CHAPTER I

INTODUCTION

1.1 PHYSICAL LAYER SECURITY SCHEME

Information security is critical for any communication systems. In wireless communications, spoofing is a severe security threat due to the broadcast nature of radio signal propagation, in which adversaries attempt to impersonate the legitimate user within a network in order to gain illegitimate advantages. In order to defend systems against spoofing attacks, the receiving end should be equipped with authentication and confidentiality mechanism. By exploiting the advantages of securing wireless transmissions at the physical layer, a variety of physical layer authentication schemes have been proposed by using the inherent properties of wireless channels or the imperfections of hardware devices.

The fundamental principle behind channel based physical layer security is that the spatial, spectral and temporal properties of the wireless fading channel have natural randomness and they are rapidly decorrelated between different geographic locations [4]. As a consequence, the properties of the channel link between legitimate terminals are only available to the intended receiver but cannot be duplicated by adversaries. Physical layer security techniques for wireless communications can prevent malicious attacks without upper layer data encryption. However, the reliability of traditional channel-based physical layer security schemes is hampered by severe channel conditions. In order to overcome this limitation, the application of multiple antennas has been explored to combat channel

fading and improve the performance of secure wireless communications. However, as a result of cost and size limitations of multiple antennas, these scenarios are rarely implemented in practice. For the practical implementation of channel-based authentication systems, efficiently exploiting the advantages of multiple antenna arrays to enhance the performance of spoofing detection has yet to be investigated

1.2 WIRELESS SECURITY CHALLENGES

Security is an implicit part of any communication system that is relied upon for the transmission of private information. Consequently, the reliability to share secret information in the presence of malicious attackers is critically important. From a general perspective, security is concerned with unauthorized users trying to access, forge or modify messages intended for legitimate receivers. Wireless communications is based on electromagnetic waves using radio frequencies (RF) propagating through open space, which provides the freedom of user mobility and the flexibility of data transmission, but also brings significantly more security challenges than traditional wired communications. Therefore, secure wireless communications becomes critical for wireless data transmission.

There are many factors contributing to the increasing security challenges in wireless communications. Primarily, the broadcast nature of the wireless medium makes transmitted signals available to any receiver within the transmission range, which leads to easy access to adversaries. Moreover, the mechanisms of high-level security in a wired network cannot be directly applied in wireless scenarios. Additionally, limited processing power is incurred by the limited space, cost and power constraints of wireless devices [2]. Considering these essential limitations of wireless communications, security mechanisms for wireless systems should be developed to address increasing threats.

1.3 PHYSICAL LAYER SECURITY TECHNIQUES

Physical layer security, which exploits physical link properties, is a promising paradigm to provide energy-efficient security solutions and enhance the

security performance of wireless communications systems [3]-[6]. Security from the information-theoretic perspective was pioneered by Shannon, who introduced the definition of perfect secrecy and theoretically characterized that the fundamental ability of the physical layer can provide secure communications. Physical layer security techniques are classified into three major categories based on the wireless channel, RF-DNA and diversity technique, respectively.

1.3.1 WIRELESS CHANNEL-BASED PHYSICAL LAYER SECURITY

In wireless communications, due to the presence of scatters and reflectors in the environment, a transmitted signal undergoes multiple paths that combine constructively or destructively at the receiver [5]. Consequently, the received signal is the superposition of multiple copies of the transmitted signal via different paths from the transmitter to the receiver, where each copy experiences differences in attenuation, phase shift and propagation delay.

The wireless channel characterized by CIR has the following major properties:

• Reciprocity: As during the coherence time, the observed channel impulse responses at two geographically separated communicating terminals are the same.

• Correlated temporal variation: Wireless channels vary with time but the variations usually highly correlated in time.

• Spatial decorrelation: According to the propagation theory, the radio channel response decorrelates rapidly in space from one transmitter-receiver pair to another if these two pairs are at least half a wavelength away.

