Performance analysis of synchronization in chaotic DSSS-CDMA system under Jamming attack

A. Tayebi, S.M. Berber, and A. Swain

***Abstract*— This paper investigates the performance of synchronization of the direct sequence spread spectrum (DSSS-CDMA) system under jamming. A result of initial investigation shows that the synchronization in DSSS-CDMA is vulnerable to the jamming attacks. This vulnerability has a tragic effect on the system's error rate. A mathematical expression for of the probability of detection and probability of false alarm has been derived and being used to study the performance of synchronization. . Further, we have computed the amount of jamming power which is required to collapse the synchronization. Performance analysis using Monte Carlo simulation in MATLAB conforms the theoretical results.**

Keywords*— Physical layer security; jamming attacks; synchronization; wireless sensor networks

I. INTRODUCTION

WRELESS sensor networks (WSN) are valuable to the different security attacks [1]. Because WSNs are playing an important role in various applications such as environment monitoring and target detection, it is important to evaluate their performance against security attacks. Amongst various types of security attacks, jamming is one of the simplest and the most dangerous attack [2]. A jammer can target different sections of a communication link [3]. In this study we focus on synchronization in the chaotic DSSS-CDMA system and evaluate its performance against jamming.

The communication system considered in this study is DSSS-CDMA, which uses chaotic sequences. In [4] the chaotic DSSS-CDMA performance is analyzed in the case of Gaussian noise for *N* single-users. The synchronization for this system is mathematically modeled and simulated in [5]. Also, the synchronization performance with the presence of channel noise and fading is analyzed in [6-8]. In addition, in [9], the authors propose an algorithm to attack the synchronization packets. In their investigation, the synchronization packets and data packets are assumed to be separated. Since the synchronization packets are fixed and periodic, it is possible to detect and attack them. However, in DSSS-CDMA system the synchronization bits are sent with the data bits at the same time. The robustness of synchronization in OFDM to different security attacks is investigated in [10, 11]. In addition, the synchronization of the MIMO-OFDM system is analyzed in [12].

This paper is organized as follows: In section-II, we describe the chaotic DSSS-CDMA system and its block-schematic. In section-III, the importance of the synchronization in DSSS-CDMA system is explained followed by block-schematic of acquisition section of synchronization. In the next section, we develop the mathematical model for the probability of detection and probability of false alarm. In section V, we analyze the mathematical model and show the simulation result for verifying the theoretical results obtained through mathematical expression.

II. SYSTEM DESCRIPTION

A. DSSS-CDMA system

The system block schematic is shown in the fig. 1. This system is introduced in [13] which is based on the chaotic communication. DSSS-CDMA system uses sequences to present a bit. These sequences have to be orthogonal so that multiple users can share the same channel. Each member of the sequences is called a chip. The chips can be generated based on different functions [13]. In this study, we used Chebyshev maps, which has following function

$$X_{K+1} = 2X_K^2 - 1 \tag{1}$$

These sequences have the mean value equal to 05. In order to make comparison with the conventional binary sequences , we multiply them by $\sqrt{2}$. In addition, their probability density function is equal to

$$f_{C_i}(c_i) = \frac{1}{\pi\sqrt{2-c_i^2}}, \text{ for } -\sqrt{2} \le c_i \le \sqrt{2} \tag{2}$$

Moreover, the mean value will be equal one and also,

$$E\{c_i^4\} = \int_{-\sqrt{2}}^{\sqrt{2}} c_i^4 \frac{1}{\pi\sqrt{2-c_i^2}} dc_i = \frac{3}{2} \cdot \tag{3}$$

In fig. 1, the bit b_j^1 is the jth bit of the message which is sent by the user one. Based on the nature of DSSS-CDMA system, b_j^1 is spread by sequence of chips (c_i^1). It is then passed through a modulation and interleaver block. The effect of modulation and interleaver are studied in [14].

In the channel, noise and jammer are introduced to the signal and also signal is get affected by the delay. On the receiver side, the signal is demodulated and passed through deinterleaver. Next, it is multiplied by the chip sequences

generated locally by the sequence synchronization block. Then, it enters to the correlator. Finally, the decision making circuit constructs $b_j^{1\prime}$.

