A Secure MQAM Scheme Based on Signal Constellation Hopping

Yingxian Zhang[1], Aijun Liu[1], Xiaofei Pan[1] and Zhan Ye[1]
[1] College of Communications Engineering, PLA University of Science and Technology
Nanjing, Jiangsu 210007 - China
[e-mail: zhangyingxian@126.com]
*Corresponding author: Yingxian Zhang

Received May 6, 2013; revised May 12, 2014; accepted June 5, 2014; published July 29, 2014

Abstract

In this paper, a secure multilevel quadrature amplitude modulation (MQAM) scheme is proposed for the physical layer security (PLS) of the wireless communications. In the proposed scheme, each transmitted symbol's signal constellation (SC) is hopping with the control of two unique factors: *amplitude distortion (AD) factor* and *phase hopping (PH) factor*. With unknown the two factors, the eavesdropper cannot extract effective information from the received signal. We first introduce a security metric, referred to as *secrecy gain*, and drive a lower bound on the gain that the secrecy capacity can be improved. Then, we investigate the relationship among the secrecy gain, the signal to noise power ratios (SNRs) of the main and wiretap channels, and the secrecy capacity. Next, we analyze the security of the proposed scheme, and the results indicate that the secrecy capacity is improved by our scheme. Specifically, a positive secrecy capacity is always obtained, whether the quality of the main channel is better than that of the wiretap channel or not. Finally, the numerical results are provided to prove the analytical work, which further suggests the security of the proposed scheme..

Keywords: Secure MQAM scheme, signal constellation hopping (SCH), amplitude distortion (AD) factor, phase hopping (PH) factor, secrecy gain

http://dx.doi.org/10.3837/tiis.2014.07.003

1. Introduction

In 1975, Wyner introduced a general model for the physical layer security (PLS) of communications [1], where a transmitter (Alice) sends information to a legitimate user (Bob) through the main channel. Meanwhile, the eavesdropper (Eve) can extract the information from the output signal of the wiretap channel. He proposed a security metric for the system, i.e., *secrecy capacity*, which is defined as the difference capacity of main and wiretap channel, and its general expression was further proposed in [2]. Since then, PLS has received considerable attentions [3]-[27].

In [3]-[7], authors proved that the system with multiple-input multiple-output (MIMO) channel can obtain the secrecy capacity by optimizing beam-forming [3]-[5], proper signal power allocation [6]-[7] and space-time coding [7], when the channel state information (CSI) is known. While in [8]-[12], secure cooperation communications were investigated. With known the perfect CSI, authors proposed optimal relay selection and weight schemes for different numbers of eavesdroppers and different relay strategies. In [13]-[14], authors further proved that the orthogonal frequency division multiplexing (OFDM) modulation system can also achieve the secrecy capacity by optimizing the carrier power. And in [15]-[16], the radio fingerprinting (RF) tachniques were applied to the communications authorization, where the RF feature of the received signal is utilized to detect the malicious intruders. In [17]-[19], artificial noise (AN) were explored to the PLS of the wireless communications. Authors in [17] proved that, when Alice and her helpping relays have more antennas than Eve, PLS can be guaranteed by injecting the AN at the transmitter. And authors in [18]-[19] proposed the schemes that the AN is sent by Bob or relays. The methods are both robust for their security do not depend on the feedback of CSI and the condition that Eve's antennas are less than Bob's. In addition, some researchers propose the usage of coding to achieve the maximum secrecy rate. As shown in [20]-[24], authors proved that we can utilize the existing coding schemes, e.g., low density parity check (LDPC) coding [20], network coding [21], polar coding [22]-[23] and lattice coding [24], to design constructive codes which satisfy both reliability and security conditions [1], while the secrecy rate approaches the secrecy capacity. Some researchers also investigate cryptography security enhancement schemes based on the physical layer techniques [25]-[26]. As shown in [25]-[26], the secret key can be extracted from the fading channel coefficients. Based on the difference of the main and wiretap channels, Eve cannot intercept the key. And in [27], a joint encryption, error correction and modulation scheme was proposed to improve both the security and reliability of the communications.

In deed, all the techniques in [3]-[27] have provided effective solutions for different secure communication scenarios. However, there exist some challenges for these techniques. As shown in [3]-[14], CSI is needed for transmission strategy optimization, while it is usually difficult in practice. Due to the dynamic environment, the signal RF feature is always changing, which makes it hard to extract the signal RF [15]-[16]. When AN is utilized for the security, it needs additional power to transmit AN. However, it is not desirable for some power constraint communication scenario, e.g., satellite communication. While coding schemes will lead to the decrease of transmission efficiency, as shown in [20]-[24]. When it exploits the cross-layer techniques proposed in [25]-[26], the system complexity will increase significantly.

Motivated by above observations, we propose a secure multilevel quadrature amplitude modulation (MQAM) scheme based on signal constellation hopping (SCH) in this paper. Different from traditional modulation scheme, each transmitted symbols' signal constellation

(SC) is hopping with the control of two unique factors: *amplitude distortion (AD) factor* and *phase hopping (PH) factor*, which are both generated by an AD-PH generator. At the receiver, with known the two factors, the demodulator can rebuild the correct SC. Otherwise, the receiver will get uncorrect SC and decision regions, which will lead to the demodulation failure, i.e., the communication security is guaranteed. The main contributions of this paper are summarized as follows.

1) We introduce a security metric, referred to as *secrecy gain*, and drive a lower bound on the gain that the secrecy capacity can be improved. And the relationship among the secrecy gain, the signal to noise power ratios (SNRs) of the main and wiretap channels, and the secrecy capacity is also investigated.
2) We analyze the security of our scheme and prove that, when the secrecy gain is larger enough, a positive secrecy capacity can be always obtained, whether the quality of the main channel is better than that of the wiretap channel or not. Additionally, we also discuss the anti-attack ability of the proposed scheme with a conclusion that, it is difficult to estimate AD and PH factors when it exists noise in the channel.
3) Three sets of simulations with 16QAM and 64QAM are provided to prove the analytical results, where both the main channel and the wiretap channel are assumed as additive white Gaussian noise (AWGN) channels.

The rest of the paper is organized as follows. In Section 2, we introduce the proposed scheme, and analyze the theory error performance. And in Section 3, we first propose the secrecy gain and drive a lower bound on the gain that the secrecy capacity can be improved. Then, relationship among the secrecy gain and secrecy capacity is investigated. And the anti-attack ability of the proposed scheme is also discussed. Next, in Section 4, three sets of simulations are set up to evaluate the security performance of our scheme. Finally, we make some concluding in Section 5.