1.3.2 RF-DNA BASED PHYSICAL LAYER SECURITY

RF-DNA fingerprinting involves exploiting natural imperfections and unclonable variations of a unique device induced by the analog components to

identify and authenticate devices at the physical layer, which cannot be changed post-production and mimicked by adversaries in a manner analogous to biometrics. Various RF characteristics, such as transient amplitude and phase, I/Q modulator imbalance and CFO [24], are extracted from the intrinsic physical properties of devices. These hardware impairments are observed differentially even in two devices constructed with the same manufacturing and packaging processes, and they are allowed by manufacturers as wireless transceivers as such minor imperfections are acceptable for practical implementations in the communication standards. Therefore, the distinct features of the RF-DNA fingerprint can be utilized to provide additional protection against identity-related threats via the physical layer.

1.3.3 DIVERSITY TECHNIQUE-BASED PHYSICAL LAYER SECURITY

The capacity of single antenna systems is bounded by the Shannon limit, diversity techniques have been developed to improve system performance by using multiple replicas of transmitting signals passed over multiple channels of different characteristics. Multiple antenna techniques provide physical layer secrecy with new and exciting opportunities, and also provide extremely high spectral efficiency as well as link reliability through space diversity for wireless communications [10]. MIMO systems use the technique of space diversity to improve communications performance where multiple antennas are equipped at the transmitter and receiver. However, the hardware implementation of MIMO systems is not feasible, particularly in mobile equipment's, due to size, weight and cost limitations. As an alternative, cooperative diversity is achieved through user cooperation, in which information is allowed to be transmitted between source and destination via other nodes in a network in order to enjoy the advantages of MIMO systems with single antenna equipped users [7]. More specifically, cooperative communications provides the advantages of higher spatial diversity and achievable data rates, lower transmission delay and power, better frequency reuse and more adaptability to

network conditions. Additionally, cooperative communications techniques exploit user cooperation to combat channel fading and enhance the security performance of wireless networks.

1.4 CONFIDENTIALITY

One of the main security aspects is ensuring the confidentiality of the transmitted data [1]. Confidentiality is commonly used to describe the degree of protection in the transmitted data against eavesdroppers. Typically, confidentiality is achieved using encryption where a secret key is used to encrypt data at the transmitter and decrypt it at the legitimate receivers [9]. Conventional encryption suffers from some practical challenges such as the complexity of the encryption algorithms and the signalling overhead required in key distribution/agreement protocols [10]. Thus, encryption/decryption process represents a real challenge for resource-limited users.

1.5 AUTHENTICATION

Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system or within an authentication server. Different systems may require different types of credentials to ascertain a user's identity [23]. Three categories in which someone may be authenticated are: something the user knows, something the user is, and something the user has.

1.5.1 LOCATION AUTHENTICATION

- Location-based authentication is a special procedure to prove an individual's identity
- Authenticity on appearance simply by detecting its presence at a distinct location.

- To enable location-based authentication, a special combination of objects is required. The individual that applies for being identified and authenticated has to present a sign of identity.
- The individual has to carry at least one human authentication factor that may be recognized on the distinct location.
- The distinct location must be equipped with a resident means that is capable to determine the coincidence of individual at this distinct location.

1.5.2 LOCATION-BASED SERVICES (LBS)

Location-based services (LBS) use real-time geo-data from a mobile device or Smartphone to provide information, entertainment or security. Some services allow consumers to "check in" at restaurants, coffee shops, stores, concerts, and other places or events [23]. Location-based services use a Smartphone's GPS technology to track a person's location, if that person has opted-in to allow the service to do that. After a Smartphone user opts-in, the service can identify his or her location down to a street address without the need for manual data entry.