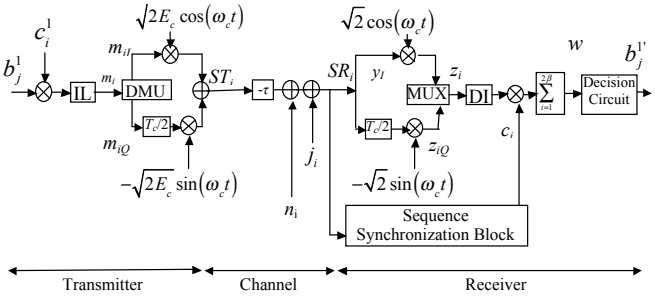

Fig. 1. Direct sequence spread spectrum system block schematic.

B. Jammer

In the present study, we assume that the jammer uses wideband Gaussian noise due to lack of information about the system's operating frequency. The modulation used in our system is a narrow band signal. The overlap of the narrowband signal and the wideband jammer is a narrowband jammer, which can describe as

$$j(k) = j_I(k)\sqrt{2E_j}\cdot\cos(\omega_c t) - j_Q(k)\sqrt{2E_j}\cdot\sqrt{2E_c}\cos(\omega_c t)\cdot \tag{4}$$

III. SYNCHRONIZATION

A. The importance of synchronization in DSSS-CDMA

Without the synchronization block, there would be a delay between received signal and the locally created chips.

In order to find the importance of the synchronization in the DSSS-CDMA system, we show the effect of the delay on probability of error rate. The output of the correlator in the case of delay is given by

$$W_{unsyn} = \sqrt{E_c}\sum_{i=1}^{2\beta} c_i^1 \cdot c_{(i-\tau)}^1 + \sqrt{E_N}\sum_{i=1}^{2\beta} n_i \cdot c_{(i-\tau)}^1 + \sqrt{E_J}\sum_{i=1}^{2\beta} j_i \cdot c_{(i-\tau)}^1 \cdot \tag{5}$$
$$= A + B + C$$

Where E_c is the energy of each chip, and E_N and E_J are energies of the noise jammer that are equal to N_0 and N_j respectively. Also, τ represents a delay in the system and 2β is the number of chips per bit.

The probability of error is equal to:

$$P_e(w) = \frac{1}{2}erfc\left(\frac{E[w]}{\sqrt{2\cdot \mathrm{var}[w]}}\right). \tag{6}$$

Its mean value is equal to

$$E^2\left[W_{unsyn}\right] = E[A+B+C] = E[A]+E[B]+E[C]. \tag{7}$$

So,

$$E[A] = E\left[\sqrt{E_c}\sum_{i=1}^{2\beta} c_{(i-\tau)}^1 c_i^1\right] = 0. \tag{8}$$

The autocorrelation of the chaotic sequences has impulse behavior. Thus it is maximum when τ is equal to zero, and for the rest of τ it is near to zero. More detail of the chaotic sequence properties are studied in [15].

Also,

$$E[B] = E[C] = 0. \tag{9}$$

Therefore,

$$E\left[W_{unsyn}\right] = 0. \tag{10}$$

by replacing (10) in (6), the probability of error becomes

$$p_{e(unsyn)} = \frac{1}{2}erfc(0) = 0.5. \tag{11}$$

Thus, if there is a delay between received signal and the locally generated sequences on the receiver side, the probability of error experiences the dramatic effect. In the following section, the synchronization process in DSSS-CDMA system is explained.

B. Schematic of Synchronization Block

In DSSS-CDMA system, the synchronization happens in two phases: acquisition and tracking [5].

In the acquisition phase, the delay will be removed with the resolution of a chip duration (*Tc*). Then, during the tracking phase, a fine tuning is done to eliminate the delay within a chirp duration.

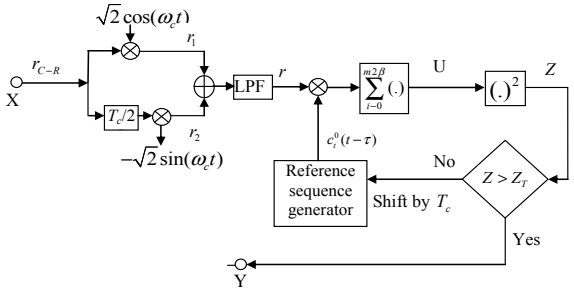

Fig .2. Acquisition section of synchronization block schematic.

In this paper, we assume that the delay is a multiple of *Tc*. Therefore, only acquisition phase is investigated here. The performance of the tracking part against jamming is the subject of our future studies.

