Novel Physical Layer Security by Adaptive Modulation based on channel SNR and Phase

Lavanya. D.L[1*], RamaPrabha. R[2], Vaishnavi Varatharajan[3], Gunaseelan. K[4]

[1]DRDL, DRDO, Hyderabad, India
[2]ECE Department, College of Engineering Guindy, Anna University, Tamilnadu, India
[3]ECE Design Manufacturing department, Indian Institute of Information Technology Design Manufacturing, Kancheepuram, Tamilnadu, India
[4]ECE Department, College of Engineering Guindy, Anna University, Tamilnadu, India
[*]lavanya@drdl.drdo.in

Abstract: Establishing secured communication among the intended users of wireless networks is a major concern. Especially providing confidentiality is a critical requirement in wireless communication system which is more susceptible to eavesdroppers. Prevailing cryptographic methods were proven to meet the security needs to some extent. Sophisticated encryption techniques cannot be always deployed in wireless devices where the resources are limited. However, physical layer security is recently emerging into a promising paradigm to aid security in wireless networks by exploiting the dynamics of wireless channel. In this paper, a physical layer security technique was proposed to enhance confidentiality which selects the modulation type adaptively, based both on channel SNR and phase between transmitter and receiver. The performance of the proposed technique is evaluated for two types of eavesdroppers such as random and intelligent attackers through simulations. The proposed method improves the symbol error rate even at low SNR values and enhances the confidentiality than the existing algorithms.

[1] Introduction

Information security is a prerequisite for any communication system. Especially wireless networks demand high level of security due to its vulnerable nature. Also highly sophisticated cryptographic techniques of wired communication system cannot be completely adapted to their wireless counterparts due to the limited resources. This constraint in wireless security has resulted in the emerging of physical layer security schemes, which in recent years, have proven to be an excellent means to impart wireless data security. The fundamental principle of physical layer security is to utilize the inherent characteristics of wireless channels to provide security. Amongst the different categories of security services, confidentiality is the main security aspect of this paper. This paper presents yet another physical layer security technique to assure confidentiality and to enhance the overall system performance in terms of Symbol Error Rate (SER).

Physical layer security techniques can be grouped into three categories based on the wireless channel, diversity techniques and hardware impairments. In this paper, the complete work is based on the exploitation of wireless channel characteristics to achieve confidentiality. Physical layer security holds different pattern of traditional wireless security techniques, in which confidentiality is achieved by using the uniqueness of the wireless channel. A physical layer security scheme based on signal constellation approach was presented in [1], where confidentiality of the transmitted symbol is attained by exploitation of the channel phase. Moreover, utilization of channel based physical layer security converts the open nature which is a disadvantageous factor of a wireless channel, into an advantageous one [2]-[6]. Another method of physical layer security is the channel based secret key generation, in which the two-way pilot signals are exchanged between the two communicating users. A secret key is generated based on the observation of the wireless channel which is unavailable for the eavesdropper due to difference in wireless channel properties. The Received Signal Strength (RSS), a location dependent feature associated with transmitter power and Channel State Information (CSI), is utilized in this method to differentiate between the users and eavesdroppers. Nevertheless, even in such cases, physical layer security is uncertain if eavesdroppers can adjust their transmitting power [7]-[10]. In [11], security is incorporated by rotating the symbol by a specific angle before transmission that can be decrypted only by the intended receiver by reversing the angle of rotation. This method is vulnerable to attacks like brute force search algorithm because the rotation angle is fixed. Besides, with large number of symbols, it becomes easy to identify the rotation angle. In [12], technique based on key sharing between the users for selecting modulation types is being discussed. Similarly, [13]-[15] employs a key distribution algorithm for allocation of pre-shared key between the two communicating users.

Recently, signal constellation based physical layer security approaches is gaining attention because of its less complexity. Another physical layer security scheme based on the signal constellation diagram called signal design approach is used in [16]. In this approach, the signal constellation is altered and sometimes the symbol is rotated so that the eavesdropper cannot correctly decode the received signal. Also in [1], signal modulation is altered for each transmission based on estimated channel phase. Based on the selected modulation type the transmitted bits are mapped to a symbol and the phase of the mapped symbol is rotated clockwise by an angle equal to the estimated channel phase. The limitation in this method is that the modulation type is chosen without the consideration of the channel's SNR. This may result in two undesired conditions. One, there is fair chance to choose higher order modulation at low SNR values which results in increasing the outage probability by not meeting the target error rate. Other one is the reverse condition that decreases the achievable throughput by choosing lower order modulation type at high SNR values.

Motivated to overcome this constraint, this paper presents a physical layer security scheme which takes into account the practical consideration of channel's SNR as well as phase. Modulation types that satisfy the targeted error rate, based on SNR, only are considered for that particular transmission. Other modulation types which are not deemed to support the desired error rate for that SNR are excluded for that transmission. This method, while maintaining the confidentiality, also assures a desirable error rate even at low SNRs. Compared to [1], our proposed method guarantees reasonably low error rates even at low SNR while retaining all other security features of it. Compared to key exchange based techniques our proposal does not require any key exchange between the transmitter and receiver for adopting the modulation type and our proposal is robust against the eavesdropper attacks such as brute force search attacks, random text attacks and adaptive random text attacks. This is mainly due to the channel phase and SNR, which varies independently over time. Compared to the fixed phase rotation, adaptive phase modulation technique based on the channel phase and SNR provides more confidentiality and immunity against attackers. Our channel phase and SNR is distant independent parameter, which is more difficult for eavesdropper to estimate it, and it also provides SNR guard interval and phase guard interval which also increases the robustness to channel phase estimation errors and channel SNR estimation errors.

The rest of the paper is organised as follows. Section 2 deals with the system model and Section 3 explains the proposed adaptive modulation scheme followed by the attacker model in Section 4. Section 5 consists of the performance evaluation and simulation results which are followed by the conclusion in Section 6.

[2] System Model

Consider a wireless communication system with a transmitter and receiver operating in full or half-duplex time division channels. Data transmission commences with exchange of pilot signals between them in same time slot or consecutive two time slots in a full or half-duplex system respectively. Depending on the received pilot signals, impulse response of the channel is estimated without acknowledgment [17]. Due to the reciprocity nature of the TDD channels being considered in this case, the instantaneous magnitude and phase of the channel between transmitter and receiver is known only to them and concealed from eavesdroppers.