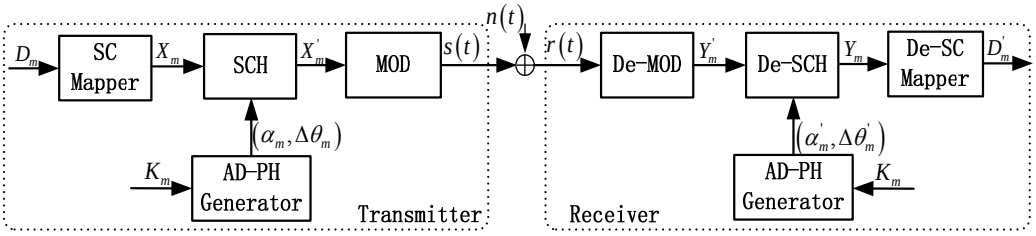


Fig.1. Block diagram of the SCH MQAM system.

2. Proposed SCH MQAM Scheme

2.1 System Model

The general ideal of our proposed scheme is to change each transmitted symbol's SC with the AD and PH factors and to map all the symbols onto hopping SCs. With unknown the AD and PH factors, the receiver cannot make correct decision on each received symbols, i.e., it fails to extract the information from the received signal. The block diagram SCH MQAM system is illustrated in **Fig.1**.

We can observe from the figure that, at the transmitter, the information bits (D_m) are first mapped onto MQAM symbols, i.e., X_m. Then, through the processing of SCH with the AD and PH factors, i.e., (α_m, $\Delta\theta_m$), we can get the transmitted SCH MQAM symbol as X_m'. Next, through modulating, the final transmitted signal $s(t)$ is given by

$$\begin{aligned} s(t) &= \sum_{m=0}^{\infty} \mathrm{Re}\left[X_m \bullet \alpha_m e^{j\Delta\theta_m} \bullet g(t-mT_s) e^{j(2\pi f_c(t-mT_s))} \right] \\ &= \sum_{m=0}^{\infty} \mathrm{Re}\left[X_m' g(t-mT_s) e^{j(2\pi f_c(t-mT_s))} \right] \\ &= \sum_{m=0}^{\infty} \mathrm{Re}\left[\alpha_m A_m e^{j(\theta_m+\Delta\theta_m)} g(t-mT_s) e^{j(2\pi f_c(t-mT_s))} \right] \\ &= \sum_{m=0}^{\infty} \alpha_m A_m g(t-mT_s) \cos\left(2\pi f_c(t-mT_s) + \theta_m + \Delta\theta_m\right), \end{aligned} \tag{1}$$

where A_m, θ_m are amplitude and phase of X_m, $g(t)$ is the shape filter, T_s is the symbol period, and f_c is the carrier frequency. For each MQAM symbol, there has

$$X_m = A_m e^{j\theta_m} = A_{mi} + jA_{mq},\ A_m = \sqrt{A_{mi}^2 + A_{mq}^2},\ \text{and}\ \theta_m = \tan^{-1}\left(A_{mq}/A_{mi}\right), \tag{2}$$

where A_{mi}, A_{mq} are the information-bearing signal amplitudes of quadrature carriers.

At the receiver, the received signal $r(t)$ will be

$$r(t) = h(t) * s(t) + n(t), \tag{3}$$

where '$*$' is the convolution, $h(t)$ is the channel impulse response, $n(t)$ is the additive Gaussian noise with power spectral density of $N_0/2$. For the AWGN channel, there has

$$h(t) \equiv 1. \tag{4}$$

From (1), (3) and (4), $r(t)$ can be written as

$$r(t) = \sum_{m=0}^{\infty} \alpha_m A_m g(t-mT_s) \cos\left(2\pi f_c(t-mT_s) + \theta_m + \Delta\theta_m\right) + n(t). \tag{5}$$

Suppose that there is no frequency and phase offsets, the received SCH MQAM symbol, denoted as Y_m', will be

$$Y_m' = r_m(\alpha_m, A_m, \theta_m, \Delta\theta_m) + n_m' = \alpha_m A_m e^{j(\theta_m+\Delta\theta_m)} + n_m', \tag{6}$$

where n_m' is a complex i.i.d Gaussian variable with mean 0 and variance N_0.

Finally, through the processing of the de-SCH with the synchronization AD and PH factors, i.e., $(\alpha_m', \Delta\theta_m')$, the received MQAM symbol, denoted as Y_m, is given by

$$Y_m = Y_m' \alpha_m' e^{j\Delta\theta_m'} = \alpha_m' \alpha_m A_m e^{j(\theta_m+\Delta\theta_m+\Delta\theta_m')} + n_m' \alpha_m' e^{j\Delta\theta_m'}. \tag{7}$$

Then, we can get the estimated information bits (D_m') based on Y_m and the decision rules of the MQAM.

It is noticed from the above presentation that, the security of our scheme is closely related to $(\alpha_m, \Delta\theta_m)$ and $(\alpha_m', \Delta\theta_m')$, which are all obtained from the AD-PH generator. In this paper, we assume that the AD-PH generator is driven by a random sequence, and its mth element is denoted as K_m. And it is also assumed that K_m is known to both Alice and Bob but unknown to Eve.

Remark 1: The role of K_m in our scheme is the same as that of the secret key in the cryptography scheme. While in this paper, we do not introduce how to keep K_m secret in detail.

2.2 Signal Constellation Hopping

In this subsection, we introduce how to make the MQAM symbols' SC hopping with the control of the AD and PH factors. As shown in **Fig.2**, with the modification of $(\alpha_m, \Delta\theta_m)$, i.e.,

$X_m^{'} = \alpha_m A_m e^{j(\theta_m + \Delta\theta_m)}$, the constellation of a 16QAM symbol is changed. Since the AD and PH factors are both unique to each 16QAM symbol, its constellation will be different. Hence, when the symbol number increases, the transmitted SC will be fuzzy, correspondingly, just like the SC is hopping, as shown in **Fig.3**.

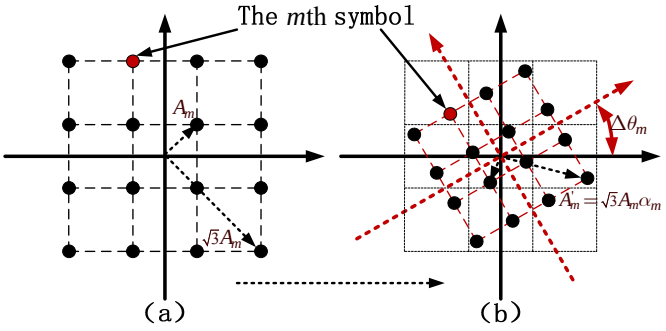


Fig.2. (a) Original 16QAM symbol constellation. (b) SCH 16QAM symbol constellation.