As mentioned earlier, the synchronization is crucial for DSSS-CDMA system. In order to perform the synchronization, a synchronization signal is sent with the message signal. The synchronization signal always has a value equal to +1. Similar to the message, each

synchronization bit is spread with a sequence.

The acquisition section's block diagram is illustrated in the Fig. 2. In the acquisition section, the received signal is demodulated. Then, it is multiplied by the locally generated signal and passed through the correlator. The outcome of the correlator is given by

$$U = \sqrt{E_c}\sum_{i=1}^{2\beta} c_i^0 . c_{(i-\tau)}^0 + \sqrt{E_N}\sum_{i=1}^{2\beta} n_i \cdot c_{(i-\tau)}^0 + \sqrt{E_J}\sum_{i=1}^{2\beta} j_i \cdot c_{(i-\tau)}^0 . \quad (12)$$

where, c_i^0 presents the chip sequence of the synchronization signal. Please note that, the synchronization block also receives the message signal. However, due to orthogonality of message chips and synchronization chirp, the effect of the message signal in the synchronization becomes negligible.

In the next step, the correlator outcome is passed through the square law device. Similar to the autocorrelation function, the square law device has its maximum when τ is equal to zero. In other words, the synchronization signal and locally generated chips are aligned. Therefore, a threshold value (Z_T) is set (Z_T). If the square law device outcome becomes greater than Z_T, the synchronization is successful. Else, the locally generated chips are shifted for a chip and the process is repeated again utill the outcome of the square law device becomes greater than Z_T.

IV. MATHEMATICAL MODEL

In this section, the performance of DSSS-CDMA synchronization is modeled mathematically. Our performance analysis is based on the two key factor of the synchronization block: probability of detection and probability of false alarm.

Probability of detection is the probability in which the synchronization block detects the delay when the two signals are aligned. On the other hand, the probability of false alarm is the probability in which the synchronization detects the delay but two signals are not aligned. In this case, the outcome of the synchronization is an error.

A. The probability of the false alarm

A false alarm can happen when the square law device outcome become greater than the threshold value (Z_T). In order to find that, we calculate the probability density function of the square law device in the case of misalignment.

The correlator outcome, in the case of misalignment, can be expressed as

$$\begin{aligned} U_{unsyn} &= \sqrt{E_c}\sum_{i=1}^{2\beta} c_i^0 . c_{(i-\tau)}^0 + \sqrt{E_N}\sum_{i=1}^{2\beta} n_i \cdot c_{(i-\tau)}^0 + \sqrt{E_J}\sum_{i=1}^{2\beta} j_i \cdot c_{(i-\tau)}^0 \\ &= A + B + C. \end{aligned} \quad (13)$$

The mean value of (13) is given by

$$E\left[U_{unsyn}\right] = E[A+B+C] = 0, \quad (14)$$

Also, the variance of U_{syn} is obtained from

$$\begin{aligned} \sigma_{U_{unsyn}}^2 &= E[{U_{unsyn}}^2] - E^2\left[U_{unsyn}\right] = E[(A+B+C)^2] - E^2\left[U_{unsyn}\right] \\ &= E[A^2] + E[B^2] + E[C^2]. \end{aligned} \quad (15)$$

So,

$$\begin{aligned} E[A^2] &= E\left[\left(\sqrt{E_c}\sum_{i=0}^{2\beta}(c_{i-\tau}^0)(c_i^0)\right)^2\right] = E_c 2\beta E\left[\left(c_i^0\right)^2\right] E\left[\left(c_{i-\tau}^0\right)^2\right] \\ &\quad + E_c 2\beta(2\beta-1) E\left[\left(c_i^0\right)\right] E\left[\left(c_{i-\tau}^0\right)\right] E\left[\left(c_i^0\right)\right] E\left[\left(c_{i-\tau}^0\right)\right] \\ &= E_c 2\beta, \end{aligned} \quad (16)$$

$$E[B^2] = E\left[\left(\sqrt{E_N}\sum_{i=1}^{2\beta} n_i \cdot c_{(i-\tau)}^0\right)^2\right] = 2\beta N_0/2 \quad (17)$$

and

$$E[C^2] = E\left[\left(\sqrt{E_J}\sum_{i=1}^{2\beta} j_i \cdot c_{(i-\tau)}^0\right)^2\right] = 2\beta N_j/2 . \quad (18)$$

