International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 6, ISSN No. 2455-2143, Pages 32-40
Published Online October 2018 in IJEAST (http://www.ijeast.com)

CAM: CHAOTIC ADAPTIVE MODULATION SECURE SYSTEM

Amr Sayed AbdelFattah
Higher Colleges of Technology
Alain, UAE

Abstract— **This paper discusses the uses of chaotic signals in secure wireless communication systems. A novel system, called chaotic adaptive modulation, CAM, has been developed. The system is mainly designed to simplify the chaotic secure communication system by adding conventional QAM scheme at transmitter end where the states of QAM is chosen randomly due to the beforehand data-chaotic stream key Xoring block. The performance of the proposed system under imperfect fading channel is evaluated.**

Keywords—chaotic signal; adaptive modulation; secure system; BER.

I. INTRODUCTION

There is an ongoing evolution in the communications industry. Experts are becoming more keenly aware that communications systems are valuable commodities that are increasingly under attack. In an effort to reduce the number of successful attacks and thus stem the tide of loss associated with a compromised communication system, security experts are employed to build defenses around or within the communication system to prevent adversarial manipulations of that system. Wireless network security based on encryption is widely prevalent at this time. However, encryption techniques do not take into account wireless network characteristics such as random bit errors due to noise and burst errors due to fading. This results in a fundamental trade-off between security and throughput in encryption based wireless security. The more secure a system is, the more you have compromised in terms of performance and usability. When designing a secure system, you should determine all the possible threats, vulnerabilities, and attacks and choose the techniques to implement security based on threat mitigation first and performance second.

In this paper, a novel system, called chaotic adaptive modulation, has been developed. Here and after we call that system as CAM, This system uses channel opportunities (acceptable signal to noise ratio) to maximize the throughput subject to desired security constraints. So, the problem then is to maximize the overall throughput while guaranteeing a minimum and/or an average security level(s) for the message.

II. DESCRIPTION OF CAM SYSTEM

The proposed chaotic adaptive modulation (CAM) system is shown in Fig. 1. CAM transmitter can be divided mainly into two stages:

The first stage (chaotic encryption) is conventional Vernam's one-time pad as shown in Fig. 2. Vernam's one-time pad, which encrypts a message *m* by XORing it with a truly random signal, is the most famous perfectly secret cipher, it even resists all the passive attacks mentioned in [1]. This can be mathematically proven by Shannon's theory. Vernam's one-time pad is perfectly secret, due to the existence of true random key string *k*, the message *m* is encrypted by XORing with *k*, consequently the encrypted message *c(t)* is a truly random bit sequence for the adversary [2]. In our work, we should design chaotic random number generator (CRNG) to generate truly random key string *k*, the randomness behavior should be guaranteed by international randomness test such as NIST.

Our novel system proposes adding adaptive modulation after encryption stage, thus it is called chaotic adaptive modulation (CAM), the idea of suggested CAM is quite simple; CAM depends on changing chaotically the phase and amplitude of carrier signal in M-QAM while the status of transmission channel determines the *M* value.

The term of Link adaptation is used in wireless communications to denote the matching of the modulation, coding and other signal and protocol parameters to the conditions on the radio link (e.g. the path-loss, the interference due to signals coming from other transmitters, the sensitivity of the receiver, the available transmitter power margin, etc.). Adaptive modulation systems invariably require some channel state information at the transmitter. This could be acquired in time division duplex systems by assuming that the channel from the transmitter to the receiver is approximately the same as the channel from the receiver to the transmitter. Alternatively, the channel knowledge can also be directly measured at the receiver, and feedback to the transmitter. Adaptive modulation systems improve the rate of transmission, and/or bit error rates, by exploiting the channel state information that is present at the transmitter. Especially over fading channels which model wireless propagation environments, adaptive modulation systems exhibit great performance enhancements compared to systems that do not exploit channel knowledge at the transmitter [3-4].