Considering the data transmission occurring from Tx to Rx, the received signal y_r at intended receiver can be expressed as

$$y_r = h(t).x(t) + n(t) \qquad (1)$$

where *x(t)* is the transmitted signal, *h(t)* is the channel response and *n(t)* is the zero-mean additive white Gaussian noise with variance σ_n^2. Thus for Rayleigh fading channel, the impulse response *h* is modelled as Gaussian random variable with zero mean and unity variance, expressed in polar form as

$$h(t) = |h(t)|e^{j\Phi(t)} \qquad (2)$$

where h(t) is the magnitude and Φ(t) is the phase of the channel which is uniformly distributed in the interval [0,2π] [18].

Fig. 1, shows the signal flow starting from session initialization to end of transmission between transmitter and receiver in the presence of eavesdroppers. Two types of eavesdroppers with different capabilities are assumed. Before commencement of data transmission, session initialization is carried out using pilot signals. Pilot signals are transmitted between transmitter and receiver, and estimation of SNR and channel phase is performed. Only Phase Shift Keying (PSK) modulation of different orders is considered in this paper, for ease of analysis.

Consider the maximum number of modulation types supported for data communication between transmitter and receiver for a particular session is denoted as M. In this proposed scheme, depending on SNR, M is fixed for that particular transmission session. Sorting of modulation type depending on SNR was made based on the Adaptive Modulation Coding techniques (AMC) [19]-[21].

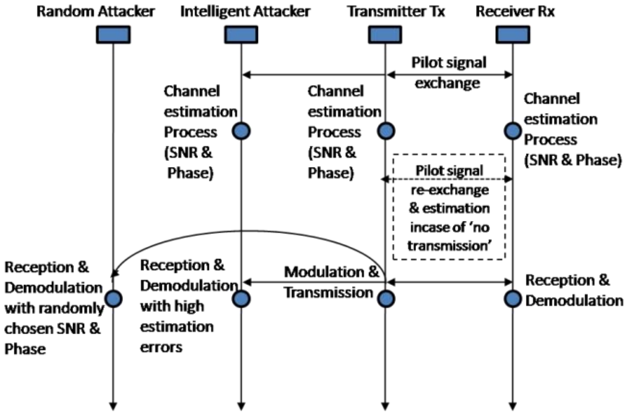
Random Attacker
Intelligent Attacker
Transmitter Tx
Receiver Rx
Pilot signal exchange
Channel estimation Process (SNR & Phase)
Channel estimation Process (SNR & Phase)
Channel estimation Process (SNR & Phase)
Pilot signal re-exchange & estimation incase of 'no transmission'
Reception & Demodulation with randomly chosen SNR & Phase
Reception & Demodulation with high estimation errors
Modulation & Transmission
Reception & Demodulation

Fig.1 *Signal flow among transmitter, receiver and attackers.*

Depending on the channel phase, m^{th} modulation type from a set of M modulation types is selected, where it employs m-ary PSK where $1 \leq \mathrm{m} \geq \mathrm{M}$ and 2^m denoting the number of symbols transmitted. The transmitted signal x can be expressed in polar form as

$$x = e^{j\theta m} \qquad (3)$$

where the magnitude of the signal is unity and phase $\theta_m = \frac{2\pi}{M}(m-1)$ where m is the symbol index in the bit block of size M.

The estimation process is followed by the modulation and transmission of signal from transmitter and demodulation of the received signal at receiver is carried out depending on the estimated parameters. If the estimated SNR or phase falls into their respective guard interval, *'no transmission'* is declared which results in re-initialization of session by exchanging pilot signals again. Guard intervals are the cushion in between two consecutive categories of modulation types, which is explained in detail subsequently. The condition of no transmission is assumed in order to reduce the SER which may occur due to mismatch of modulation types selected at transmitter and receiver.

The estimation process is followed by the modulation and transmission of signal from transmitter and demodulation of the received signal at receiver is carried out depending on the estimated parameters. If the estimated SNR or phase falls into their respective guard interval, *'no transmission'* is declared which results in re-initialization of session by exchanging pilot signals again. Guard intervals are the cushion in between two consecutive categories of modulation types, which is explained in detail subsequently. The condition of no transmission is assumed in order to reduce the SER which may occur due to mismatch of modulation types selected at transmitter and receiver.

To ensure the security of the transmitted data, physical layer approaches utilizes any of the physical layer properties. Physical layer properties can be of channel-based or hardware based. Channel based schemes make use of channel state information and hardware based schemes make use of device impairments like modulator imbalances or carrier frequency offset. Channel based techniques exploits the properties of channel impulse response of a wireless channel like reciprocity, correlation in temporal variation and de-correlation in spatial variation.In our proposed method SNR and phase are used as physical layer signatures.

[3] Proposed Adaptive modulation scheme

The proposed adaptive modulation scheme exploits channel SNR and phase to carry out the entire modulation process. The proposed scheme incorporates three levels of security such as adaptive selection of modulation size, adaptive selection of order of modulation and rotation of symbol based on SNR and phase.

The size of the modulation schemes M is adaptively selected based on SNR. For example if SNR is between 13dB to 17dB, then the M is chosen as 3 and m = 1, 2 & 3. The modulation set consists of three different modulation schemes such as BPSK (m=1), QPSK (m=2) and 8PSK (m=3).

Once M is fixed, the order of PSK modulation is chosen based on the channel phase. For each value of M, the complete channel phase of 0 to 2π is divided into M equal intervals. The Phase set consisting of M categories, is denoted by P_m, where $1 \leq m \leq M$. Every P_m is assigned a predefined level of modulation type of order 2^m - ary PSK. Depending on the channel phase, particular P_m and subsequently the modulation level is chosen for data transmission with a symbol length of $\log_2 m$. P_m can be represented as,

$$\mathrm{P_m} = \frac{2(\mathrm{m}-1)\pi}{\mathrm{M}} \leq \Phi(\mathrm{t}) < \frac{2\mathrm{m}\pi}{\mathrm{M}} \qquad (4)$$

Message bits are mapped into symbols as per the selected modulation type. To incorporate third layer of security, the selected symbol, after mapping, is rotated by a phase value Θ_{rot} which depends both on estimated SNR and phase. Θ_{rot} is formulated as,

$$\theta_{\mathrm{rot}} = (\Phi(\mathrm{t}) * \mathrm{m}) \bmod 360 \qquad (5)$$

Fig. 2, illustrates the proposed adaptive modulation scheme. The sequence of steps involved for each transmission is illustrated in the following Algorithm 1. Table 1 enumerates the selection of modulation type based on SNR and phase.