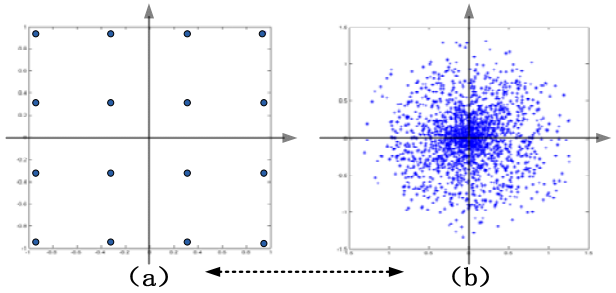


Fig.3. (a) Original 16QAM SC. (b) Fuzzy 16QAM SC.

2.3 Error Performance

In this subsection, we analyze the error performance of the legitimate receiver (Bob) and the eavesdropper (Eve), where both the main channel and the wiretap channel are assumed as AWGN channels, and their noise samples are denoted as n_m^B and n_m^E, respectively. In addition, we refer the synchronization AD and PH factors of Bob and Eve to be different as $(\alpha_m^{B'}, \Delta\theta_m^{B'})$ and $(\alpha_m^{E'}, \Delta\theta_m^{E'})$.

Since the AD and PH factors are known to Bob, we have

$$\alpha_m^{B'}\alpha_m = 1 \text{ and } \Delta\theta_m + \Delta\theta_m^{B'} = 0. \tag{8}$$

According to (7) and (8), Bob's received symbol, denoted as Y_m^B, is given by

$$Y_m^B = A_m e^{j(\theta_m)} + n_m^B \alpha_m^{B'} e^{j\Delta\theta_m^{B'}} = A_m e^{j(\theta_m)} + n_m^{B'}, \tag{9}$$

where $n_m^{B'}$ is the equivalent noise sample of the Bob's channel.

Suppose that Eve know Alice's signal procesing method, and she will try to recover the SC with $(\alpha_m^{E'}, \Delta\theta_m^{E'})$. Therefore, from (7), Eve's received symbol, denoted as Y_m^E, will be given by

$$Y_m^E = \alpha_m^{E'}\alpha_m A_m e^{j\left(\theta_m + \Delta\theta_m + \Delta\theta_m^{E'}\right)} + n_m^E \bullet \alpha_m^{E'} e^{j\Delta\theta_m^{E'}} = \beta A_m e^{j(\theta_m + \phi)} + n_m^{E'}, \tag{10}$$

where $n_m^{E'}$ is the equivalent noise sample of the Eve's channel, and β, ϕ are the estimation offsets of the AD and PH factors, i.e.,

$$\beta = \alpha_m^{E'} \alpha_m \text{ and } \phi = \Delta\theta_m + \Delta\theta_m^{E'}, \tag{11}$$

In order to analyze the error performance of Bob and Eve, we first introduce the statistic characteristics of $n_m^{B'}$ and $n_m^{E'}$ with the following theorem.

***Theorem 1*:** Suppose that the random variables X', Y and θ are mutual independent, and $X' \sim N(0, N_0)$, $Y \sim U(0, A)$, $\theta \sim U(0, 2\pi)$. The complex variable $V' = X' Y e^{j\theta}$ will be a Gaussian variable with mean 0 and variance $A^2 N_0$.

Proof: The proof of this theorem is implemented in Appendix-A.

Theorem 1 shows that both $n_m^{B'}$ and $n_m^{E'}$ follow the Gaussian distribution. Hence, we can exploit the analysis method presented in 0 to evaluate the error performance of Bob and Eve.

It is shown in 0 that, the symbol error rate (SER) of a digital modulation scheme is equal to the average pairwise error probability, i.e., the probability of event that the transmit symbol is X_m but detected symbol is X_n.

According to (9), the pairwise error probability of Bob, denoted as $p_{m\to n}^B$, is given by

$$p_{m\to n}^B = P\left[\left\|Y_m^B - A_m e^{j(\theta_m)}\right\| > \left\|Y_m^B - A_n e^{j(\theta_n)}\right\|\right] = P\left[\left\|n_m^{B'}\right\| > \left\|A_m e^{j(\theta_m)} + n_m^{B'} - A_n e^{j(\theta_n)}\right\|\right] \tag{12}$$

To simplify (12), we define three vectors as $\mathbf{n} = (n_1, n_2)$, $\mathbf{s}_m = (s_{m1}, s_{m2})$ and $\mathbf{s}_n = (s_{n1}, s_{n2})$, where $n_1 = \mathrm{Re}[n_m^{B'}]$, $n_2 = \mathrm{Im}[n_m^{B'}]$, $s_{m1} = \mathrm{Re}[A_m e^{j(\theta_m)}]$, $s_{m2} = \mathrm{Im}[A_m e^{j(\theta_m)}]$, $s_{n1} = \mathrm{Re}[A_n e^{j(\theta_n)}]$, $s_{n2} = \mathrm{Im}[A_n e^{j(\theta_n)}]$. Then, (12) can be written as

$$p_{m\to n}^B = P\left[\mathbf{n}(\mathbf{s}_n - \mathbf{s}_m) > d_{mn}^2/2\right], \tag{13}$$

where d_{mn} is the Euclidean distance of X_m to X_n, and $\mathbf{n}(\mathbf{s}_n - \mathbf{s}_m)$ follows Gaussian distribution with mean 0 and variance $d_{mn}^2 A^2 N_0/2$. Therefore, the SER of Bob will be

$$p_e^B = \frac{1}{M}\sum_{m=1}^{M}\sum_{\substack{1\le n\le M \\ n\ne m}} Q\left(\sqrt{d_{mn}^2/2A^2N_0}\right). \tag{14}$$

And from (10), the pairwise error probability of Eve, denoted as $p_{m\to n}^E$, is given by

$$p_{m\to n}^E = P\left[\left\|\beta A_m e^{j(\theta_m+\phi)} + n_m^{E'} - A_m e^{j(\theta_m)}\right\| > \left\|\beta A_m e^{j(\theta_m+\phi)} + n_m^{E'} - A_n e^{j(\theta_n)}\right\|\right]. \tag{15}$$