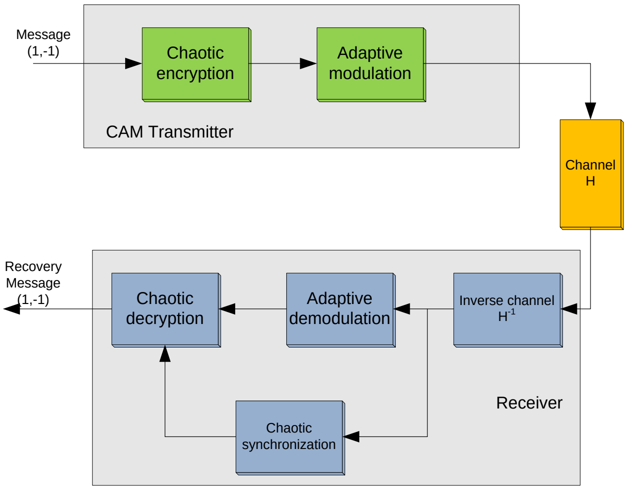

Fig. 1. Simple block diagram for CAM system

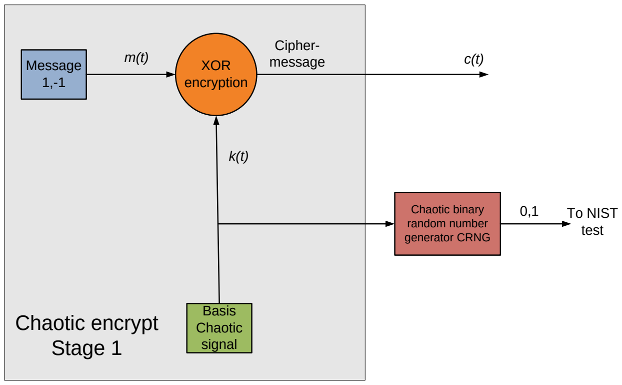

Fig. 2. First encryption stage depending on Vernam's one time pad or XORing

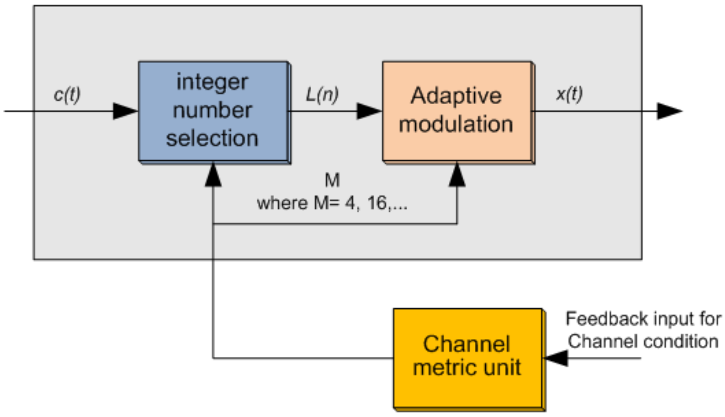

Fig. 3. Selection of the phase and amplitude of transmitted signal

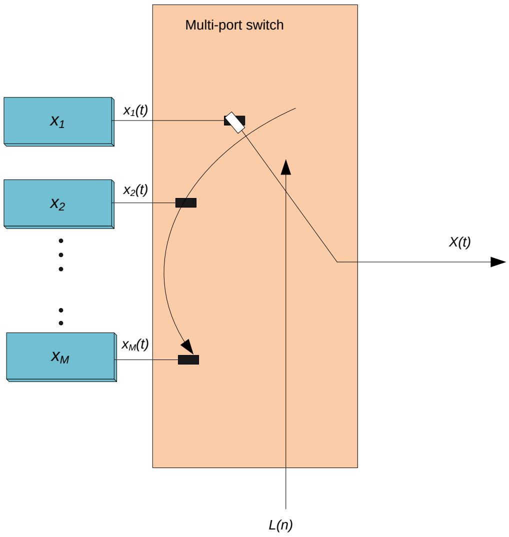

Fig. 4. Selection of constellation point in QAM depending on input *L(n)*

In essence, it is a way to optimize the transmission scheme according to the state of the channel for a required fidelity. For example, when the channel is in a poor state (i.e., low SNR) we can reduce the signal constellation size in order to improve fidelity (reduce BER). Conversely, when the channel is in a good state (high SNR) we can increase the signal constellation size in order to increase the achievable data rate. Basically, adaptive modulation can be expressed in simple formula *M-QAM* where *M*=4, 16, 32, 64,128, or 256.

The modulation scheme in CAM that is proposed in this paper depends on changing chaotically the phase and amplitude of carrier signal x_1, x_2, $x_{3,}\ldots x_M$, where x_i is the transmitted constellation point and *M*=4, 16, 32, 64, 128, 256, and (*M*) depends on the channel parameter.

Our novel idea is quite simple; that is, if the input signal of QAM is from well-designed CRNG, the phase and amplitude of carrier signal of QAM output is selected randomly and doesn't depend on the input data, consequently the security is achieved whereas the adaptive modulation improves rate of transmission, and/or bit error rates. Moreover the QAM scheme quite simplifies the transmitted symbol contrary to the transmission of chaotic signal as in most chaotic systems.

Fig. 3 illustrates how the phase and amplitude of transmitted signal is selected in our proposed system, firstly an *integer number selection* produces output *L(n),* in time step *n*, where *L(n)*=1,2,..*M* and *M* value depends on the feedback of channel conditions *(M=4,16,32,OR 64*). The second block is conventional adaptive modulation which selects phase and amplitude of output signal from x_1 up to x_M equivalent to *L(n)* as indicated in Fig. 4.

Several channel parameters could be used in channel metric block of Fig. 3, one of them is SNR. The SNR at the receiver is a good channel metric to decide the value of *M*. For example if *M* equals 4 this means we have only four states x_1, x_2, x_3,and x_4 to transmit, then the output of CAM, x_n, at time slot *n* is one of them depending on the value of input integer *L(n)* of CAM. Table 1 illustrates example for adaptive modulation scheme. If SNR below 17 dB, *M* is selected to be 4, else if SNR between 17 dB and 23 dB, *M* should equals 16, finally if SNR is greater

TABLE I. MODULATION SCHEME TO SNR RANGE

M value	Signal to noise ratio (SNR)
M=4	SNR<17 dB
M=16	17 dB ≤ SNR ≤ 23 dB
M=32	SNR > 23 dB

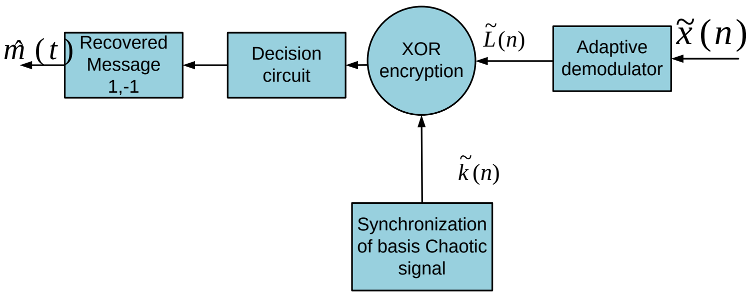

Fig. 5. Simple block diagram of CAM receiver

than 23 dB, *M* equals 32. At the receiver side, the inverse process of transmitter is done.

As shown in Fig. 1, first step in the receiver is inverse channel filter, equalizer, which is used to compensate the channel effects. This stage should be designed carefully to minimize synchronization error of chaotic signal and improve the BER.

The conventional adaptive demodulator is used to extract $\tilde{L}(n)$, as shown in Fig. 5, then Xoring it with synchronized chaotic signal $\tilde{k}(t)$. Finally, the output is sent to the decision circuit in order to recover the message $\hat{m}$ (1,-1).