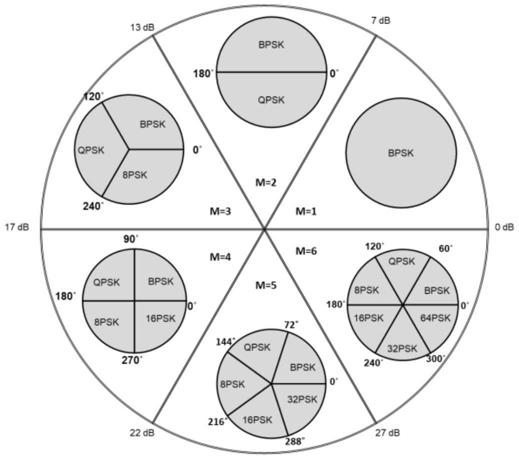

Fig.2 *Proposed scheme using SNR and Phase for M=6*

Algorithm 1: Proposed Adaptive Modulation Scheme

Step 1: Session initialization by exchanging pilot signals between the transmitter and receiver without feedback. Channel estimation by both stations for estimating SNR and channel phase. If the estimated value falls in guard interval, repeat the session initialization.

At Sender end:

Step 2: Based on SNR value, decide the size of modulation M.

Step 3: Based on channel phase, select the modulation type m from the modulation set and map the message bits to the symbols. Symbol length

depends on the type of PSK modulation scheme selected.
Step 4: Rotate the symbols with phase $e^{-j\Theta rot}$ and transmit.
At Receiver end:
Step 5: Select the modulation size and type based on the estimated channel SNR and phase,
Step 6: Rotate the received symbols with $e^{j\Theta rot}$ and demodulate it, where Θ_{rot} is phase used for rotation and it is computed using estimated phase as mentioned in (5).

3.1. Channel Estimation Errors

As the complete modulation and demodulation depends on the channel estimation process at transmitter Tx and receiver Rx, necessary cushion for estimation errors was also considered. Two estimation errors are formulated - SNR estimation error (ϵ_s) and phase estimation error (ϵ_p). SNR estimation error, ϵ_s is the difference between the estimated SNR $\gamma(t)$ at transmitter and estimated SNR $\hat{\gamma}(t)$ at receiver and is given as,

$$\varepsilon_s(t) = \gamma(t) - \hat{\gamma}(t) \qquad (6)$$

ϵ_s is modelled as a uniform random variable in the interval [-ρ_r, ρ_r], where ρ_r is the maximum SNR estimation error at Rx. Phase estimation error is the difference between the actual phase $\phi(t)$ and estimated phase $\hat{\phi}(t)$ and is given as,

$$\varepsilon_p(t) = \phi(t) - \hat{\phi}(t) \qquad (7)$$

ϵ_p is modelled as a uniform random variable in the interval [-Δ_r , Δ_r], where Δ_r is the maximum phase estimation error at Rx.

3.1.1. *Probability of incorrect modulation due to SNR estimation error:* Estimation errors may lead to selection of different modulation types at Tx and Rx. Incorrect selection of modulation type result in increasing SER at Rx. The probability of choosing incorrect modulation type due to SNR estimation error, σ_1 is given as,

$$\sigma_1 = \sum_{m=0}^{M-1} \xi_m \left(1 - \left(\int_{\max(-\rho_r, R^U_{m-1} - \gamma(t))}^{\min(\rho_r, R^L_{m+1} - \gamma(t))} f_{\varepsilon_s} d\varepsilon_s . \right)\right) \qquad (8)$$

where ξ_m is the probability that the estimated SNR $\hat{\gamma}(t)$ lies in the region $\mathrm{R_m}$. R^U_M and R^L_M are the upper and lower bounds of $\mathrm{R_m}$ respectively. The function $f\epsilon_s$ is the uniform pdf of ϵ_s and is given as,

$$f_{\varepsilon_s} = \begin{cases} \dfrac{1}{2\Delta_r}, -\Delta_r \le \varepsilon_s \le \Delta_r \\ 0, otherwise \end{cases} \qquad (9)$$

The total probability of incorrect selection of modulation type due to SNR estimation error, σ_1 becomes zero when $\min(\rho_r, R^L_{m+1} - \gamma(t)) = \rho_r$ and $\max(-\rho_r, R^U_{m-1} - \gamma(t)) = -\rho_r$

Table 1 SNR and phase thresholds for Selection of modulation size and order of modulation

SNR	Modulation Size (M)	Phase Sets (P_m)	Phase interval	Modulation Type
< 7dB	1	P_1	$0 \le \Phi(t) < 2\pi$	BPSK
7dB ≤ SNR < 13dB	2	P_1	$0 \le \Phi(t) < \pi$	BPSK
		P_2	$\pi \le \Phi(t) < 2\pi$	QPSK
13dB ≤ SNR < 17dB	3	P_1	$0 \le \Phi(t) < 2\pi/3$	BPSK
		P_2	$2\pi/3 \le \Phi(t) < 4\pi/3$	QPSK
		P_3	$4\pi/3 \le \Phi(t) < 2\pi$	8-PSK
17dB ≤ SNR < 22dB	4	P_1	$0 \le \Phi(t) < \pi/2$	BPSK
		P_2	$\pi/2 \le \Phi(t) < \pi$	QPSK
		P_3	$\pi \le \Phi(t) < 3\pi/2$	8-PSK
		P_4	$3\pi/2 \le \Phi(t) < 2\pi$	16-PSK
22dB ≤ SNR < 27dB	5	P_1	$0 \le \Phi(t) < 2\pi/5$	BPSK
		P_2	$2\pi/5 \le \Phi(t) < 4\pi/5$	QPSK
		P_3	$4\pi/5 \le \Phi(t) < 6\pi/5$	8-PSK
		P_4	$6\pi/5 \le \Phi(t) < 8\pi/5$	16-PSK
		P_5	$8\pi/5 \le \Phi(t) < 2\pi$	32-PSK
27dB ≤ SNR < ∞	6	P_1 to P_M	$0 \le \Phi(t) < 2\pi/M$ To $2(m-1)\pi/M \le \Phi(t) < 2m\pi/M$	BPSK to 2^M – ary PSK