Based on the similar simplification as (12), we can get the SER of Eve, i.e.,

$$p_e^E(\beta,\phi) = \frac{1}{M}\sum_{m=1}^{M}\sum_{\substack{1\le n\le M \\ n\ne m}} Q\left(\left|\left(d_{en}^2 - d_{em}^2\right)/2\right| \Big/ \sqrt{\left(d_{em}^2 + d_{en}^2\right)A^2N_0/2}\right), \tag{16}$$

where d_{em}, d_{en} are the Euclidean distances of $\beta A_m e^{j(\theta_m+\phi)}$ to X_m and X_n, respectively, and $d_{en}^2 - d_{em}^2$, $d_{en}^2 + d_{em}^2$ are obtained by

$$d_{en}^2 - d_{em}^2 = A_m^2 - A_n^2 - 2\beta A_m^2\cos\phi + 2\beta A_m A_n\cos(\theta_m + \phi - \theta_n), \tag{17}$$

$$d_{en}^2 + d_{em}^2 = 2\beta^2 A_m^2 + \left(A_m^2 + A_n^2\right) - 2\beta A_m\left[A_m\cos\phi + A_n\cos(\theta_m + \phi - \theta_n)\right]. \tag{18}$$

It is noticed from (16)-(18) that the SER of Eve depends on β, ϕ. We assume that β and ϕ both follow the uniform distribution, i.e., $\beta \sim U(0, T_0)$ and $\phi \sim U(0, 2\pi)$. Then, the average SER of Eve will be

$$p_e^{EAV} = \iint p_e^E(\beta,\phi)/(2\pi T_0)\,d\beta d\phi, \tag{19}$$

where T_0 is the maximum estimation offset of the AD factor.

3. Security Analysis

In this section, we analyze the security of the proposed scheme, in which the secrecy gain is introduced and the secrecy capacity is investigated. Additionally, we also discuss the anti-attack ability of our scheme.

3.1 Secrecy Gain

It is proven in [2] that the secrecy capacity of the wiretap system depends the SNR difference between the main channel and wiretap channel, which are both considered as AWGN channels. We can observe from (14) and (16) that the minimum Euclidean distance of transmitted symbol is changed by the proposed scheme, just as the SNR of channel has been modified. To quantify this "modified" SNR, here, we introduce a metric, referred to as *secrecy gain*, and its definition is given as follows.

Definition 1*:** Let SNR_B, SNR_E be the actual SNRs of the main and wiretap channel, and $SNR_B^{'}$, $SNR_B^{'}$ be their ***equivalent SNRs through the processing of the PLS technique. Suppose that $SNR_B^{'}/SNR_B = \gamma_B$, $SNR_E^{'}/SNR_E = \gamma_E$, the secrecy gain is defined as $\gamma_s = \gamma_B/\gamma_E$.

According to above definition and (14), (16), we can obtain the secrecy gain of our scheme as

$$\gamma_s = \frac{1}{M(M-1)}\sum_{m=1}^{M}\sum_{\substack{1\le n\le M\\ n\ne m}} d_{mn}^2\left(d_{em}^2+d_{en}^2\right)\Big/\left(d_{en}^2-d_{em}^2\right)^2. \tag{20}$$

Substituting (17) and (18) into (20), we have

$$\gamma_s = \frac{1}{M(M-1)}\sum_{m=1}^{M}\sum_{\substack{1\le n\le M\\ n\ne m}} \frac{\left(A_m^2+A_n^2-2A_mA_n\cos(\theta_m-\theta_n)\right)\left(2\beta^2A_m^2+\left(A_m^2+A_n^2\right)-2\beta A_m\left[A_m\cos\phi+A_n\cos(\theta_m+\phi-\theta_n)\right]\right)}{\left(A_m^2-A_n^2-2\beta A_m^2\cos\phi+2\beta A_mA_n\cos(\theta_m+\phi-\theta_n)\right)^2}. \tag{21}$$

For the 4QAM, the secrecy gain will be

$$\gamma_{s,M=4} = \frac{\beta^2+1-\beta(\cos\phi-\sin\phi)}{\beta^2(1-\sin 2\phi)}. \tag{22}$$

Furthermore, when $M\to\infty$, there has

$$\lim_{M\to\infty}\gamma_s = \lim_{\substack{\theta_m-\theta_n\to 0\\ A_m-A_n\to 0}}\gamma_s = \infty. \tag{23}$$

Additionally, from (19), (20), we can get the average secrecy gain as

$$\gamma_s^{AV} = \frac{1}{M(M-1)}\sum_{m=1}^{M}\sum_{\substack{1\le n\le M\\ n\ne m}}\iint d_{mn}^2\left(d_{em}^2+d_{en}^2\right)\Big/\left(2\pi T_0\left(d_{en}^2-d_{em}^2\right)^2\right)d\beta d\phi \tag{24}$$

We notice from **Definition 1** that the security of the PLS technique can be measured via its secrecy gain. To elaborate this point, we introduce the following theorem to give a lower bound on the secrecy gain that the secrecy capacity can be improved.

***Theorem 2*:** If the secrecy gain satisfy $\gamma_s > 1$, the secrecy capacity of the wiretap system can be improved.

Proof: The proof of this theorem is implemented in Appendix-B.

Based on (22), (23) and **Theorem 2**, we can conclude that the secrecy capacity of the wiretap system can be improved by the proposed secure MQAM scheme.

3.2 Secrecy Capacity

It is shown in [2] that, the secrecy capacity of the AWGN wiretap system is given by

$$C_s = \left(\log\left(1+\mathrm{SNR}_B\right)-\log\left(1+\mathrm{SNR}_E\right),0\right)^+ \tag{25}$$

Therefore, from (14), (16) and (25), we can obtain the secrecy capacity of our scheme as

$$C_s(\beta,\phi)=\frac{1}{M(M-1)}\sum_{m=1}^{M}\sum_{\substack{1\le n\le M\\ n\ne m}}\left(\log\left(1+\frac{1}{A^2}\mathrm{SNR}_B\right)-\log\left(1+\frac{\left(d_{en}^2-d_{em}^2\right)^2}{A^2 d_{mn}^2\left(d_{em}^2+d_{en}^2\right)}\mathrm{SNR}_E\right),0\right)^+ \tag{26}$$

Then, the average secrecy capacity will be

$$C_s^{AV}=\iint C_s(\beta,\phi)/(2\pi T_0)\,d\beta d\phi \tag{27}$$

We notice from (26), (27) that the average secrecy capacity of the proposed scheme depends on its secrecy gain and SNR_B, SNR_E. To elaborate the relationship among them, here, we introduce another theorem as follows.

Theorem 3: When the secrecy gain and SNR_B, SNR_E satisfy the condition of $\gamma_s SNR_B > SNR_E$, a positive secrecy capacity can be achieved.