1.5.3 USES OF LOCATION-BASED SERVICES

Companies have found several ways to use a device's location:

- Store locators: Using location-based intelligence, retail customers can quickly find the nearest store location.
- Proximity-based marketing: Local companies can push ads only to individuals within the same geographic location
- Travel information: LBS can deliver real-time information, such as traffic updates or weather reports, to the Smartphone so the user can plan accordingly.
- Mobile workforce management: For logistics-dependent companies that employ individuals out in the field or at multiple locations, an LBS allows employees to check in at a location using their mobile device

1.5.4 LOCATION PRIVACY

Location privacy refers to the ability of an individual to move in public areas with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use. To avoid location forgery, an essential step is location authentication, which verifies the truthfulness of the reported location data [24]. An intuitive approach is to equip provider with localization capability, which, however, falls short due to the following two limitations. First, there are places such as coffee shops and stores where the number of provider-trusted APs is not enough to perform localization. Second, the growing privacy threats of sharing location information via LBS have been widely concerned. Such privacy threats come from the fact that many untrusted Wi-Fi infrastructures aggressively collect the location data. Although mobile users can secure their location data via encryption, their location information is still at high risk of being leaked due to the broadcast nature of wireless medium. Adversary can easily infer the targeted user's physical location by collaboratively eavesdropping frames over the air from several sniffers (e.g., untrusted APs). Previous research shows that one can determine a node with meter/centimeter level resolution using several receivers. Being aware of such risks, mobile users may be reluctant to use LBS applications.

1.6 PROBLEM STATEMENT

Physical layer security holds different pattern of traditional wireless security techniques, in which confidentiality is achieved by using the uniqueness of the wireless channel. 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. 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. 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. The limitation in adaptive modulation 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.

1.7 OBJECTIVE OF THE PROJECT

The objective of the project is to design a physical layer security scheme which provides both authentication and confidentiality for LBS based Wi-Fi networks. Confidentiality is achieved by exploiting adaptive modulation which takes into account the practical consideration of channel's SNR as well as phase and authentication is done using singular value decomposition and two layer differentiation algorithm. To improve the symbol error rate even at low SNR values and enhances the confidentiality and authentication than the existing algorithms.

1.8 LITERATURE SURVEY

1.8.1 A PHYSICAL-LAYER SECURITY SCHEME BY PHASE-BASED ADAPTIVE MODULATION [1]

This paper presents a physical-layer security scheme that is light weight, efficient and resilient against eavesdroppers. This paper exploits the channel phase in order to guarantee the confidentiality of the transmitted data, and it is based on altering the employed signal modulation at each transmission time. The employed modulation type is selected among a supported set based on the probed channel phase at the beginning of each transmission. As such, channel phase must be kept secret between the transmitter and the intended receiver, which can be accomplished by channel reciprocity process where channel responses are estimated by both communicating ends without a feedback link. Upon estimating the channel phase, transmitted bits are mapped to a symbol according to the corresponding selected modulation type. Moreover, aiming at improving the confidentiality, the phase of the mapped symbol is rotated clockwise by an angle that is equal to the instantaneous channel phase. It is worth noting that hiding the modulation type leads to hiding the length of the transmitted symbol as well, which makes illegitimate decoding very difficult. This method does not require a key to be shared between the transmitter and the receiver for adapting the modulation type. This method is resilient against many popular attacks (such as plain-text, adaptive plain-text and brute force search attacks). This is due to the fact that the modulation type is changed based on the channel phase which varies independently over time. Notice that as channel phase is distant-independent parameter, it is almost impossible for an eavesdropper to predict it. Also, it is worth highlighting that method is designed in order to alleviate the impact of the channel estimation errors at the legitimate receiver by employing the guard intervals concept. Finally, a last property of the method is that it can be applied jointly with conventional key-encryption protocols, which further enhances the confidentiality.