3.1.2. *Probability of incorrect modulation due to Phase estimation error:* The probability of choosing incorrect modulation type due to phase estimation error, σ_2 is given as,

$$\sigma_2 = \sum_{m=0}^{M-1} \xi_m (1 - \left(\int_{\max(-\Delta_r, A_{m-1}^U - \phi(t))}^{\min(\Delta_r, A_{m+1}^L - \phi(t))} f_{\varepsilon_p} d\varepsilon_p \right)) \qquad (10)$$

Estimated phase $\hat{\phi}(t)$ lies in the area $\mathrm{A_m}$. A_M^U and A_M^L are the upper and lower bounds of $\mathrm{A_m}$ respectively. Similarly, the function $f\epsilon_p$ is the uniform pdf of ϵ_p and is given as,

$$f_{\varepsilon_p} = \begin{cases} \dfrac{1}{2\rho_r}, -\rho_r \le \varepsilon_p \le \rho_r \\ 0, otherwise \end{cases} \qquad (11)$$

The total probability of incorrect selection of modulation type due to phase estimation error, σ_2 becomes zero when $\min(\Delta_r, A_{m+1}^{L} - \phi(t)) = \Delta_r$

$\max(-\Delta_r, A_{m-1}^{U} - \phi(t)) = -\Delta_r$

Hence the conditions to be satisfied for zero probability of erroneous selection of modulation type can be formulated as,

$$R_{m-1}^U + \rho_r < \gamma(t) < R_{m+1}^L - \rho_r \qquad (12)$$

$$A_{m-1}^U + \Delta_r < \phi(t) < A_{m+1}^L - \Delta_r \qquad (13)$$

3.2. Guard Interval

A guard interval at Tx is introduced [22], between the upper bound and lower bound of two consecutive regions of interest to cater for the estimation errors at Rx. For sessions whose estimated values (either SNR or phase) falling in the guard interval, signal transmission is withheld and channel estimation process is repeated for another pilot signal.

A guard interval ρ_g is introduced for SNR estimation error between the upper bound and lower bound of two consecutive SNR regions (R_m). ρ_r is the maximum SNR estimation error at Rx. Similarly a guard interval of Θ_g is introduced for phase estimation error between the upper bound and lower bound of two consecutive phase regions (A_m). Δ_r is the maximum phase estimation error at Rx.

To achieve zero probability of incorrect modulation, guard interval at Tx should be equal to maximum phase estimation error at receiver, i.e $\rho_g = \rho_r$ and $\Theta_g = \Delta_r$. Fig. 3 shows the representation of guard interval for SNR estimation and Fig. 4 shows the guard interval for phase estimation.

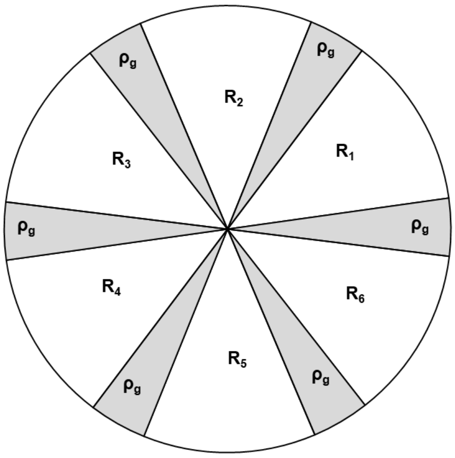

Fig. 3 *Representation of SNR region of interest with respective guard intervals for M=6*

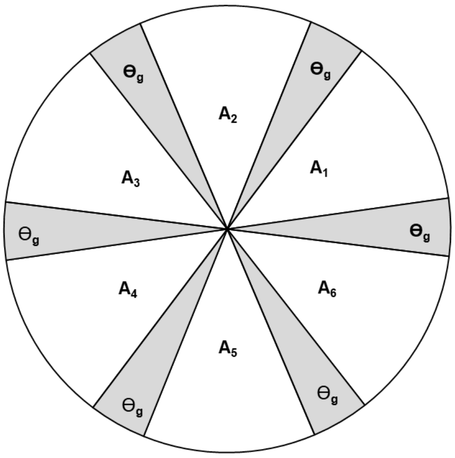

Fig. 4 *Representation of Phase region of interest with respective guard intervals for M=6*

3.3. Symbol Error Rate

The performance of the system is evaluated in terms of symbol error rate for different SNR values. The SER at Rx is given as

$$SER_R = \sigma_r + (1 - \sigma_r)\varepsilon \qquad (14)$$

where σ_r is the probability of incorrect selection of the modulation type and ε is the symbol error rate due to estimation error of SNR and phase. According to the equations (7), (12) and (13), if the guard interval width is equal to the maximum estimation errors in both SNR and phase, σ_r can be set to zero i.e., σ_r = 0 if $\rho_g = \rho_r$ and $\Theta_g = \Delta_r$. So that (14) can be simplified to $SER_R = \varepsilon$. By including the probable estimation error at the receiver, the received signal at Rx can be rewritten as follows

$$y_r(t) = |h_r(t)| x(t) e^{j\varepsilon(t)} + n(t) \qquad (15)$$

From (15), ε influences the effects of noise, n(t) and probable estimation errors. Even though symbol error due to noise is inevitable, to analyze the effects of symbol error due to estimation errors, we are ignoring the effect of noise and hence the only parameter that may cause symbol error is estimation errors $\varepsilon(t)$. Symbol error rate occurs only if the phase estimation error exceeds half of the detection area of the transmitted symbol. For example, for M = 6, if the modulation type used is QPSK, the transmitted symbol will be incorrectly detected only if $\left|\varepsilon(t)\right| > \frac{\pi}{2}$. Based on the channel SNR, M value is chosen and by considering only the phase estimation error, symbol error at receiver is formulated as follows

$$SER_R = \frac{1}{M}\sum_{m=1}^{M} \Pr ob.\left\{\left|\varepsilon(t)\right| > \frac{\pi}{2^m}\right\} \qquad (16)$$

$$SER_R = \frac{1}{M}\sum_{m=1}^{M}\int_{\min(\Delta_r,\frac{m\pi}{M})}^{\Delta_r} \frac{1}{2\Delta_r} d\varepsilon_p + \int_{-\Delta_r}^{\max(-\Delta_r,\frac{-m\pi}{M})} \frac{1}{2\Delta_r} d\varepsilon_p \qquad (17)$$

which can be simplified as follows,

$$SER_R = 1 - \frac{1}{M\Delta_r}\sum_{m=1}^{M} \min\{\Delta_r, \frac{\pi}{2^m}\} \qquad (18)$$

From (18), SER_R is equal to zero when the maximum estimation error is kept lower than $\frac{\pi}{2^m}$ (i.e., $SER_R = 0$ if $\Delta_r < \frac{\pi}{2^m}$ for all values of M).