III. SYSTEM PERFORMANCE

A. CAM system numerical simulation

Simulink\matlab® platform is used to simulate the performance of proposed CAM system. The overall Simulink model for CAM system is shown in Fig. 6. The dynamic Lorenz system is used to generate three chaotic signals *u*, *v*, *w*. only one signal "*u*" is used to spread the data streams {-1,1}, the three differential equations of Lorenz signal are as below:

$$\frac{du}{dt} = c_1 v - c_1 u \qquad (1)$$

$$\frac{dv}{dt} = c_2 u - v - uw \qquad (2)$$

$$\frac{dw}{dt} = uv - c_3 w \qquad (3)$$

where

c_1, c_2 and c_3 are arbitrary constants and taken as 10, 28, and 2.666 respectively [5]. The criteria of integer number selector block is producing integer number depends on the input signal. Finally, the state in the QAM constellation diagram is selected

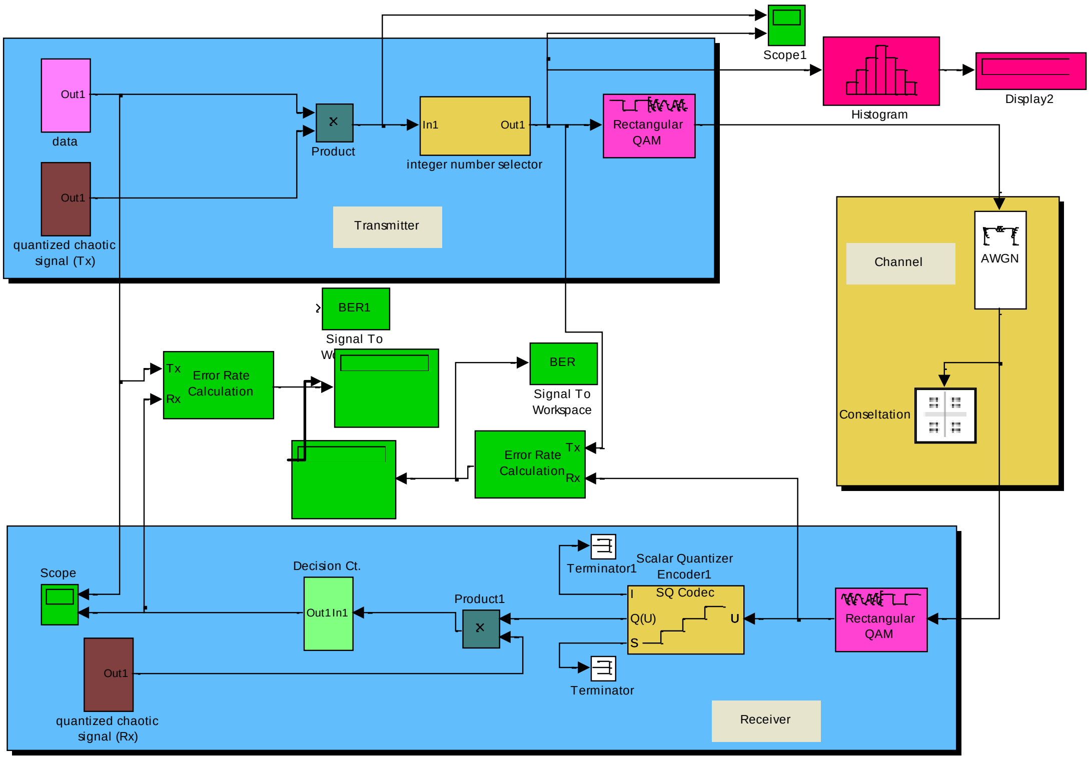

Fig. 6. The simulink model for CAM system

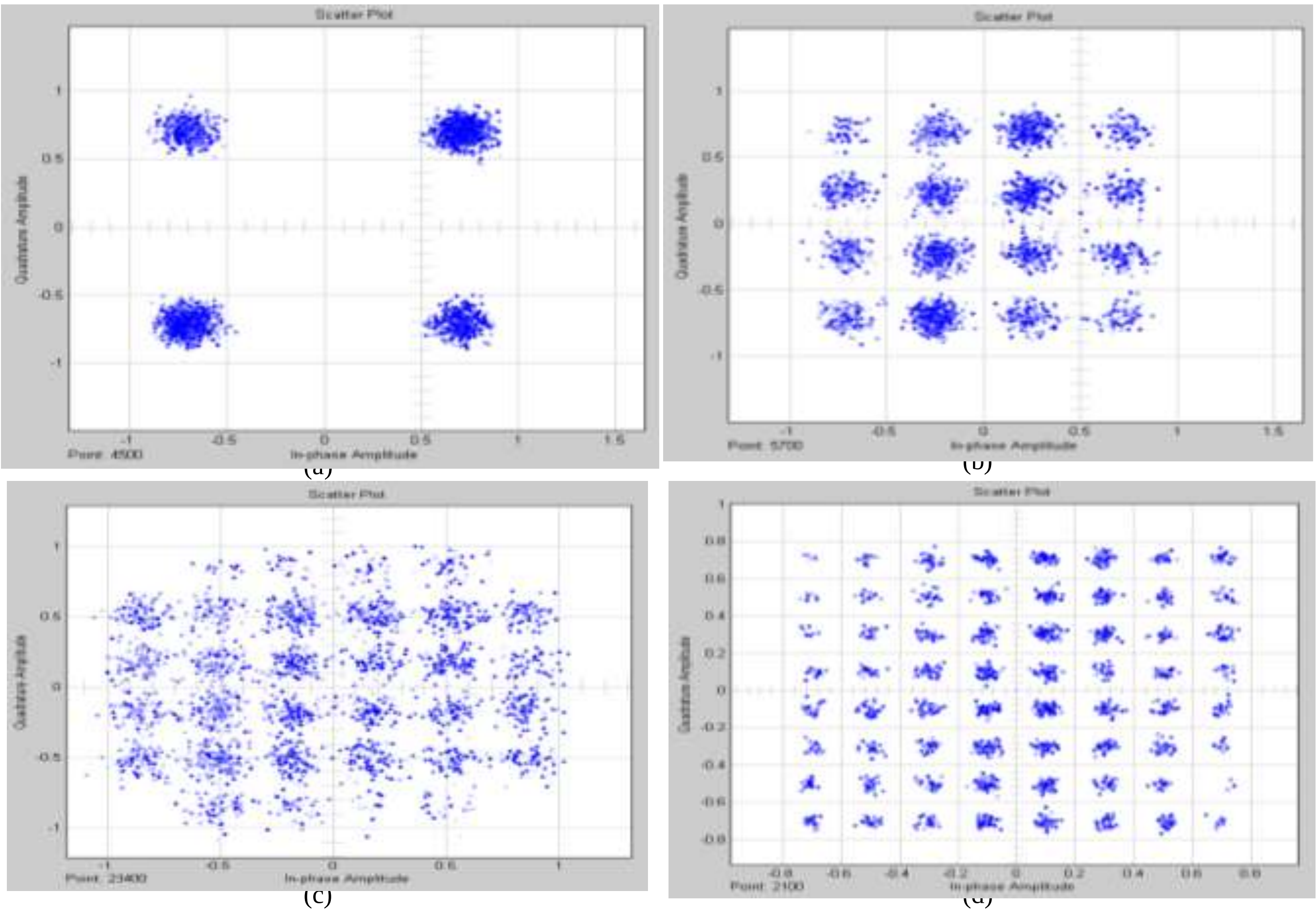

Fig. 7. The constellation diagram for M-QAM (a) 4-QAM, Eb/No=20 (b) 16-QAM, Eb/No=20 (c) 32-QAM, Eb/No=20 (d) 64-QAM, Eb/No=30

according to the input integer number.

The constellation diagram for *M*-QAM where *M*=4,16,32, and 64 after passing through AWGN channel are shown in Fig. 8.

B. *Probability distribution of transmitted symbols*

The randomness of the input for adaptive QAM block should be evaluated to ensure that the transmitted symbols or states in constellation diagram of QAM are selected randomly, thus it satisfies the prefect security conditions. A robust *random number* must reasonably represent a known probability distribution function (usually uniform over some finite domain) [6-7]. We can view distribution function using histogram which is a graphical representation showing a visual impression of the distribution of data.

A stream of random number generated by integer number selection block is displayed in a histogram. Bars in a histogram of random numbers should show a flatting or uniformly distribution. The first case is for 4-QAM, the input is an integer number between 1 and 4 represents four states of constellation diagram, the histogram output is shown in Fig. 8 indicating a uniform distribution, so the states 1 to 4 have almost equal probability. This method verifies the randomness of the transmitted symbols and strengthens the results of randomness NIST test for CRNG [8][9]. In case of 16-QAM, 32-QAM, and 64-QAM, the histograms are shown in Figs. 9-11 respectively. The figures indicate uniform distributions in all cases as well.

IV ANALYTICAL DERIVATION

A QAM scheme is a useful modulation technique for achieving high data rate transmission without increasing the bandwidth of wireless communication systems [4]. QAM, combined with other schemes, has gained great attention in overcoming detrimental channel impairments. Furthermore, an adaptive modulation scheme can maximize the throughput of wireless communication systems when combined with the QAM scheme [3][4].

Although an exact evaluation of bit error probability for M-ary square QAM can be obtained for arbitrary signal constellation size, indeed, it is quite tedious to express in a closed form [10]. As an example, the exact BER expressions for 16-QAM and 64-QAM are presented in [11] and [12].