1.8.2 PRIVACY-PRESERVING LOCATION AUTHENTICATION IN WI-FI NETWORKS [24]

Privacy-preserving location authentication can be realized within existing Wi-Fi-based LBS systems by exploiting physical layer (PHY) signatures in Wi-Fi preambles. To achieve this goal, PriLA, a Privacy-Preserving Location Authentication system in orthogonal frequency division multiplexing (OFDM) based Wi-Fi networks (e.g., IEEE 802.11a/g/n/ac) is introduced. This system allows the LBS provider to successfully conduct authentication while and meanwhile guaranteeing location privacy preservation for all mobile users against adversaries. PriLA exploits carrier frequency offset (CFO) and multipath, which can be obtained via Wi-Fi preambles. In communication systems, CFO and multipath are considered to be detrimental, while PriLA leverages them for authentication and privacy-preservation. PriLA takes advantage of the channel reciprocity property, and uses CFO together with channel state information (CSI) to generate CFO patterns that are exclusively known by the transmission pair. In particular, to defend against adversaries with localization capability, PriLA uses CFO pattern to secure users' IDs starting from the handshake (or association) phase. As such, the adversaries cannot link a frame to a certain user, or infer the presence of a user, and thus fail to localize a user via localization. To enable authentication without performing localization, PriLA leverages users' multipath profiles, which can be extracted from CSI using multiple antennas.

1.8.3 CSI-BASED INDOOR LOCALIZATION [25]

Indoor positioning systems have received increasing attention for supporting location-based services in indoor environments. Wi-Fi-based indoor localization has been attractive due to its open access and low cost properties. However, the distance estimation based on received signal strength indicator (RSSI) is easily affected by the temporal and spatial variance due to the multipath effect, which contributes to most of the estimation errors in current systems. In this work, they analyze this effect across the physical layer and account for the undesirable RSSI readings being

reported. They explore the frequency diversity of the subcarriers in orthogonal frequency division multiplexing systems and propose a novel approach called FILA, which leverages the channel state information (CSI) to build a propagation model and a fingerprinting system at the receiver. They implement the FILA system on commercial 802.11 NICs, and then evaluate its performance in different typical indoor scenarios. The experimental results show that the accuracy and latency of distance calculation can be significantly enhanced by using CSI. FILA can significantly improve the localization accuracy compared with the corresponding RSSI approach.

1.8.4 TOWARD PRIVACY PRESERVING AND COLLUSION RESISTANCE IN A LOCATION PROOF UPDATING SYSTEM [26]

Today's location-sensitive service relies on user's mobile device to determine the current location. This allows malicious users to access a restricted resource or provide bogus alibis by cheating on their locations. To address this issue, they propose A Privacy-Preserving Location proof Updating System (APPLAUS) in which collocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. They also develop user-centric location privacy model in which individual users evaluate their location privacy levels and decide whether and when to accept the location proof requests. In order to defend against colluding attacks, they also present between ranking-based and correlation clustering-based approaches for outlier detection Extensive experimental results show that APPLAUS can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks.

1.8.4 TRAFFIC SIGNATURE-BASED MOBILE DEVICE LOCATION AUTHENTICATION [27]

Spontaneous and robust mobile device location authentication can be realized by supplementing existing 802.11x access points (AP) with small cells. They show that by transferring network traffic to a mobile computing device associated with a femtocell while remotely monitoring its ingress traffic activity, any internet-connected sender can verify the cooperating receiver's location. they describe a prototype non cryptographic location authentication system they constructed, and explain how to design both voice and data transmissions with distinct, discernible traffic signatures. Using both analytical modelling and empirical results from their implementation, they demonstrate that these signatures can be reliably detected even in the presence of heavy cross-traffic introduced by other femtocell users.

1.8.6 RECEIVER ORIGINATED PHYSICAL-LAYER ROBUST SECURE TRANSMISSIONS IN WIRELESS SYSTEMS [11]

A receiver-originated physical-layer secure transmissions scheme (ROST) which consists of two-phase communications. In phase 1, the receiver sends a pseudorandom signal (only known by itself) to the transmitter and in phase 2, the transmitter directly sends out the mixture of its confidential message and the received pseudorandom signal. The receiver could estimate the channel with the help of the pseudorandom signal before cancelling it from the received mixed signal, and finally detect the confidential information. By contrast, the eavesdropper can hardly obtain any confidential information because it cannot estimate the channel without any pilot signal in both phases' transmissions and is interfered by the pseudorandom signal. Furthermore, ROST can always keep the security of the confidential message, achieve much higher secrecy capacity than the traditional scheme, even without any channel information at the transmitter.