[4] Attackers Model

To ensure the robustness of the proposed scheme against attacks by eavesdropper, two types of attackers with different capabilities were modeled. The type of attack considered here is the information secrecy attack where the attacker tries to demodulate the data. An attempt has been made to improve confidentiality of data by providing three layers of security (through SNR, phase and symbol rotation by manipulated angle) which makes it more difficult for attackers to correctly decode the data. Two types of attackers are modeled - random attacker and intelligent attacker. The following discussion explains the function and ability of the attacker models and the immunity of the proposed system to the attackers.

4.1. Random attacker

A random attacker is the one, who does not have any knowledge of the channel phase and SNR, and randomly chooses a SNR & phase and starts demodulating as per the proposed scheme. Random attacker is modeled to randomly choose a SNR ϵ_{rnds} which is uniformly distributed in interval [0, 50] and a phase ϵ_{rndp} which is uniformly distributed in interval [0, 2π].

4.2. *Intelligent attacker*

Intelligent attacker is modeled with some level of capabilities to estimate the SNR and phase. Even though there is no mechanism that an eavesdropper can estimate the channel, the system is modeled to be strong enough even when an intelligent attacker tries to tamper the confidentiality of the data. Intelligent attacker is modeled with a SNR estimation error ϵ_{ints} which is uniformly distributed in interval [$-\rho_{int}$, ρ_{int}] and a phase estimation error ϵ_{intp} which is uniformly distributed in interval [$-\Delta_{int}$, Δ_{int}].

[5] Performance Evaluation And Simulation Results

Our proposal emphasize on reducing the average SER at receiver Rx even at low SNR. Since three layers of security are incorporated in the proposed method, the simulation results have displayed improvement in confidentiality than the existing scheme. Simulations of the proposed modulation schemes were carried out using MATLAB.

First, the performance of the proposed scheme at Rx in terms of SER, considering estimation errors at Rx and guard intervals at transmitter Tx, have been analyzed. Performance evaluation of the proposed method was carried out in comparison with the method proposed in [1]. Though the performance of modulation scheme proposed by us and that in [1] are similar for high SNR values, our proposed method outperform the one in [1] with less SER at low SNR. Subsequently the robustness of the proposed scheme to two types of attackers was also compared.

5.1. SER performance

The performance of the proposed scheme in terms of SER at Rx is evaluated considering the guard intervals at Tx and estimation errors at Rx. The influence of the estimation errors in choosing an incorrect modulation is analysed by plotting probability of choosing incorrect modulation versus SNR / phase estimation errors. Analysis of the proposed method in terms of probability of selecting incorrect modulation at receiver and its effect on Symbol Error Rate (SER) is also carried out.

Fig. 5 shows the probability of having mismatching modulation types at Tx & Rx (σ_r) versus SNR estimation error (ρ_r) for different SNR guard intervals (ρ_g). As expected, increase in ρ_r results in increasing the probability of choosing wrong modulation type. Conversely, increasing guard interval ρ_g at transmitter decreases the overall probability σ_r. This is because; increasing the guard interval will increase only the probability of *no transmission*. Possibility of choosing incorrect modulation is compromised with choosing *no transmission* phase by increasing guard interval ρ_g. Hence, it is a compromise to choose optimal value so that *no communication* phase is reduced at a cost of accepting slight increase in σ_r. Fig. 6 shows the system performance in terms of SER with varying SNR estimation error at Rx with a fixed guard interval of ρ_g = 2dB, at Tx. This was analysed for different values of M. This analysis was done assuming that there is no phase estimation error. As can be seen from the graph, SER increases with increase in M size. As the M value increases, the region of interest for a particular modulation type shrinks resulting in increasing the probability of choosing different modulation type at Tx and Rx.

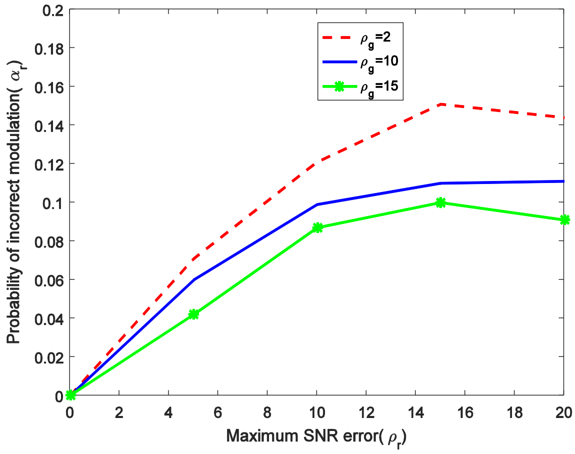

Fig. 5 *Probability of selecting incorrect modulation type at Rx (σ_r) versus maximum SNR estimation error (ρ_r), for different SNR guard interval widths (ρ_g) for M = 4.*

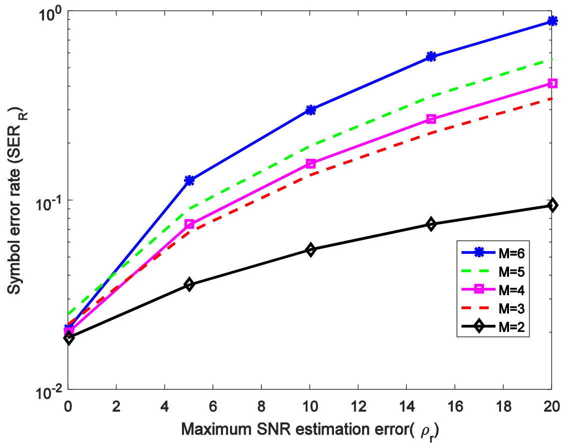

Fig. 6 *The average SER obtained at receiver Rx versus maximum SNR estimation error (ρ_r) at Rx with a fixed SNR guard interval (ρ_g) = 2dB, for different values of M.*