Thus,

$$\begin{aligned} \sigma_{U_{unsyn}}^2 &= E[A^2] + E[B^2] + E[C^2] \\ &= E_c 2\beta + 2\beta N_0/2 + 2\beta N_j/2 . \end{aligned} \quad (19)$$

So, U_{unsyn} can be presented as

$$U_{unsyn} \approx G\left(0, E_c 2\beta + 2\beta N_0/2_0 + 2\beta\varphi N_j/2\right). \quad (20)$$

The square law device outcome is equal to

$$Z = U^2 \quad (21)$$

Therefore, the PDF of the "*Z*" can be written by the chi-square distribution [16].

$$P_Z = \frac{1}{\sigma_{U_{unsyn}}\sqrt{2\pi Z}} \exp\left(-\frac{1}{2}(Z/\sigma_{U_{unsyn}}^2)\right) \quad (22)$$

As mentioned earlier, the false alarm happens when the system detects the delay by mistake. Therefore, the outcome of the square law device, in case of misalignment, should be greater than Z_T. Thus, probability of false alarm can be expressed as

$$P_F = \int_{z_T}^{\infty} \frac{1}{\sigma_{U_{unsyn}}\sqrt{2\pi Z}} \exp\left(-\frac{1}{2}(Z/\sigma_{U_{unsyn}}^2)\right) dZ \quad (23)$$

By replacing $\sqrt{Z} = x$, we have

$$P_F = \int_{\sqrt{z_T}}^{\infty} \frac{\sqrt{2}}{\sigma_{U_{unsyn}}\sqrt{\pi}} \exp\left(-\frac{1}{2}(x^2/\sigma^2_{U_{unsyn}})\right)dx$$
$$= \frac{\sqrt{2}}{\sigma_{U_{unsyn}}\sqrt{\pi}} \times \frac{\sqrt{2}\sqrt{\pi}\sigma_{U_{unsyn}}}{2} erf\left(\frac{x}{\sqrt{2\sigma^2_{U_{unsyn}}}}\right)\Bigg]_{\sqrt{z_T}}^{\infty} \quad (24)$$
$$= 1 - erf\left(\sqrt{\frac{z_T}{2\sigma^2_{U_{unsyn}}}}\right)$$

B. The probability of the false alarm

As mentioned before, detection happens when the outcome of the square law device, in case of the alignment, become greater than Z_T. Similar to the calculation of the probability of false alarm, , first, the distribution parameters of the correlator, in case of the aligned signals, is calculated. Then, the distribution of the square law device outcome is calculated. Finally, based on the probability density function of the square law device the probability of detection can be found.

Thus, the outcome of the correlator, in case of alignment, is given by

$$U_{syn} = \sqrt{E_c}\sum_{i=0}^{2\beta}(c_i^0)^2 + \sqrt{E_N}\sum_{i=1}^{2\beta} n_i \cdot c_i^0 + \sqrt{E_J}\sum_{i=1}^{2\beta} j_i \cdot c_i^0 \quad (25)$$
$$= D + F + G.$$

U_{syn} has the mean value equal to:

$$E\left[U_{syn}\right] = E\left[D + F + G\right] = E[D] + E[F] + E[G]. \quad (26)$$

Therefore,

$$E[D] = E\left[\sqrt{E_c}\sum_{i=0}^{2\beta}(c_i^0)^2\right] = \sqrt{E_c}\,2\beta, \quad (27)$$

and

$$E[G] = E[F] = 0 \quad (28)$$

Thus

$$E\left[U_{syn}\right] = \sqrt{E_c}\,m2\beta. \quad (29)$$

The variance of the U_{syn} is equal to

$$\sigma^2_{U_{syn}} = E[Z^2_{U_{syn}}] - E^2\left[U_{syn}\right] = E[(D+F+G)^2] - E^2\left[U_{syn}\right] \quad (30)$$
$$= E[D^2] + E[F^2] + E[G^2] - E^2\left[U_{syn}\right],$$

$$E[D^2] = E\left[\left(\sqrt{E_c}\sum_{i=0}^{2\beta}(c_i^0)^2\right)^2\right]$$
$$= E_c 2\beta E\left[\left(c_i^0\right)^4\right]$$
$$+ E_c 2\beta(2\beta-1)E\left[\left(c_i^0\right)^2\right]E\left[\left(c_i^0\right)^2\right] \quad (31)$$
$$= E_c 4\beta^2 + E_c\beta,$$

$$E[F^2] = E\left[\left(\sqrt{E_N}\sum_{i=1}^{2\beta} n_i \cdot c_i^0\right)^2\right] = 2\beta N_0/2 \quad (32)$$

and

$$E[G^2] = E\left[\left(\sqrt{E_J}\sum_{i=1}^{2\beta} j_i \cdot c_i^0\right)^2\right] = 2\beta N_j/2. \quad (33)$$

