15] G. Kaddoum, F. Richardson, and F. Gagnon, "Design and analysis of a multi-carrier differential chaos shift keying communication system," *IEEE Trans. on Commun.*, vol. 61, no. 8, pp. 3281–3291, Aug. 2013.

[16] G. Kaddoum, F. Gagnon, and F. Richardson, "Design of a secure multi-carrier DCSK system," in *Proc. the ninth Intlernational Symposium on Wireless Communication Systems (ISWCS)*, Aug. 2012, pp. 964–968.

[17] W. Ryan and S. Lin, *Channel codes: classical and modern*. Cambridge University Press, 2009.