Similarly the system performance in terms of probability of selection of incorrect modulation type and SER for various maximum phase estimation errors is analysed. This analysis was done assuming that there is no SNR estimation error at Rx and phase guard interval at Tx, Θ_g = 5°. Fig. 7 shows the probability of selecting different modulation types at Tx & Rx versus maximum phase estimation error (Δ_r) for different SNR values. From the results it is observed that, the probability of choosing wrong modulation type increases with increasing maximum phase estimation error Δ_r. As the maximum number of modulation type M increases, the area A_m decreases and the possibility of estimated phase falling in adjacent area increases, resulting in probability of choosing wrong modulation type is also increasing. Therefore, the probability of choosing incorrect modulation is more for SNR of with M = 6. Fig. 8 shows the system performance in terms of SER for varying maximum phase estimation error at Rx with a fixed phase guard interval Θ_g = 5° at transmitter. As expected, average SER increases with increase in maximum phase estimation error and with M as well.

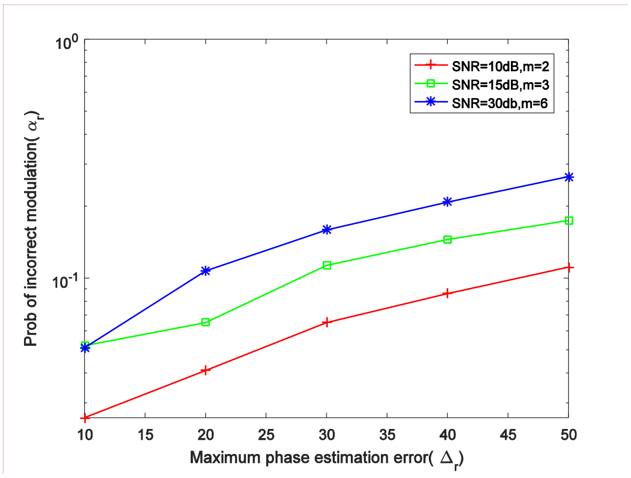

Fig. 7 *The probability of selecting incorrect modulation type at Rx (σ_r) versus the maximum phase estimation error (Δ_r), for different SNR values.*

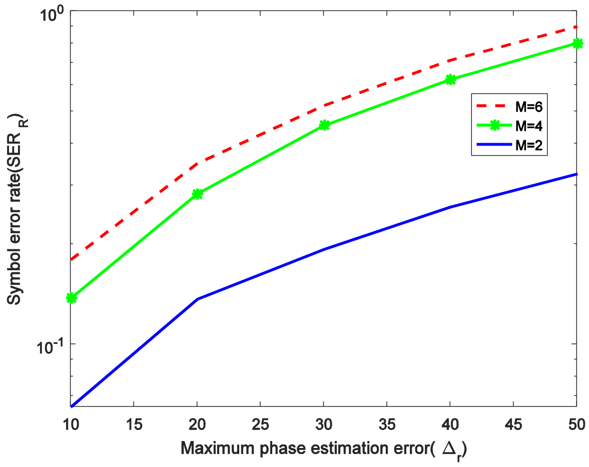

Fig. 8 *The Average SER obtained at Rx versus maximum phase estimation error (Δ_r) for M = 2, 4 & 6. (ρ_g= 2 dB and Θ_g = 5°).*

Fig. 9 shows the SER versus maximum number of modulation types M at Rx for the proposed scheme. As expected there is considerable variation in SER with increase in SNR values which is not the case with attacker. Fig. 10 shows the average SER performance at Rx for different values of SNR. The nominal guard interval for SNR (ρ_g) and Phase (Θ_g) is considered to be 2 dB and 5° respectively. In-order to maintain zero probability of choosing incorrect modulation (σ_r), the conditions ρ_g= ρ_r and Θ_g = Θ_r are retained while analysing the performance at Rx. From the results it can be observed that at low SNRs, the SER is same for any value of M. This is because, for low SNR values, only BPSK modulation is used irrespective of M. At high SNR, considerable difference in SER is observed for different values of M. The proposed technique provides improved SER performance at low SNRs than the existing algorithm proposed in [1] and comparable SER at high SNRs.

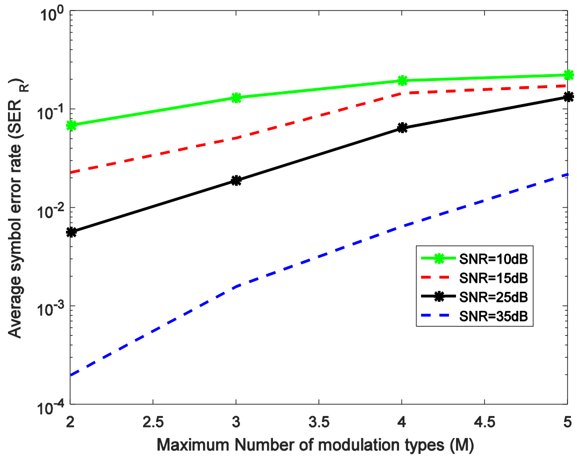

Fig. 9 The Average SER obtained at Rx versus Maximum number of modulation types (M), for different SNR values.

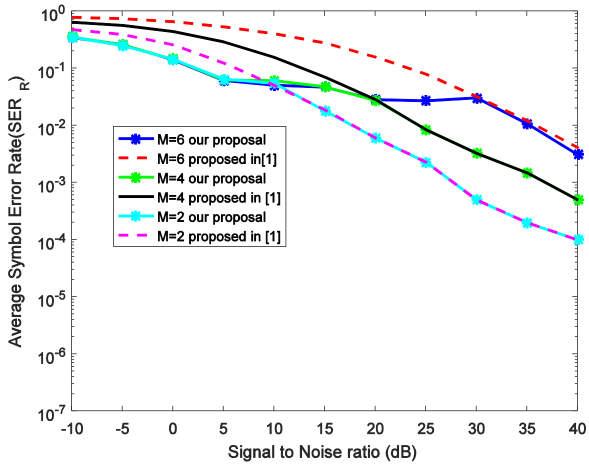

Fig. 10 The Average SER obtained at Rx versus SNR for M = 2 & 4, for proposed and existing schemes

5.2. Performance against attackers

The immunity of the proposed technique with two different types of attackers has been analyzed. To analyse the performance against attackers, the simulations were carried out considering channel estimation to be perfect at receiver Rx. Random attacker is not having any mechanism to estimate SNR or channel phase. A random phase and SNR is chosen by attacker and demodulation is done. Fig. 11 shows the SER for different SNR with M = 2 & 4 for legitimate receiver Rx and random attacker. It can be seen that even at high SNR, the average SER of random attacker is very high irrespective of M, whereas the SER of the legitimate receiver is 10^{-6} for SNR of 40 dB with M=2.