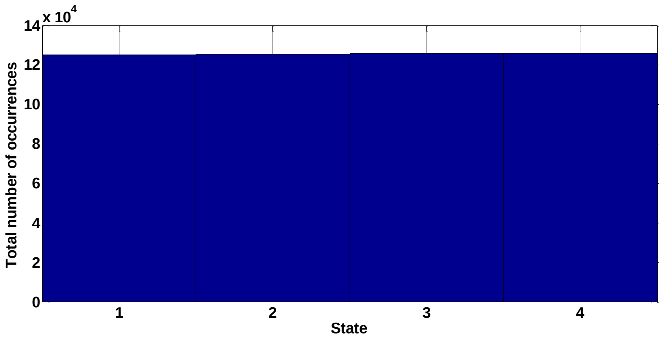

Fig. 8. The histogram of the states of 4-QAM

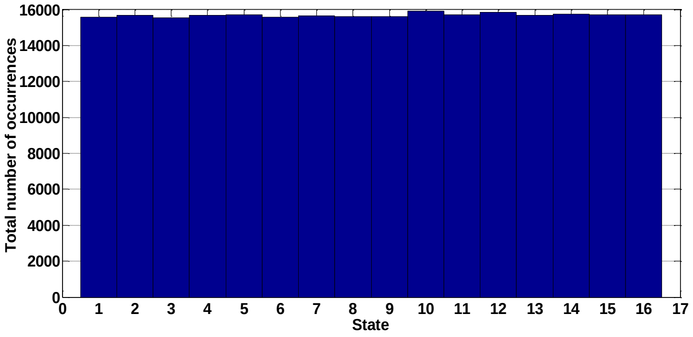

Fig.9. The histogram of the states of 16-QAM

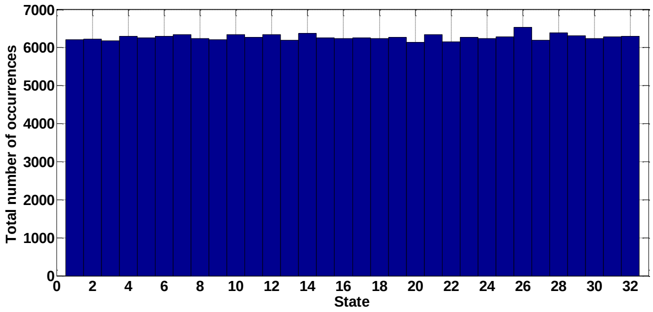

Fig.10. The histogram of the states of 32-QAM

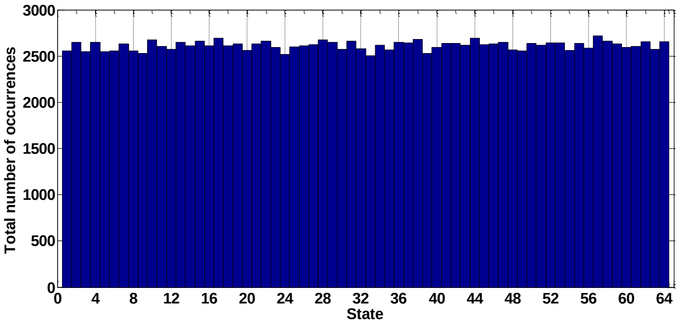

Fig.11. The histogram of the states of 64-QAM

However, the exact and general BER expression of arbitrary M–ary square QAM has not yet been derived.

Although approximate expressions in the literature may provide accurate values of the BER in high signal-to-noise ratio (SNR), the evaluation of the BER using those expressions tends to deviate from its exact values when SNR is low. The exact expression of average bit error probability of M-ary square QAM can be obtained by [10].

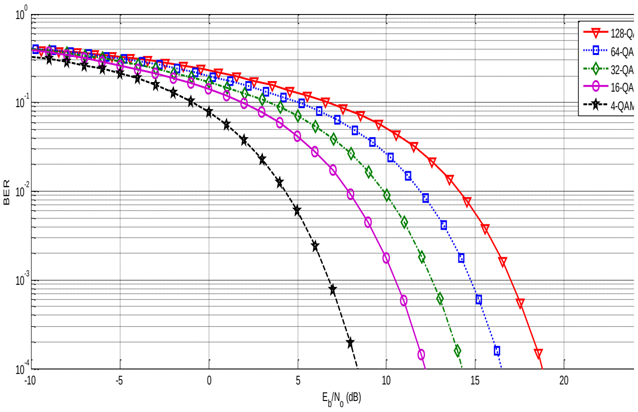

Fig.12. BER versus SNR for M-QAM where M=4, 16, 32, 64, and 128 based on (6)

$$P_b = \frac{1}{\log_2\sqrt{M}}\sum_{k=1}^{\log_2\sqrt{M}} P_b(k) \qquad (4)$$

where

$$P_b(k) = \frac{1}{\sqrt{M}}\sum_{i=0}^{(1-2^{-k})\sqrt{M}-1}\left\{(-1)^{\left\lfloor\frac{i.2^{k-1}}{\sqrt{M}}\right\rfloor}\times\left(2^{k-1} - \right.\right.$$

$i.2k-1M+12.\mathrm{erfc}2i+13\log 2M.\gamma 2M-1$
(5)

where $\gamma = (E_b/N_o)$denotes the SNR per bit, and $\lfloor x \rfloor$ denotes the largest integer to x .

Note that, for M=4, previous formula reduces to the well-known BER expression of Quadrature Phase Shift Keying (QPSK). If only the first and second terms (i=0,1) in (5) are considered, an approximate BER expression for M-ary square QAM can be obtained from (5) by neglecting the higher order terms, i.e.

$$P_b \cong \frac{\sqrt{M}-1}{\sqrt{M}\log_2\sqrt{M}}\ \mathrm{erfc}\left(\sqrt{\frac{3\log_2 M.\gamma}{2(M-1)}}\right) + \frac{\sqrt{M}-2}{\sqrt{M}\log_2\sqrt{M}}\ \mathrm{erfc}\left(3\sqrt{\frac{3\log_2 M.\gamma}{2(M-1)}}\right) \quad (6)$$

Note that the pervious formula (6) is identical to the result presented in [13]. For high SNR, the first term ($i=0$) is dominant in (5). Thus, for high SNR, the BER of M-ary square

QAM can be approximated to a certain degree of accuracy by neglecting some of the higher order terms in (5), i.e.

$$P_b \cong \frac{\sqrt{M}-1}{\sqrt{M}\log_2\sqrt{M}}\,\text{erfc}\left(\sqrt{\frac{3\log_2 M.\gamma}{2(M-1)}}\right) \qquad (7)$$

Fig. 12 shows the BER versus SNR for M-QAM where M=4, 16, 32, 64, and 128 based on (6).

V CAM PERFORMANCE UNDER NAKAGAMI-M CHANNEL

As shown in Fig. 6, the transmission rate on the point-to-point wireless channel is adaptively adjusted by utilizing an adaptive modulation scheme. In the QAM modulator block, Gray coded discrete (square and rectangular) M-ary QAM modes with M=2^n where n=2,3,…N are used for the channel adaptive scheme. The transmissions are assumed to be over a slowly varying flat-fading channel with the fading assumed in this section to follow a Nakagami-m distribution [14]. The signal at the receiver is perturbed by AWGN which is modeled as a zero-mean complex Gaussian random variable with variance *No/2* where *No* is the single-sided power spectrum density of the noise. It is assumed that perfect channel estimation is possible at the receiver and that the feedback channel is instantaneous and error free.