Thus,

$$\sigma^2_{U_{syn}} = E[D^2] + E[F^2] + E[G^2] - E^2\left[U_{syn}\right],$$
$$= E_c 4\beta^2 + E_c\beta + 2\beta N_0/2 + 2\beta N_j/2 - E_c 4\beta^2 \quad (34)$$
$$= E_c\beta + 2\beta N_0/2 + 2\beta N_j/2$$

Therefore "U" can be described as

$$U_{syn} \approx G\left(\sqrt{E_c}\,2\beta\ ,\ E_c\beta + 2\beta N_0/2 + 2\beta N_j/2\right) \quad (35)$$

Same as before, $Z=U^2$. Therefore, PDF of "Z" can be express as a chi-square distribution [16]

$$p_Z = \left(\frac{1}{\sigma_{U_{syn}}\sqrt{2\pi Z}} \exp\left(-\left(Z+\lambda/\sigma^2_{U_{syn}}{}^2\right)/2\right)\right), \quad (36)$$
$$\left(\times\cosh\left(\sqrt{Z/\sigma^4_{U_{syn}}\lambda}\right)\right)$$

where

$$\lambda = E\left[U_{syn}\right] = E_c 4\beta^2. \quad (37)$$

The probability of detection can be express as:

$$P(D)=\int_{z_T}^{\infty}\left(\frac{1}{\sigma_{U_{syn}}\sqrt{2\pi Z}}\exp\left(-\frac{\left(Z/\sigma^2_{U_{syn}}+\lambda/\sigma^2_{U_{syn}}\right)}{2}\right)\times\cosh\left(\sqrt{Z/\sigma^4_{U_{syn}}\lambda}\right)dZ\right) \quad (38)$$

Same as before, by using $\sqrt{Z}=x$, we have

$$p_D=\frac{\sqrt{2}}{\sigma 2\sqrt{\pi}}\int_{z_T}^{\infty}\exp\left(-\frac{\left(x^2+\lambda\right)}{2\sigma^2_{U_{syn}}}\right)\left(\exp\left(\sqrt{\lambda/\sigma^4_{U_{syn}}}x\right)+\exp\left(-\sqrt{\lambda/\sigma^4_{U_{syn}}}x\right)\right)dx \quad (39)$$

$$\begin{aligned}p_D&=\frac{\sqrt{2}}{\sigma_{U_{syn}}2\sqrt{\pi}}\int_{z_T}^{\infty}\exp\left(-\frac{\left(x^2+\lambda\right)}{2\sigma^2_{U_{syn}}}\right)\exp\left(\sqrt{\lambda/\sigma^4_{U_{syn}}}x\right)dx\\&+\int_{z_T}^{\infty}\exp\left(-\frac{\left(x^2+\lambda\right)}{2\sigma^2_{U_{syn}}}\right)\exp\left(-\sqrt{\lambda/\sigma^4_{U_{syn}}}x\right)dx\\&=K+L\end{aligned} \quad (40)$$