Proof: The proof of this theorem is implemented in Appendix-C.

Theorem 3 shows that, when the secrecy gain is large enough, a positive secrecy capacity can be always obtained, even SNR_E is larger than SNR_B. Hence, we can conclude from (23) that our SCH MQAM scheme can achieve a positive secrecy capacity.

3.3 Anti-Attack Ability

It is noticed from the previous subsections that the security of our scheme depends on the assumption that Eve is unknown about the AD and PH factors. To achieve this goal, we exploit an AD-PH generator driven by a random sequence to generate these factors. In general, the driven sequence can be obtained from the coefficients of the main channel [25]-[26], or from a homogenous, stationary and acyclic sequence. For the former case, Eve needs to know the CSI of the main channel, which is difficult in practice. While for the latter case, Eve needs to estimate the whole acyclic sequence, and it is more difficult. In fact, even the driven sequence is obtained from a periodical sequence, our scheme is still security. The reason is that, due to the existence of the channel noise, it cannot accurately estimate the AD and PH factors. Here, we take the estimation of AD sequence for example, as shown in **Fig.4**.

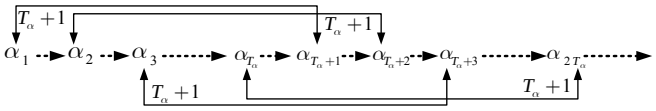


Fig.4. Estimation of AD factor sequence, and T_α is the sequence period.

We can observe from **Fig.4** that, with accurate AD factors, we can estimate the AD sequence correctly by

$$\alpha_1=\alpha_{T_\alpha+1},\alpha_2=\alpha_{T_\alpha+2},\alpha_3=\alpha_{T_\alpha+3},\cdots,\alpha_{T_\alpha}=\alpha_{2T_\alpha}. \tag{28}$$

Though it needs long time to observe the AD factor sample. However, with the noised AD factors, there may exists

$$\alpha_1\ne\alpha_2\ne\alpha_3\ne\cdots\ne\alpha_{T_\alpha}\ne\alpha_{T_\alpha+1}\ne\alpha_{T_\alpha+2}\ne\alpha_{T_\alpha+3}\ne\cdots\ne\alpha_{2T_\alpha}\ne\cdots, \tag{29}$$

which means that it is impossible to estimate the AD sequence accurately. Hence, we can conclude that our proposed scheme is robust for Eve's passive attacking.

4. Numerical Results

In this section, three sets of simulations are set up to evaluate the performance of our scheme. In these simulations, 16QAM and 64QAM are exploited, both the main and wiretap channels are assumed as AWGN channels, the maximum value of β is set to 1,i.e., $T_0 = 1$.

4.1 Simulations for Secrecy Gain

In the first set, we investigate relationship between the secrecy gain and β, ϕ, where the results are shown in **Fig.5**. It is noticed from the figure that, the secrecy gain of SCH 16QAM scheme is larger than 10dB. Specifically, when $\beta < 0.1$, the secrecy gain is more than 30dB. Even β is close to 1, the positive secrecy gain still exists, i.e., 12.5dB. In addition, **Table 1** provides the average secrecy gains of the SCH 16QAM and SCH 64QAM schemes. We can observe that the average secrecy gains of the two schemes are both larger than 450dB.

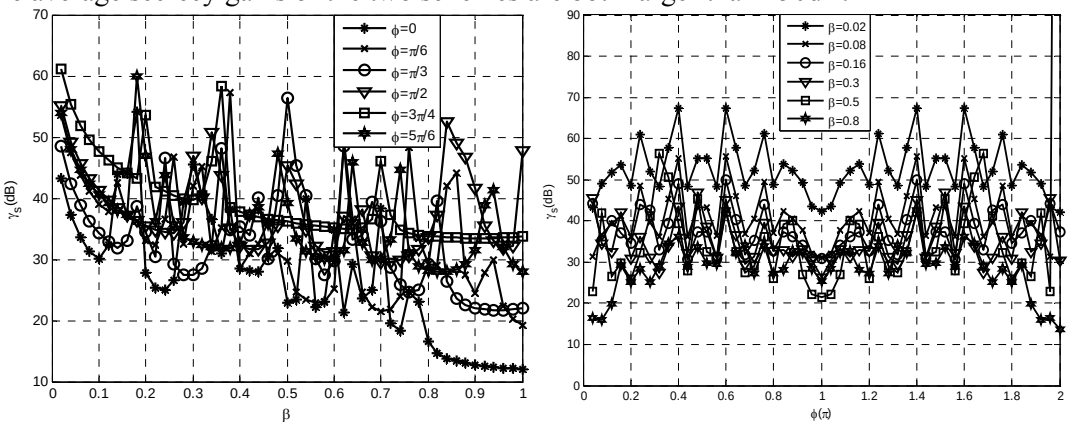


Fig.5. Secrecy gain of the SCH 16QAM scheme with different β and ϕ .

Table 1. Secrecy Gains of SCH 16QAM and SCH 64QAM Schemes

Modulation		Average Secrecy Gain(dB)
MQAM	16QAM	458.7506
	64QAM	466.7669

4.2 Simulations for Secrecy Capacity

In the second set, we first investigate the relationship between the secrecy capacity and β, ϕ, where the results are shown in **Fig.6**. It is assumed that $SNR_B = SNR_E = 6dB$, we know from (25) that, with the original MQAM scheme, the secrecy capacity will be zero in this case. However, it is noticed from **Fig.6** that, there exists a positive secrecy capacity with the SCH 16QAM scheme. Specifically, even β is close to 1 and ϕ is close to 0, the positive secrecy capacity still exists, e.g., when $\phi = 0.04\pi$, $\beta = 1$, the secrecy capacity is 0.048, and when $\beta = 0.02$, $\phi = 2\pi$, it will be 0.435.