At the receiver, the received signal is given by $r = \alpha e + n_d$ where *e* is the transmitted signal, n_d is the AWGN and α is the Nakagami-m fading co-efficient with the probability density function (pdf) given by (8),

$$P_\alpha(\alpha) = \frac{2}{\Gamma(m)}\left(\frac{m}{\Omega}\right)^m \alpha^{2m-1}\exp\left(-\frac{m\alpha^2}{\Omega}\right) \qquad (8)$$

where m is the Nakagami fading parameter and $\Gamma(m)$ is the Gamma function defined by $\Gamma(m) = \int_0^\infty y^{m-1}\exp(-y)\,dy$ and $\Omega = E[|\alpha|^2]$, E being the expectation. Define the received instantaneous SNR as

$$\gamma = \frac{|\alpha|^2 E_S}{N_O} \qquad (9)$$

And E_S is the symbol energy. For a Nakagami-m fading channel, the pdf of γ is given by [15]

$$P_\gamma(\gamma) = \left(\frac{m}{\bar\gamma}\right)^m \frac{\gamma^{m-1}exp\left(\frac{-m\gamma}{\bar\gamma}\right)}{\Gamma(m)} \quad ,\gamma \geq 0 \qquad (10)$$

where

$$\bar\gamma = E[\gamma] = \frac{\Omega E_S}{N_O} \qquad (11)$$

The received SNR range is split into (*N + 1*) fading regions (bins), with region *n* having a corresponding mode *M$_n$*. The set $\{\gamma_n\}$ contains the lower thresholds for the *N* fading regions, calculated such that the target BER (referred to as BERo) is achieved for each *M$_n$*-QAM modulation scheme. γ_1 is set to 0 dB and $\gamma_{N+1}$to ∞. Thus when the received instantaneous SNR, γ , falls within region n $(\gamma_n \leq \gamma \leq \gamma_{n+1})$, the associated fading index n is sent back to the transmitter through a dedicated feedback channel. To avoid deep fades, no data is sent when $\gamma_1 \leq \gamma \leq \gamma_2$ (outage).

In [16] and [17], the investigation of adaptive schemes for improving the spectral efficiency of transmissions over fading channels was developed. The schemes presented are to use the principle that adaptive schemes originally designed for AWGN channels can be used over a fading channel. The adaptive schemes in [16] and [17] used the approximation expression shown in (12) for the BER of coherent M-QAM with two-dimensional Gray coding over the AWGN channel

$$P_b(\gamma) \cong 0.2\exp\left(\frac{-3\gamma}{2(M-1)}\right) \qquad (12)$$

The average BER in a slow and flat Nakagami-m fading channel is derived by averaging the error rates for the AWGN channel over the pdf of the SNR in Nakagami-m fading [15]:

$$P_b(\bar\gamma) = \int_{-\infty}^{\infty} P_b(\gamma)P_\gamma(\gamma)\,d\gamma \qquad (13)$$

$$= \int_0^\infty 0.2\exp\left(\frac{-3\bar\gamma}{2(M-1)}\right)\left(\frac{m}{\bar\gamma}\right)^m \frac{\bar\gamma^{m-1}exp\left(\frac{-m\gamma}{\bar\gamma}\right)}{\Gamma(m)}\; d\bar\gamma$$

$$= \frac{0.2}{\Gamma(m)}\left(\frac{m}{\bar\gamma}\right)^m \int_0^\infty \gamma^{m-1}exp(-\gamma\beta)\,d\gamma$$

(14)

where $\beta = \frac{3\bar\gamma+2m(M-1)}{2(M-1)\bar\gamma}$. After completing the integration and some simplification, the following expression for the average BER can be derived:

$$P_b(\bar\gamma) = 0.2\left(\frac{m}{\bar\gamma\beta}\right)^m \qquad (15)$$

The simulation results on M-QAM over a Nakagami-m fading channel shows that using the approximate expression in (15) will result in inaccuracies in an adaptive M-QAM modulation scheme over a Nakagami-m fading channel. Thus a more accurate expression for the BER performance is required in order to design the adaptive scheme. Therefore the closed-form expressions for the average SER is written below

$$P_s(\bar\gamma) = a\left\{\left(\frac{3m}{3m+2b\bar\gamma}\right)^m + \frac{1}{3}\left(\frac{2m}{2m+b\bar\gamma}\right)^m - \frac{a}{2}\left(\frac{m}{m+b\bar\gamma}\right)^m\right\}$$

(16)

and

$$P_b(\bar\gamma) = \frac{P_S(\bar\gamma)}{k} \qquad (17)$$

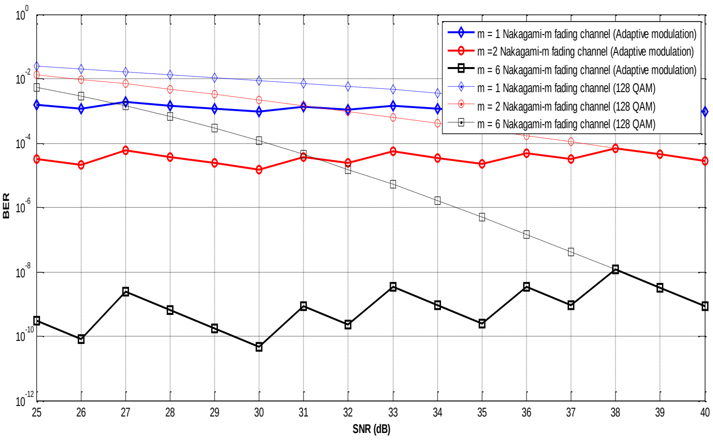

Fig.13. BER versus SNR for adaptive modulation in scenario A under Nakagami-m fading channel (m=1,2,3) and fixed 128-QAM is plot for comparison purpose

where

$$k = log_2 M \text{ bit/symbol} \qquad (18)$$

and

$$a = \left(1 - \frac{1}{\sqrt{M}}\right) \text{ and } b = \frac{3}{M-1} \qquad (19)$$

In order to simulate the performance of adaptive modulation, two different scenarios have been taken. In the first scenario, the received SNR range is split into 6 regions. M_n-QAM modulation schemes are selected where M_1=4, M_2=8, M_3=16, M_4=32, M_5=64, and M_6=128. In the second scenario, SNR range is split into 5 regions where M_1=4, M_2=16, M_3=32, M_4=64, M_5=128. The sets $\{\gamma_n\}$ are listed in Table 2 for two scenarios and the results for Nakagami-m fading channel (*m*=1,2,6) are shown in Fig. 13. BER for 128-QAM is plotting for comparison as well.