1.8.7 CD-PHY: PHYSICAL LAYER SECURITY IN WIRELESS NETWORKS THROUGH CONSTELLATION DIVERSITY [13]

CD-PHY, a physical layer security technique that exploits the constellation diversity of wireless networks which is independent of the channel variations. The sender and the receiver use a custom bit sequence to constellation symbol mapping to secure the physical layer communication which is not known a priori to the eavesdropper. Through theoretical modeling and experimental simulation, it shows that this information theoretic construct can achieve Shannon secrecy and any brute force attack from the eavesdropper incurs high overhead and minuscule probability of success. Results also show that the high bit error rate also makes decoding practically infeasible for the eavesdropper, thus securing the communication between the sender and receiver.

1.8.8 MULTIPLE-ACCESS CHANNELS WITH CONFIDENTIAL MESSAGES [15]

A two-user multiple-access channel (MAC) with confidential messages, which generalizes the classical MAC by allowing both users to receive noisy channel outputs. This channel model is motivated by wireless communications, in which transmitted signals are broadcast over open media and can be received by all nodes within communication range. For this channel, we assume that two users (users 1 and 2) have common information and each user has its private (confidential) information intended for a destination. The two users also receive channel outputs; they may extract each other's confidential information from their received channel outputs. However, each user treats the other user as a wiretapper, and wishes to keep its confidential message as secretes possible from this wiretapper. The level of secrecy of one user's confidential message at the other user(wiretapper) is measured by the equivocation rate. Our goal is to study the capacity–equivocation region of the MAC with confidential messages.