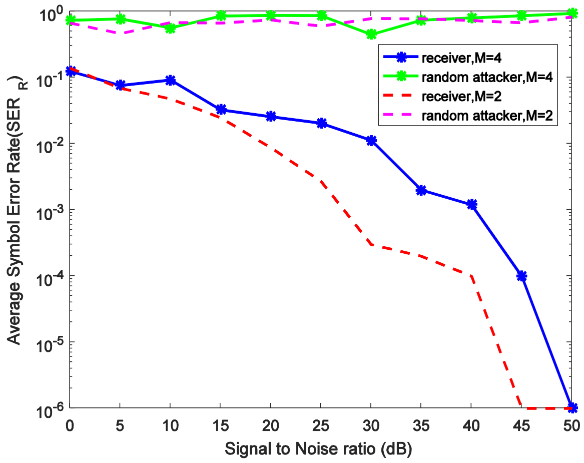

Fig. 11 The Average SER versus SNR for Rx and random attacker for M = 2 & 4.

Similarly, the proposed technique is analyzed with intelligent attacker who is assumed to possess some level of intelligence to estimate the SNR and phase. Fig. 12 shows the SER versus SNR for receiver and intelligent attacker with M = 2 & 4. Even though SER performance of intelligent attacker is better than random attacker, there is no acceptable SER performance. Hence this proposed method provides improved security than the existing method.

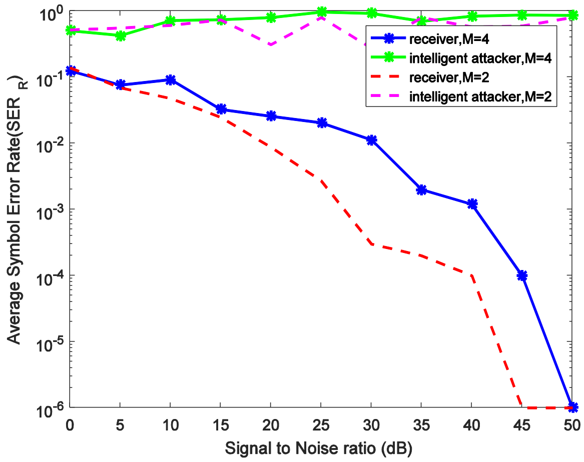

Fig. 12 The Average SER versus SNR for Rx and intelligent attacker for M = 2 & 4.

Further to validate the strength of our proposed algorithm, it is assumed that the attackers are aware of the modulation sequences except for the values of SNR and phase with which modulation is carried out. Fig. 13, compares the SER performance of the proposed technique with existing technique proposed in [1] for random attackers with M = 2 and M = 4. In existing method, random attacker after receiving the signal randomly chooses a channel phase and starts demodulation. In our proposed method, random attacker randomly chooses a SNR value as well as channel phase and starts demodulation. Due to the three layers of adaptation, the random attacker's probability of selecting incorrect modulation is very high, resulting in high SER.

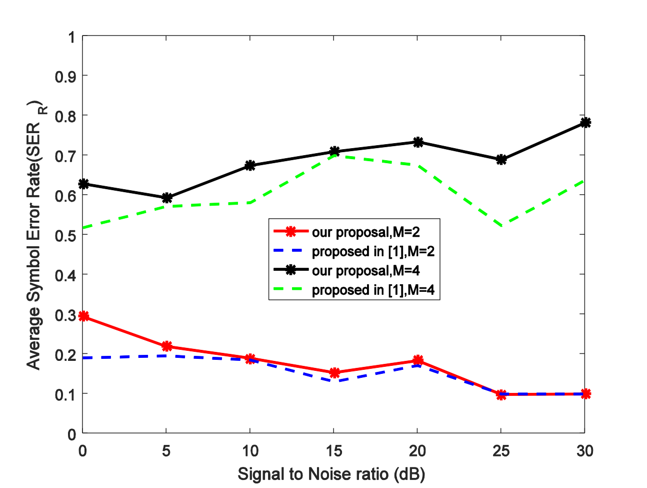

Fig. 13 *The Average SER for random attackers versus SNR for M= 2& 4.*

The system performance of the proposed algorithm is compared with existing technique for intelligent attacker as well. In existing method, the intelligent attacker is assumed to estimate the channel phase with an error spanning uniformly in [-45˚, 45˚]. Intelligent attacker in our proposed method can estimate SNR and phase with an error spanning in [-ρ_{int}, ρ_{int}] and [-Δ_{int}, Δ_{int}] respectively. Considering, ρ_{int} = 2dB and Δ_{int} = 45˚, the estimation errors of our intelligent attacker spans in the interval of [-2, 2] and [-45˚, 45˚]. In Fig. 14, it can be observed that our proposed method for intelligent attacker have high SER due the probability of selecting incorrect modulation being very high, ultimately resulting in greater security performance than the existing method.

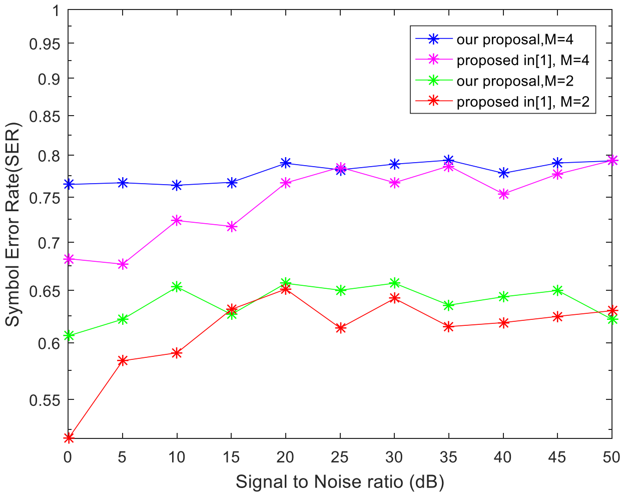

Fig. 14 *The Average SER for intelligent attackers versus SNR for M = 2 & 4.*

[6] Conclusion

A new physical layer security scheme to enhance the confidentiality of the transmitted message from transmitter to receiver against attackers has been proposed and analyzed in this paper. In this proposed scheme, three layers of security such as adaptive selection of modulation size based on channel SNR, adaptive selection of modulation type based on the channel phase and adaptive phase rotation based on both phase and SNR, has been incorporated. The performance of the proposed method is analysed by investigating its immunity against attackers and estimation errors. The simulation results show a significant improvement in the confidentiality and SER performance than the existing physical layer security schemes. In future, this scheme will be integrated with location preserving authentication technique [22] - [24] to establish complete security for Location Based Services (LBS) based systems.