$$\begin{aligned}K&=\frac{\sqrt{2}}{\sigma_{U_{syn}}2\sqrt{\pi}}\int_{z_T}^{\infty}\exp\left(-\frac{\left(x^2+\lambda\right)}{2\sigma^2_{U_{syn}}}\right)\exp\left(\sqrt{\lambda/\sigma^4_{U_{syn}}}x\right)dx\\&=\frac{\sqrt{2}}{\sigma_{U_{syn}}2\sqrt{\pi}}\int_{z_T}^{\infty}\exp\left(-\frac{x^2-2\sqrt{\lambda}x+\lambda}{2\sigma^2_{U_{syn}}}\right)dx\\&=\frac{\sqrt{2}}{\sigma_{U_{syn}}2\sqrt{\pi}}\int_{z_T}^{\infty}\exp-\left(x/\sqrt{2}\sigma_{U_{syn}}-\sqrt{\lambda}/\sqrt{2}\sigma_{U_{syn}}\right)^2dx\\&=\frac{\sqrt{2}}{\sigma_{U_{syn}}2\sqrt{\pi}}\frac{\sqrt{\pi}\sqrt{2}\sigma_{U_{syn}}}{2}erf\left(x/\sqrt{2}\sigma_{U_{syn}}-\sqrt{\lambda}/\sqrt{2}\sigma_{U_{syn}}\right)\Big]_{Z_T}^{\infty}\\&\frac{1}{2}erf\left(\sqrt{Z/2\sigma^2_{U_{syn}}}-\sqrt{\lambda/2\sigma^2_{U_{syn}}}\right)\Big]_{Z_T}^{\infty}\\&=\frac{1}{2}\left(1-erf\left(\sqrt{Z_T/2\sigma^2_{U_{syn}}}-\sqrt{\lambda/2\sigma^2_{U_{syn}}}\right)\right)\end{aligned} \quad (41)$$

and

$$L=\frac{1}{2}\left(1-erf\left(\sqrt{Z_T/2\sigma^2_{U_{syn}}}+\sqrt{\lambda/2\sigma^2_{U_{syn}}}\right)\right). \quad (42)$$

Therefore,

$$\begin{aligned}p_D&=K+L\\&=1-\frac{1}{2}\left(erf\left(\sqrt{Z_T/2\sigma^2_{U_{syn}}}-\sqrt{\lambda/2\sigma^2_{U_{syn}}}\right)+erf\left(\sqrt{Z_T/2\sigma^2_{U_{syn}}}+\sqrt{\lambda/2\sigma^2_{U_{syn}}}\right)\right)\end{aligned} \quad (43)$$

V. Result and Discussion

In previous section, we derived the mathematical expression of the probability detection of false alarm under jamming attack. Here, we analyze our mathematical expressions in different scenarios. In all of these analytic scenarios, we set number of chips per bit (2β) equal to 300. Also, we normalize the power of each bit (E_b=1).

Fig. 3 shows the ROC plot for jammer with different power. To focus on the effects of the jammers, in this scenario, we assume that there is no environment noise i.e SNR=inf. As can be seen in Fig. 3, even a jammer, which can cause SJR=5 dB, can have a dramatic effect on the system's performance. In this scenario, we set Z_T to 200.

In addition, to evaluate our mathematical expressions we run Monte Carlo simulation on Matlab. The results are shown in the green straight lines, and the theoretical outcomes are shown by blue dashed lines. As can be seen from the figure, the simulation results match with the theory. This simulation is run for 10^4 times.

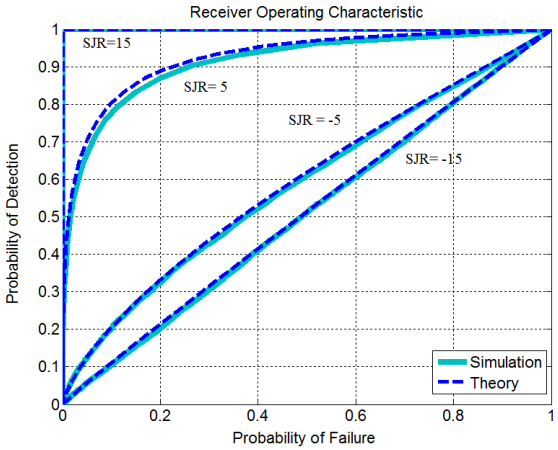

Fig. 3. ROC curves in the case of jammer with deferent power based on the theory and simulation.

(43) and (24) show that the probability of detection and false alarm are sensitive to the choice of Z_T. Therefore, to optimize the system performance, it is necessary to find Z_T in which, the probability detection become maximum and the false alarm become minimum. Fig. 4 demonstrates the probability of detection and false alarm based on Z_T in the different SJR. The straight blue line and dotted blue line are probabilities of detection and false alarm in case of no existing jammer (SJR=inf). In this case, Z_T can be chosen smaller than 200. As the jammer power increases, the probability of detection decreases and the probability of false alarm increases. However, the probability of false alarm seems to get

more affected than probability of detection. For SJR=-10 dB, the probability of false alarm is getting close to the probability of detection.