TABLE. 2 SETS $\{\gamma_n\}$ FOR TWO DIFFERENT SCENARIOS

	γ_1(dB)	γ_2(dB)	γ_3(dB)	γ_4(dB)	γ_5(dB)
Scenario A	27	31	33	36	38
Scenario B	23	25	27	29	--

TABLE. 3 SETS $\{\gamma_n\}$ FOR TWO DIFFERENT BER TARGETS

Target BER	γ_{min} (dB)		γ_1(dB)		γ_2(dB)		γ_3(dB)		γ_4(dB)	
	m=1	m=2	m=1	m =2	m =1	m=2	m =1	m=2	m=1	m=2
10^{-2}	0	12	23	18	25	20.5	27	23	29	26
10^{-3}	27.5	17.5	33	24	35	26.5	37	29	40	32
10^{-4}	37.5	22.7	42.5	29	45	31.7	47	34.5	50	37.4

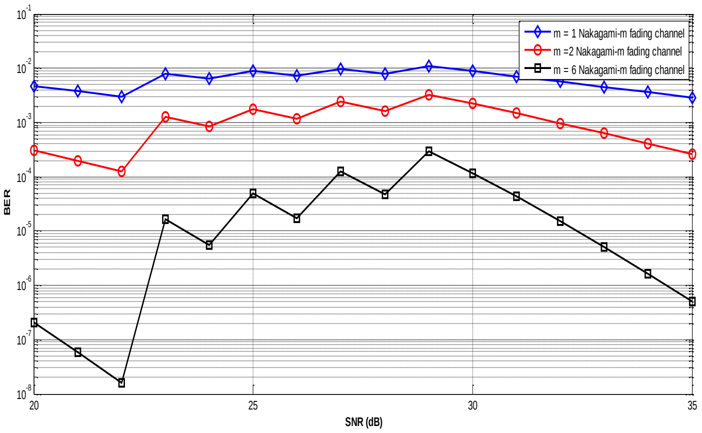

Fig.14. BER versus SNR for adaptive modulation in scenario B under Nakagami-m fading channel (m=1,2,3)

AS shown the BER of scenario A do not vary much within the designated SNR range. Furthermore, at small SNR, the BER is much lower than conventional Q-128. Moreover, at higher values of *m*, the difference between our scenario and the conventional 128-QAM is much more significant. Fig. 14 shows the BER versus SNR for Scenario B.

In order to design a good adaptive modulation, a target BER (maximum acceptable BER) should be defined and for each target BER there is an associated minimum SNR ($\gamma_{\min}$) and we suppose the transmission is cut under $\gamma_{\min}$. the received SNR range is split into 5 regions. M_n-QAM modulation schemes are selected where $M_1=4$, $M_2=16$, $M_3=32$, $M_4=64$, and $M_5=128$, The sets $\{\gamma_n\}$ are listed in Table 3 for *m*=1,2 at three different BER target (10^{-2}, 10^{-3}, and 10^{-4}), the results are shown Fig. 15 and Fig. 16.

On the other hand, the adaptive modulation enhances the spectral efficiency, SE, of overall system where SE can be defined by

$$SE = log_2 M \text{ bit/symbol} \qquad (20)$$

Fig. 17 and Fig.18 show SE of the scenarios in Table. 3 and for comparison SE of fixed 16-QAM is plotted as well.

VI CONCLUSIONS

In this paper, a novel chaotic secure communication system is presented, that is called chaotic adaptive modulation (CAM). The proposed system uses adaptive modulation technique to overcome the effects of time variant channel where random bit errors due to noise and burst errors due to fading may be occurred. This technique uses channel opportunities to maximize the throughput. The performance and limitation of the system was studied showing its advantages and drawbacks.

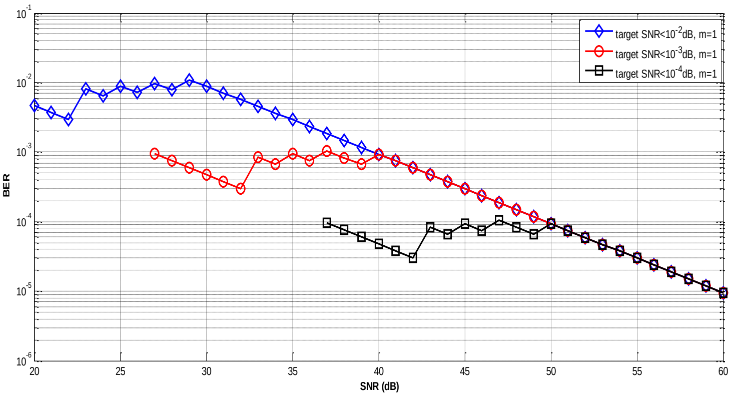

Fig.15. BER versus SNR for adaptive modulation under m=1 Nakagami-m fading channel for different BER target

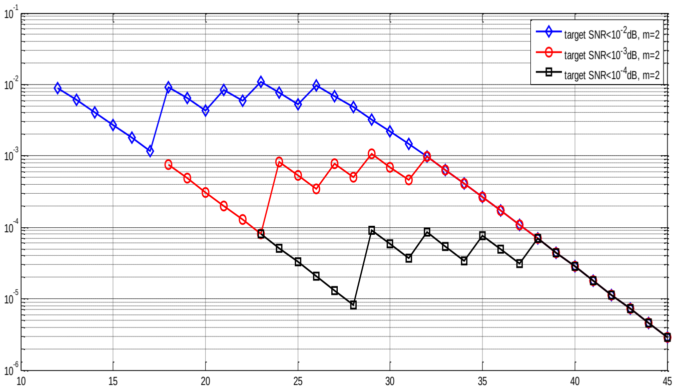

Fig.16. BER versus SNR for adaptive modulation under m=2 Nakagami-m fading channel for different BER target