[7] References

[1] Saud Althunibat, Victor Sucasas, Jonathan Rodriguez,: ‘A Physical-Layer Security Scheme by Phase-Based Adaptive Modulation’, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, 2017, 66,pp 1-11

[2] Xiao L., Greenstern L. J.,Mandayam N. B. and Trappe W., :‘Channel-based spoofing detection in frequency-selective rayleigh channels’, IEEE Trans. Wireless Commun., 2009,8 (12), pp. 5948-5956

[3] Tugnait J. K. and Kim H., :‘A channel-based hypothesis testing approach to enhance user authentication in wireless networks’, IEEE Int. Conf. Commun. syst. and networks, Mar. 2010, pp. 1-9

[4] Shiu Y.-S., Chang S. Y., Wu H.-C.,Huang S. C.-H. and Chen H.-H., :‘Physical layer security in wireless networks: a tutorial’ ,IEEE Wireless Commun., 2011, 18(2), pp. 66-74

[5] Shan D., Zeng K., Xiang W., Richardson P. and Dong Y.,: ‘PHY-CRAM: physical layer challenge-response authentication mechanism for wireless networks’, IEEE J. Sel. Areas in Commun.,2013,31(9), pp. 1817-1827

[6] Hou W., Wang X., Chouinard J.-Y. and Refaey A.,:‘Physical layer authentication for mobile systems with time-varying carrier frequency offsets’ IEEE Trans. Commun., 2014, 62(5), pp. 1658-1667

[7] Liu Y., Draper S. C. and Sayeed A. M.,: ‘Exploiting channel diversity in secret key generation from multipath fading randomness’, IEEE Trans. Inf. Forens. Security, 2012, 7(5), pp. 1484-1497

[8] Xiao L., Greenstein L., Mandayam N. and Trappe W.,: ‘A physical-layer technique to enhance authentication for mobile terminals’,IEEE Int. Conf. Commun., 2008, pp. 1520-1524

[9] Wang Q., Su H., Ren K., and Kim K.,: ‘Fast and scalable secret key generation exploiting channel phase randomness in wireless

networks', IEEE Conf. Comput. Commun., 2011, pp. 1422–1430

[10] Li X. and Ratazzi E. P.,: 'MIMO transmissions with information theoretic secrecy for secret-key agreement in wireless networks' IEEE Mil. Commun. Conf. (MILCOM), Oct. 2005, 3, pp. 1353–1359

[11] opperetal C.P.,' Investigation of signal and message manipulations on the wireless channel', Eur. Symp. Res. Comput. Security, Sep. 2011, pp. 40–59

[12] Xiong T., Lou W., Zhang J., and Tan H.,:'MIO: Enhancing wireless communications security through physical layer multiple inter-symbol obfuscation' ,IEEE Trans. Inf. Forensics Security,2015,10(8),pp.1678– 1691

[13] Tang L., Ambrose J. A., Parameswaran S., and Zhu S., :'Reconfigurable convolutional codec for physical layer communication security application', IEEE Mil. Commun. Conf., 2014,pp. 82– 87

[14] Tang L., Ambrose J. A., Kumar A., and Parameswaran S.,:'Dynamic reconfigurable puncturing for secure wireless communication', Design, Autom. Test Europe Conf. Exhib.,2015, pp. 888–891

[15] Zang G., Huang B., Chen L., and Gao Y.,: 'One transmission scheme based on variable MSK modulator for wireless physical layer security' Wireless Commun. Signal Process., 2015, pp. 1–5

[16] Husain M.I., Mahant S.,and Sridhar R.,:'CD-PHY: Physical layer security in wireless networks through constellation diversity',IEEE Mil. Commun. Conf., Oct./Nov. 2012, pp. 1–9

[17] Fragkiadakis A., Tragos E., and Traganitis A.,: 'Lightweight and secure encryption using channel measurements'*4th Int. Conf. WirelessCommun., Veh. Technol., Inf. Theory Aerosp.Electron. Syst.*, Aalborg, 2014, pp. 1–5

[18] Proakis J.,: '*Digital Communications*' ,(New York, NY, USA: McGraw-Hill, 1995)

[19] Ijaz A., Awoseyila A.B., Evans B.G.,: 'Signal-to-noise ratio estimation algorithm for adaptive coding and modulation in advanced digital video broadcasting–radar cross section satellite systems', *IET Communications*,2012.6,pp.1587

[20] Manish Dangi and Mahesh Kumar Porwal,:'Analyses of SNR Threshold for Minimum BER in Various Modulations Schemes and Development Of an Adaptive Modulation Scheme', IJISET - International Journal of Innovative Science, Engineering & Technology, March 2015, 2

[21] Siva Kumar Reddy B., Lakshmi B.,: 'Adaptive Modulation and Coding with Channel State Information in OFDM for WiMAX', I.J. Image, Graphics and Signal Processing, 2015, 1, 61-69

[22] El Hajj Shehadeh Y. and Hogrefe D., :'An optimal guard intervals based mechanism for key generation from multipath wireless channels', *IFIP Int. Conf. New Technol., Mobility Security*, 2011, pp. 1–5.

[23] Nasrullah Pirzada, M Yunus Nayarr, Fazli Subharr. M Fadzil Hassan, :'Design of an indoor localization system using device-free localization technique',IEEE International Conference on Control System, Computing an Engineering (ICCSCE), 23-25 Nov. 2013

[24] Wei Wang, Student Member, Yingjie Chen, and Qian Zhang, Fellow, :'Privacy-Preserving Location Authentication in Wi-Fi Networks Using Fine-Grained Physical Layer Signatures', IEEE Transactions On Wireless Communications, 2016,15(2)