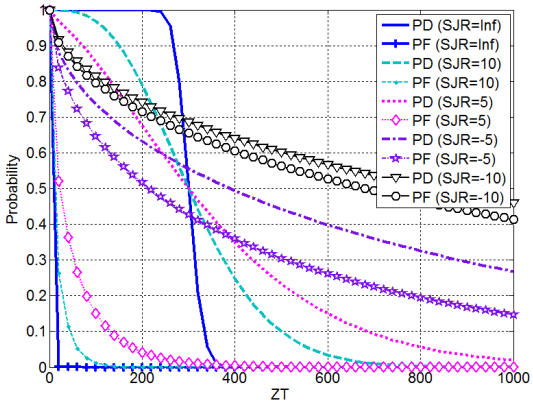

Fig. 4. Probability of detection and false alarm based on Z_T for deferent jammer powers.

Fig. 5 presents the probability of detection and false alarm based on the jammer power (SJR) when Z_T is equal to 200, 300 and 400. As shown in the figure, for Z_T=200, the probability of detection is better compared to the others. However, it has the worse probability of false alarm. Consequently, for Z_T=400 has the best probability of false alarm and worse probability of detection. Also, the probability of false alarm rises after SJR=10 dB. After this point, the communication system starts to experience a noticeable effect on its error rate.

As can be seen in Fig. 5, in Area I, when the jammer power increases, the probability of detection is decreased, and the probability of false alarm is increased. By decreasing Z_T, we can increase the chance of detection; however, the probability of false alarm is increased as well which is not desirable.

On the other hand, both probability of detection and false alarm is increasing by jammer power in the area II. In fact, in that area, the probability of false alarm and detection become equal due to the high level of the jamming signal.

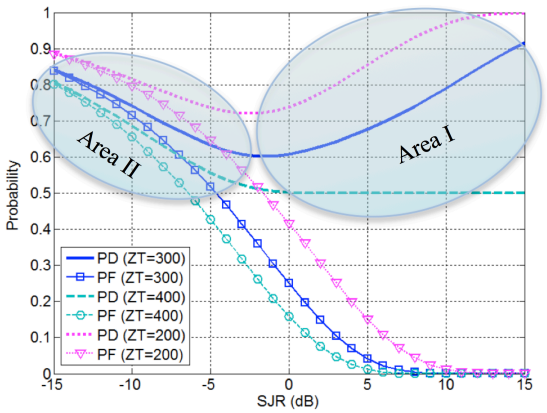

Fig. 5. Probability of detection and false alarm based on SJR.

VI. Conclusion

In this paper, we investigate the effects of jammer on DSSS-CDMA system using chaotic sequences. We specifically study the effect jamming attack on accusation section of the synchronization block. We show that the synchronization in DSSS-CDMA system is quite vulnerable to the jamming attacks. In order to consider the effect of these jammers on synchronization block, mathematical expressions of the probability of detection and false alarm are developed in closed form. Also, we run a simulation based on Monte Carlo method to evaluate our mathematical expressions.

Our result also shows how the vulnerability of synchronization block to jamming signals can cause tragic effects on the system probability of error. Our investigation reveals that even low power jammer (with SJR=10 dB in our scenario) can make the whole system collapse.

References

[1] A. Tayebi, S. Berber, and A. Swain, "Department of Electrical and Computer Engineering, University of Auckland, Auckland, New Zealand," in *Sensing Technology (ICST), 2013 Seventh International Conference on*, 2013, pp. 97-102.

[2] D. Fudenberg and J. Tirole, "A" signal-jamming" theory of predation," *The RAND Journal of Economics,* pp. 366-376, 1986.

[3] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *Network, IEEE,* vol. 20, pp. 41-47, 2006.

[4] G. S. Sandhu and S. M. Berber, "Investigation on operations of a secure communication system based on the chaotic section shift keying scheme," in *Information Technology and Applications, 2005. ICITA 2005. Third International Conference on*, 2005, pp. 584-587 vol.2.

[5] S. M. Berber and B. Jovic, "Sequence synchronization in a wideband CDMA system," 2007.

[6] R. Vali, S. M. Berber, and S. K. Nguang, "Effect of Rayleigh fading on non-coherent sequence synchronization for multi-user chaos based DS-CDMA," *Signal Processing,* vol. 90, pp. 1924-1939, 2010.