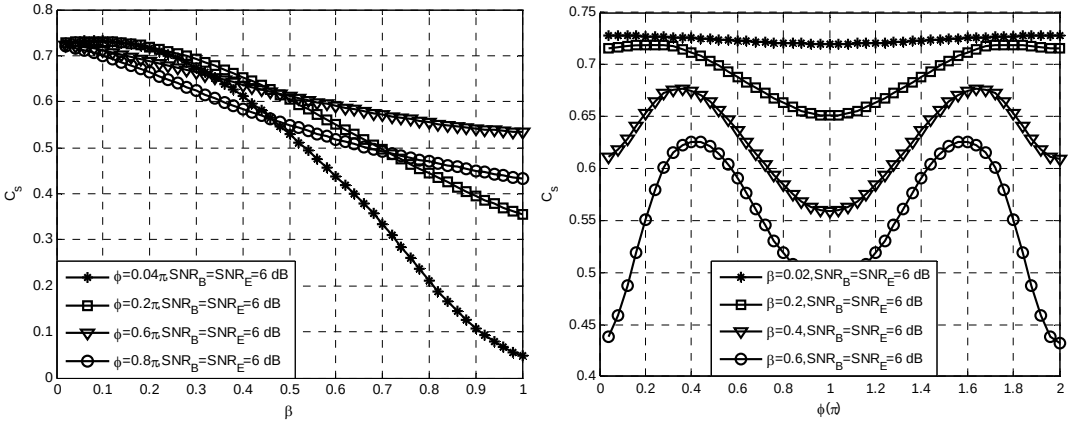
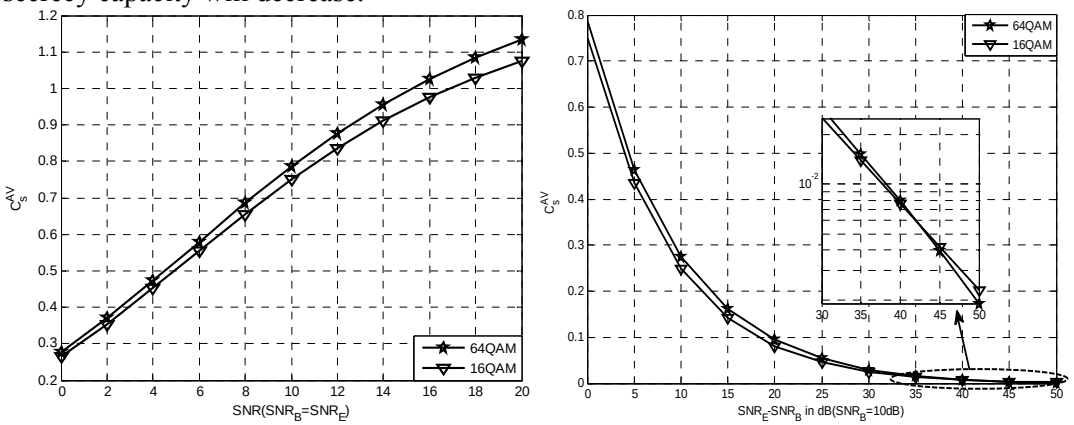


Fig.6. Secrecy capacity of the SCH 16QAM scheme with different β and ϕ .

Then, we explore the average secrecy capacities of the SCH 16QAM and SCH 64QAM schemes with $SNR_E = SNR_B$ and $SNR_E > SNR_B$, where the results are illustrated in **Fig.7**. We observe from the figure that, the average secrecy capacities of two schemes are both larger than 0.27. When $SNR_E = SNR_B = SNR > 0$ dB, the average secrecy capacities are increasing with SNR. It is also noticed that, even $SNR_E > SNR_B$, there still exists a positive secrecy capacities for the two schemes, e.g., when $SNR_E - SNR_B$ is equal to 50dB, the corresponding secrecy capacities are 0.0022 and 0.0018, respectively. And when $SNR_E - SNR_B$ increases, the secrecy capacity will decrease.



(a) $SNR_E = SNR_B$ (b) $SNR_E > SNR_B$

Fig.7. Average secrecy capacities of SCH 16QAM and SCH 64QAM schemes.

4.3 Simulations for Error Performance

In the third set, we first investigate the error performance of our scheme via bit error rate (BER), where the results are shown in **Fig.8**. It is noticed from the figure that, when SC is not hopping or the AD and PH factors are exactly synchronized, the BER is almost equal to the theory value. However, when the factors are not synchronized, the BER is around 0.13, which means that the receiver cannot extract the information. In addition, to evaluate the robust of our scheme, we also consider the case that Eve can get partial AD and PH factors. We notice that, even the ratio of the factors obtained by Eve is high to 60%, its BER is still close to the case that the factors are not synchronized.

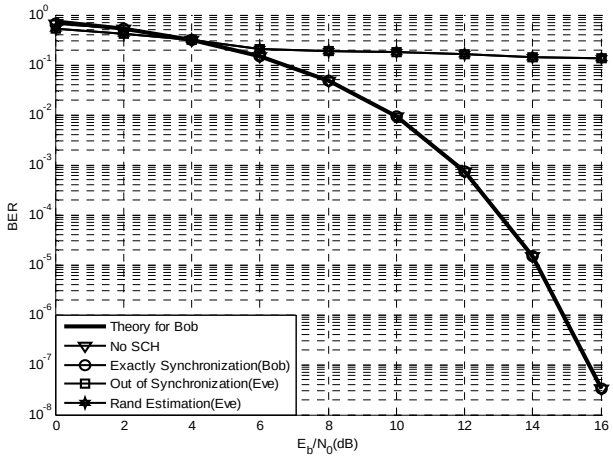


Fig.8. BER comparison among the SCH 16QAM scheme with different cases.

Then, we explore the theory bounds on the SERs of the SCH 16QAM and SCH 64QAM schemes without the AD and PH factors, where the results are shown in **Fig.9**. It is noticed from the figure that, when SNR is less than 65 dB, the SER is increasing with SNR. Otherwise, it will keep at around 0.01, which indicates the security of the SCH MQAM scheme.

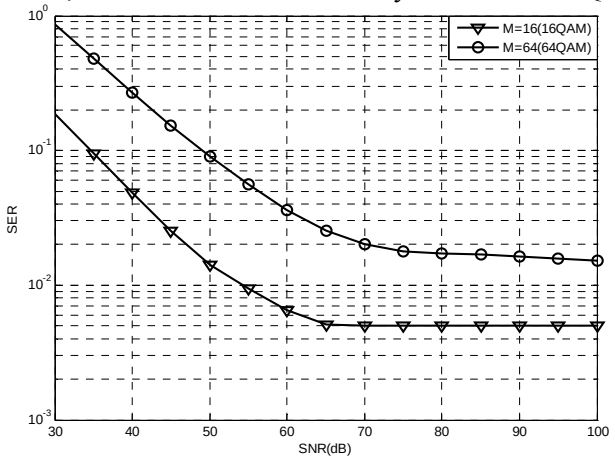


Fig.9. Bounds on the SERs of the SCH MQAM scheme without the AD and PH factors.