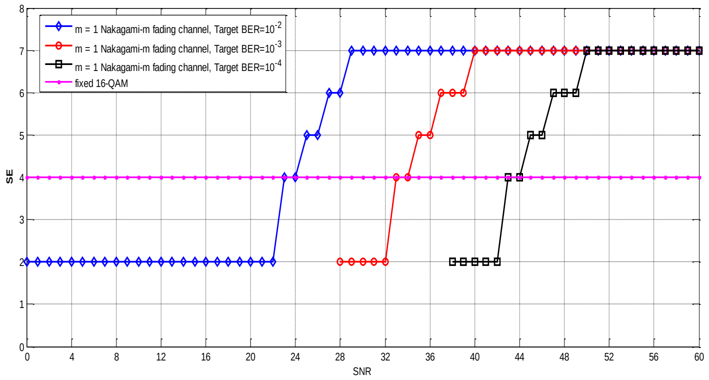

Fig.17. SE versus SNR for adaptive modulation under m=1 Nakagami-m fading channel for different BER target

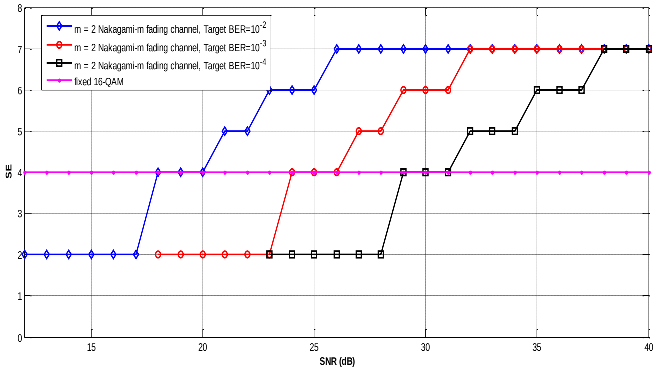

Fig.18. SE versus SNR for adaptive modulation under m=2 Nakagami-m fading channel for different BER target

The numerical simulation of the proposed system was executed by using Matlab/Simulink® platform. The randomness of QAM states (transmitted symbols) is verified through two methods 1) the NIST test and 2) the uniform probability distribution in cases of 4-QAM, 16-QAM, 32-QAM, and 64-QAM via histogram in Matlab®.

The performance of the proposed system over Nakagami-*m* fading channel was evaluated under two scenarios with SNR range is split into 5 and 6 regions. Also the performance under conditions of specific SNR (maximum acceptable BER) with SNR range is split into 5 regions. The study proved the advantages of adaptive modulation technique over fixed modulation technique.

The proposed system achieves fundamental trade-off between security and throughput in encryption based wireless communication. Furthermore, the proposed system is unsophisticated and smartly designed to simplify the transmitter and receiver circuits while the encryption and decryption processing time are short. Moreover, this work demonstrates that the proposed system can be designed under condition of maximum allowable BER using the adaptive modulation advantages.

REFERENCES

[1] G.S. Vernam. (1922). Secret signaling system, United States Patent Office, Serial No. 253962, Application filed September 13, 1918.

[2] Claude E. Shannon. (1949). Communication theory of secrecy systems, Bell System Technical Journal, vol.28, no. 4, (pp.656-715).

[3] Savo G. Glisic. (2011). Advanced wireless communications and internet: future evolving technologies, Wiley, 3rd Edition, 2011.

[4] Zhechen Zhu, and Asoke K. Nandi. (2015). Automatic modulation classification: principles, algorithms and applications, Wiley; 1 edition.

[5] Marcio Eisencraft, Romis Attux, and Ricardo Suyama. (2013). Chaotic signals in digital communications, CRC Press.

[6] C. E. Shannon. (1949). Communication theory of secrecy systems, Bell Syst. Tech. J., vol. 28, (pp. 656–715).

[7] Fabio Pareschi, Gianluca Setti, and Riccardo Rovatti. (2010). Implementation and testing of high-speed CMOS

true random number generators based on chaotic systems, IEEE Transactions on Circuits And Systems I: Regular Papers, vol. 57, no. 12, (pp. 3124-3137).

[8] Amr Sayed AbdelFattah. (2013). Performance of Wireless Chaotic Secure Communication System, Ph.D dissertation, College of Eng., Ain Shams Univ., Egypt.

[9] National Institute of Standards and Technology (NIST). (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications, Special Publication 800-22, Revision 1a, http://csrc.nist.gov/rng/

[10] Kyongkuk Cho and Dongweon Yoon. (2002). On the general BER expression of one- and two-dimensional amplitude modulations, IEEE Transactions on Communications, vol. 50, no. 7, (1074-1080).

[11] M. P. Fitz and J. P. Seymour. (1994). On the bit error probability of QAM modulation, International Journal of Wireless Information Networks, vol. 1, no. 2, (pp. 131–139).

[12] W. T. Webb and L. Hanzo. (1994). Modern quadrature amplitude modulation, IEEE Press.

[13] L. Yang and L. Hanzo. (2000). A recursive algorithm for the error probability evaluation of M-QAM, IEEE Communication Letter, vol. 4, no. 10, (pp. 304-306).

[14] Michel Daoud Yacoub, Jose Edson Vargas Bautista, and Leonardo Guerra de Rezende Guedes. (1999). On higher order statistics of the Nakagami-*m* distribution, IEEE Transactions On Vehicular Technology, vol. 48, no. 3, (pp. 790-794).

[15] Tahmid Quazi and HongJun Xu. (2011). Performance analysis of adaptive M-QAM over a flat-fading Nakagami-m channel, South Africa Journal of Science, vol. 107, no. 1, (pp. 40-46).

[16] Goldsmith AJ, Chua SG. (1997). Variable-rate variable-power MQAM for fading channels, IEEE Transactions on Communication, vol.45, no.10, (pp. 1218–1230).

[17] Goldsmith AJ, Chua SG. (1998). Adaptive coded modulation for fading channels, IEEE Transactions on Communication, vol. 46, no. 5, (pp. 595-602).