[7] B. Jovic, C. Unsworth, G. S. Sandhu, and S. M. Berber, "A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems," *Signal Processing,* vol. 87, pp. 1692-1708, 2007.

[8] R. Vali, S. M. Berber, and N. Sing Kiong, "Analysis of Chaos-Based Code Tracking Using Chaotic Correlation Statistics," *Circuits and Systems I: Regular Papers, IEEE Transactions on,* vol. 59, pp. 796-805, 2012.

[9] C. Yuan, H. Fei, Y. Jian, C. Xiang, and G. Yuantao, "A smart tracking-based jamming scheme for signals with periodic synchronization sequences," in *Wireless Communications and Signal Processing (WCSP), 2011 International Conference on*, 2011, pp. 1-5.

[10] M. J. La Pan, T. C. Clancy, and R. W. McGwier, "An Assessment of OFDM Carrier Frequency Offset Synchronization Security for 4G Systems," in *Military Communications Conference (MILCOM), 2014 IEEE*, 2014, pp. 473-478.

[11] M. J. La Pan, T. C. Clancy, and R. W. McGwier, "Section warping and differential scrambling attacks against OFDM frequency synchronization," in *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*, 2013, pp. 2886-2890.

[12] C. Shahriar, S. Sodagari, and T. C. Clancy, "Performance of pilot jamming on MIMO channels with imperfect synchronization," in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 898-902.

[13] S. Berber and S. Feng, "Theoretical Modeling and Simulation of a Chaos-Based Physical Layer for WSNs."

ISBN: 978-1-61804-290-3

[14] S. M. Berber, "Fading mitigation in an interleaved noise-based DS-CDMA system for secure communications," in *Proceedings of the Fifth IASTED International Conference on Signal Processing, Pattern Recognition and Applications*, 2008, pp. 260-265.
[15] G. S. Sandhu and S. M. Berber, "Investigation on orthogonal signals for secure transmission in multiuser communication," 2007.
[16] H. O. Lancaster and E. Seneta, *Chi-Square Distribution*: Wiley Online Library, 1969.

Arash Tayebi received the B.S degree in electrical engineering from Shiraz University, Shiraz, Iran in 2009, and Master degree in telecommunication engineering from University of Melbourne, Melbourne, Australia in 2011. He is currently working toward the PhD degree in electrical engineering at University of Auckland, Auckland, New Zealand. His research interests include chaos-based communication systems, physical layer security, and CDMA and OFDM communication. He is student member of IEEE.

Stevan Mirko Berber was born in Stanisic, Serbia, former Yugoslavia. He completed his undergraduate studies in electrical engineering in Zagreb, master studies in Belgrade, and PhD studies in Auckland, New Zealand. Currently Stevan is with the Department of Electrical and Computer Engineering at Auckland University, New Zealand. He was appointed Visiting Professor at the University of Novi Sad in 2004 and Visiting Scholar at the University of Sydney in 2008. His teaching interests are in communication systems, information and coding theory, discrete stochastic signal processing and wireless sensor and computer networks. His research interests are in the fields of digital communication systems and signal processing with the emphasis on applications in CDMA systems and wireless computer, communication and sensor networks. He is the author of more than 80 refereed journal and conference papers, 8 books and three book chapters. Dr Berber is a referee for papers in leading journals and conferences in his research area. He has been leading or working on a large number of research and industry projects. Dr. Berber is a senior member of IEEE, a member of New Zealand Scientists, and an accredited NAATI translator for English language.

Akshya Swain received B.Sc. Engineering degree in Electrical Engineering and M.Sc. Engineering degree in Electronic Systems and Communication from Sambalpur University, India, in 1985 and 1988, respectively. From 1994 to 1996 he was Commonwealth Scholar in the United Kingdom and obtained Ph.D. degree from the Department of Automatic Control and Systems Engineering at the University of Sheffield in 1997. From 1986 to 2002, he worked as Lecturer, Assistant Professor and Professor of Electrical Engineering at the National Institute of Technology, Rourkela, India. During 1988/1989 he was Assistant Director in the Ministry of Energy for the Indian government. He joined the Department of Electrical and Computer Engineering at The University of Auckland in September 2002. His research interests include nonlinear system identification & control, biomedical signal processing, sensor networks and control applications to power system and inductive power transfer systems. Currently he acts as a member of the Editorial Board of the International Journal of Automation and Control and International Journal of Sensors, Wireless Communications and Control.