5. Conclusion

In this paper, a secure MQAM scheme was proposed for the PLS of the wireless communications. In our scheme, each transmitted symbol's SC was hopping with the control of two unique factors: amplitude distortion factor and phase hopping factor. With unknown those two factors, the eavesdropper could not extract the information from the received signal. We first introduced a security metric, i.e., secrecy gain, and drove a lower bound on the gain that the secrecy capacity can be improved. Then, we investigated the relationship among the secrecy gain, the SNRs of the main and wiretap channels, and the secrecy capacity. The analytical and simulation results showed that the secrecy capacity can be improved by our scheme. Specifically, a positive secrecy capacity can be always obtained, whether the quality of the main channel is better than that of the wiretap channel or not, which indicates the

security of our scheme.

Finally, One important point should be noted that, the security of our scheme is closely related to the security of the driven sequence of the AD-PH generator. While in this paper, we did not introduce the detailed methods to generate the driven sequence and to keep it secret. Hence, the research on the driven sequence should be further conducted.

Appendix

A. Proof of Theorem 1

Let X and V be the real parts of $X^{'}$ and $V^{'}$. Suppose that the probability density functions (PDFs) of X and Y are

$$f_X(x)=\frac{1}{\sqrt{\pi N_0}}e^{-\frac{x^2}{N_0}},\ \text{and}\ f_Y(y)=\begin{cases}\dfrac{1}{A}, & y\in(0,A)\\ 0, & \text{others}\end{cases}. \tag{30}$$

Since $\theta\sim U(0,2\pi)$, the PDF of $z=\sin\theta$ will be

$$f_z(z)=\begin{cases}\dfrac{1}{\pi\sqrt{1-z^2}}, & z\in(-1,1)\\ 0, & \text{others}\end{cases}. \tag{31}$$

To prove **Theorem 1**, we need the PDF of $V=XYZ$, which can be obtained by its cumulative distribution function (CDF), i.e,

$$F_V(v)=P(V\le v)=P(XYZ\le v)=\iiint\limits_{\substack{XYZ\le v\cap z\in(-1,1)\\ \cap y\in(0,A)\cap x\in(-\infty,+\infty)}}\frac{e^{-\frac{x^2}{N_0}}}{A\pi\sqrt{\pi N_0}\sqrt{1-z^2}}dxdydz \tag{32}$$

Through a complexity derivation, we obtain

$$F_V(v)=\begin{cases}\displaystyle\int_{-\infty}^{v/A}\frac{e^{-\frac{x^2}{N_0}}}{\sqrt{\pi N_0}}dx+2\bullet\int_{-1}^{0}\frac{e^{-\frac{v^2}{N_0A^2u^2}}}{\pi\sqrt{\pi N_0}}\left(\arcsin u\text{-}u\left(\ln|u|-\ln\left(1+\sqrt{1-u^2}\right)\right)\right)\left(\frac{-vdu}{Au^2}\right), & v\le 0\\ \displaystyle\int_{0}^{v/A}\frac{e^{-\frac{x^2}{N_0}}}{\sqrt{\pi N_0}}dx+2\bullet\int_{1}^{0}\frac{e^{-\frac{v^2}{N_0A^2u^2}}}{\pi\sqrt{\pi N_0}}\left(\arcsin u\text{-}u\left(\ln|u|-\ln\left(1+\sqrt{1-u^2}\right)\right)\right)\left(\frac{-vdu}{Au^2}\right), & v>0\end{cases} \tag{33}$$

It is easy to prove that the second part of (33) approaches to 0 for any v, A, N_0, u. Hence, we can get the PDF of V, i.e., $f_V(v)=e^{-v^2/N_0A^2}/A\sqrt{\pi N_0}$, which indicates that V is a Gaussian variable with mean 0 and variance $A^2N_0/2$. Hence, $V^{'}$ will be a complex Gaussian variable with mean 0 and variance A^2N_0.

B. Proof of Theorem 2

To prove **Theorem 2**, we first define a function as

$$f(x,y)=(1+Ax)(1+y)-(1+x)(1+By), A>0, B>0, x>0, y>0. \tag{34}$$

And if $A=B$, there has

$$f(x,y)=(1+Ax)(1+y)-(1+x)(1+By)=-A(x-y)^2\le 0. \tag{35}$$

While if $A \neq B$, we can obtain the stationary point of $f(x,y)$ as

$$\begin{cases} \dfrac{\partial f}{\partial x} = A(1+y) - (1+By) = A - 1 + (A-B)y = 0 \\ \dfrac{\partial f}{\partial y} = (1+Ax) - B(1+x) = 1 - B + (A-B)x = 0 \end{cases} \Rightarrow \begin{cases} x_0 = \dfrac{B-1}{A-B} \\ y_0 = \dfrac{1-A}{A-B} \end{cases}. \tag{36}$$

Since $f(x,y) > f(x_0,y_0)$, in order to ensure $f(x,y) > 0$ always satisfied for any x, y, there must has

$$f(x_0,y_0) = x_0 y_0 (A-B) > 0 \Rightarrow A > B. \tag{37}$$

Therefore, when $\gamma_B > \gamma_E$, we have

$$\log(1+\gamma_B \mathrm{SNR}_B) - \log(1+\gamma_E \mathrm{SNR}_E) > \log(1+\mathrm{SNR}_B) - \log(1+\mathrm{SNR}_E). \tag{38}$$

That is to say, when $\gamma_s > 1$, the secrecy capacity is improved.

C. Proof of Theorem 3

When a positive secrecy capacity exists, we must have $C_s > 0$. According to **Definition 1** and (25), there has

$$\begin{aligned} \log(1+\gamma_B \mathrm{SNR}_B) - \log(1+\gamma_E \mathrm{SNR}_E) &= \log\left((1+\gamma_B \mathrm{SNR}_B)/(1+\gamma_E \mathrm{SNR}_E)\right) \\ &= \log\left(\frac{1/\gamma_E + \gamma_B/\gamma_E \,\mathrm{SNR}_B}{1/\gamma_E + \mathrm{SNR}_E}\right) = \log\left(\frac{1/\gamma_E + \gamma_s \mathrm{SNR}_B}{1/\gamma_E + \mathrm{SNR}_E}\right) > 0 \end{aligned}. \tag{39}$$

Therefore, it is easy to obtain the conclusions of **Theorem 3** from (39), i.e.,

$$\frac{1/\gamma_E + \gamma_s \mathrm{SNR}_B}{1/\gamma_E + \mathrm{SNR}_E} > 1 \Rightarrow \gamma_s \mathrm{SNR}_B > \mathrm{SNR}_E. \tag{40}$$

References

[1] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, January, 1975. Article (CrossRef Link)

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transaction on Information Theory*, vol. 24, no. 3, pp. 339-348, May, 1978. Article (CrossRef Link)

[3] H. Kim and J. D. Villasenor, "Secure MIMO communications in a system with equal numbers of transmit and receive antennas," *IEEE Communications Letters*, vol. 12, no. 5, pp. 386-388, May, 2008. Article (CrossRef Link)

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-part I:The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088-3014, July, 2010. Article (CrossRef Link)

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-part II: The MIMOME Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515-5532, November, 2010. Article (CrossRef Link)

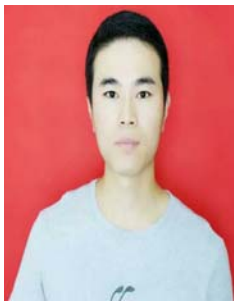
[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel", *IEEE Transaction on Information Theory*, vol. 57, no. 8, pp. 4961-4972, August, 2011. Article (CrossRef Link)

[7] S. Yan, N. Yang, R. Malaney and J. Yuan, "Transmit antenna selection with alamouti coding and power allocation in MIMO wiretap Channels," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1656-1667, March, 2014. Article (CrossRef Link)

[8] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. of 46th Annual Allerton Conf. on Communication, Control, and Computing*, pp. 1132-1138, Sept. 23-26, 2008. Article (CrossRef Link)

[9] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Amplify-and-Forward based cooperation for secure wireless communications," in *Proc. of IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, pp. 2613-2616, Apr. 19-24, 2009. Article (CrossRef Link)
[10] A. Mukherjee, "Imbalanced beam-forming by a multi-antenna source for secure utilization of an untrusted Relay," *IEEE Communications Letters*, vol. 17, no. 7, pp. 1309-1312, July, 2013. Article (CrossRef Link)
[11] J. Deng, R. Zhang, L. Song, Z. Han and B. Jiao, "Truthful mechanisms for secure communication in wireless cooperative system," *IEEE Transactions on Wireless Communications*, vol. 12, no. 9, pp. 4236-4245, September, 2013. Article (CrossRef Link)
[12] Y. Zou, X. Wang and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099-2111, October, 2013. Article (CrossRef Link)
[13] F. Renna, N. Laurenti and H. V. Poor, "Physical layer secrecy for OFDM systems," in *Proc. of European Wireless Conference*, pp. 782-789, Apr. 12-15, 2010. Article (CrossRef Link)
[14] X. Wang, M. Tao, J. Mo and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 693-702, September, 2011. Article (CrossRef Link)
[15] A. A. Tomko, "Physical-layer intrusion detection in wireless networks," in *Proc. of IEEE Military Communication Conference*, pp. 1-7,Oct. 23-25, 2006. Article (CrossRef Link)
[16] P.-S. Murvay and B. Groza, "Source identification using signal characteristics in controller area networks," *IEEE Signal Processing Letters*, vol. 21, no. 4, pp. 395-399, April, 2014. Article (CrossRef Link)
[17] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on wireless communications*, vol.7, no.6, pp.2180-2189, June, 2008. Article (CrossRef Link)
[18] W. Li, M. Ghogho, B. Chen and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628-1631, October, 2012. Article (CrossRef Link)
[19] Z. Ding, Z. Ma and P. Fan , "Asymptotic studies for the impact of antenna selection on secure Two-Way relaying communications with artificial noise," *IEEE Transactions on Wireless Communications*, vol. 13, no. 4, pp. 2189-2203, April, 2014. Article (CrossRef Link)
[20] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933-2945, August, 2007. Article (CrossRef Link)
[21] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1124-1135, February, 2011. Article (CrossRef Link)
[22] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428-6443, October, 2011. Article (CrossRef Link)
[23] E. Sasoglu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *Proc. of 2013 IEEE International Symposium on Information Theory (ISIT 2013)*, pp. 1117-1121, July, 2013. Article (CrossRef Link)
[24] Y. Yan, L. Liu and C. Ling, "Polar lattices for strong secrecy over the mod-Λ Gaussian wiretap channel," arXiv:1401.4532, January, 2014. Article (CrossRef Link)
[25] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe and Narayan, "Information- theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240-254, June, 2010. Article (CrossRef Link)
[26] G. R. Tsouri and D. M. Wagner, "Threshold constraints on symmetric key extraction from Rician fading estimates," *IEEE Transactions on Mobile Computing*, vol. 12, no. 12, pp. 2496-2506, December, 2013. Article (CrossRef Link)
[27] O. Adamo, E. Ayeh and M. Varanasi, "Joint encryption error correction and modulation (JEEM) scheme," in *Proc. of IEEE International Workshop Technical Committee on Communication Quality and Reliability*, pp. 1-5, May 15-17, 2012. Article (CrossRef Link)

[28] J. G. Proakis, *Digital Communications*, 5th Edition, McGraw-Hill Higher Education, New York, USA, June, 2007.



Yingxian Zhang, received his B.S. degree in information engineering, M.S. degree in communications and information system from College of Communications Engineering, PLA University of Science and Technology (PLAUST), Nanjing, China, in 2009 and 2011, respectively. He is currently pursuing the Ph.D. degree in communications and information system in College of Communications Engineering, PLAUST. His research interests focus on satellite communication, physical layer security, channel coding, and information theory. He was an Exemplary Reviewer for the IEEE Communications Letters and IET Communications in 2013 and 2014, respectively. Email: zhangyingxian@126.com.

Aijun Liu, received the B.S. degree in microwave communications, M.S. degree and Ph.D. degree in communications engineering and information systems from College of Communications Engineering, Nanjing, China, in 1990, 1994 and 1997, respectively. Since 1986, Dr. Liu has been with the College of Communications Engineering, PLA University of Science and Technology, where he is currently a Full Professor and the Head of the Department of Teaching and Research, College of Communications Engineering. He has published over 50 papers in refereed mainstream journals and reputed international conferences and has been granted over 10 patents in his research areas. His current research interests are satellite communication system theory, satellite communication anti-jamming, signal processing, space heterogeneous networks, channel coding, and information theory. Email: liuaj.cn@163.com.

Xiaofei Pan, received the B.S. degree in communications engineering, M.S. degree and Ph.D. degree in communications engineering and information systems from College of Communications Engineering, Nanjing, China, in 2001, 2004 and 2007, respectively. His major research interests include satellite communication anti-jamming and space heterogeneous networks. Email: motonula@163.com.

Zhan Ye, received the B.S. degree in communications engineering, M.S. degree and Ph.D. degree in communications engineering and information systems from College of Communications Engineering, Nanjing, China, in 1999, 2004 and 2011, respectively. His major research interests include satellite communication anti-jamming and signal process. Email: yezhi5223@163.com.