CHAPTER 2

PROPOSED PHYSICAL LAYER SECURITY TECHNIQUE

2.1 SYSTEM MODEL

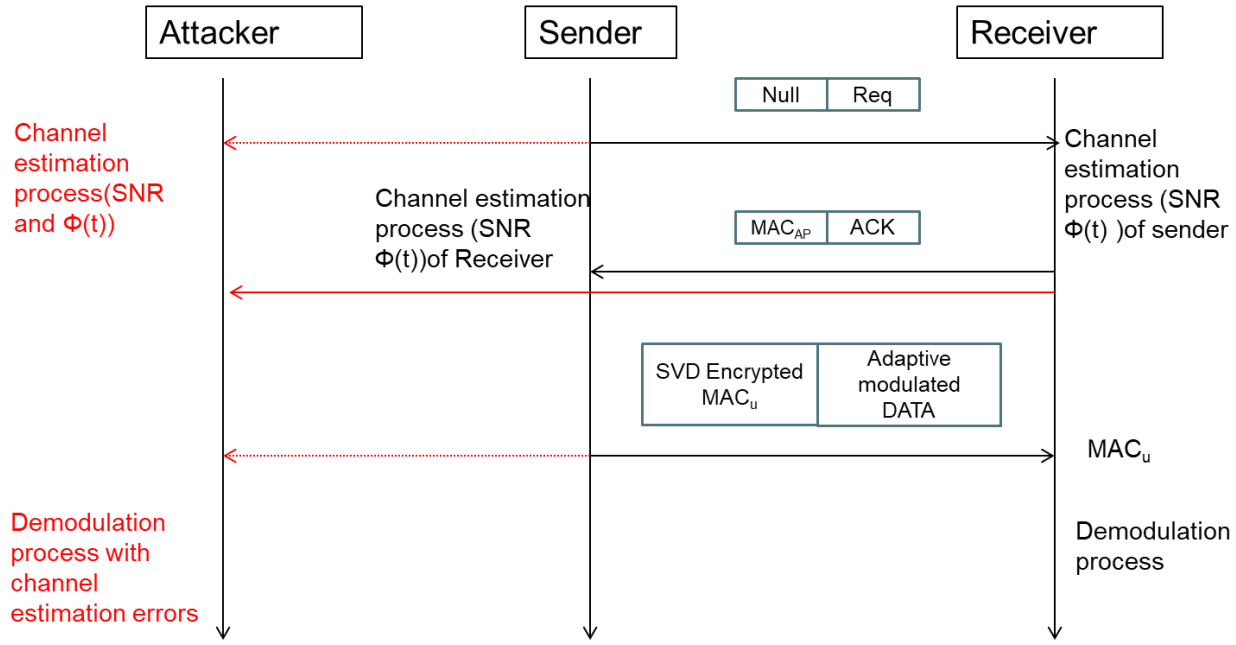

Fig 2.1. System Model of Proposed Physical layer security technique

As depicted in Fig. 2.1, the request frame sets the transmitter address as "NULL" to hide the user's MAC address from adversaries. The provider extracts the CSI information and phase from the preamble. Then, the provider returns an acknowledge frame (ACK) to the user. Data is modulated using adaptive modulation process and MAC of the user is encrypted using SVD encryption process. The user extracts the CSI information from the ACK, and uses the CSI information to encrypt the subsequent frames. The provider extracts and then finds

the matched CSI information based on previously logged mappings. Due to reciprocity of a wireless link, the phase and CSI information obtained by the user and the provider is (theoretically) identical. Therefore, the provider can use the phase and CSI information obtained at the AP side to decrypt the frame. On the other hand, even if the adversaries can eavesdrop all frames sent by the user and the provider, they cannot acquire the MAC address of the user.

2.2 SYSTEM MODEL OF PROPOSED ADAPTIVE MODULATION

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

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

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(t)* is modelled as Gaussian random variable with zero mean and unity variance, expressed in polar form as

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

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].

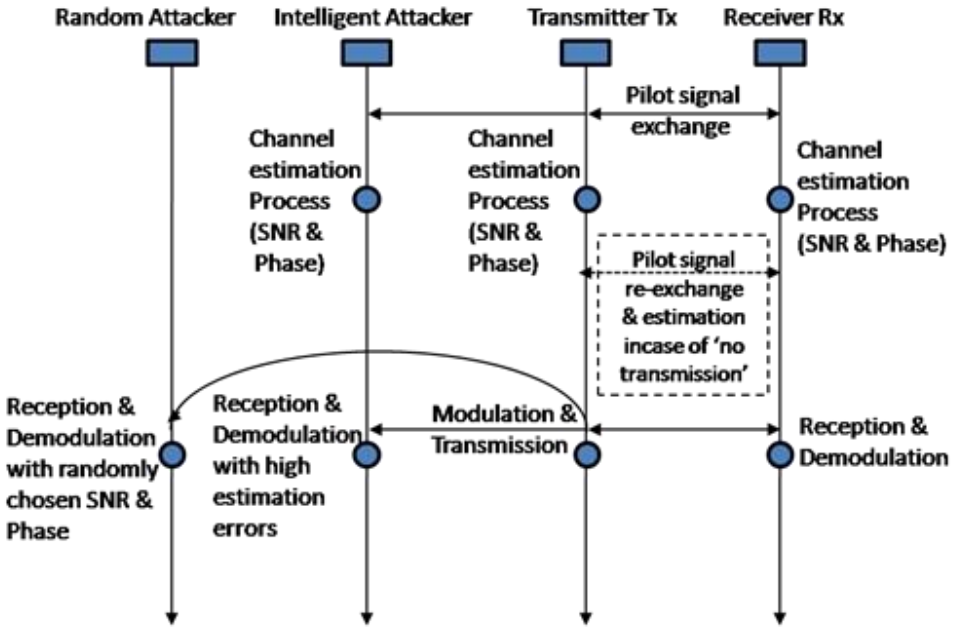

Fig.2.2 Signal flow among transmitter, receiver and attackers.

Fig. 2.2 , 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. Selection of modulation type depending on SNR was made based on the Adaptive Modulation Coding techniques (AMC) [19]-[21]. 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 $1 \leq m \leq M$ and 2^m denoting the number of symbols transmitted.

The transmitted signal *x(t)* can be expressed in polar form as

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

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.

2.2.1 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,

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

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,

$$\theta_{rot} = (\Phi(t).m) \bmod 360 \quad (5)$$

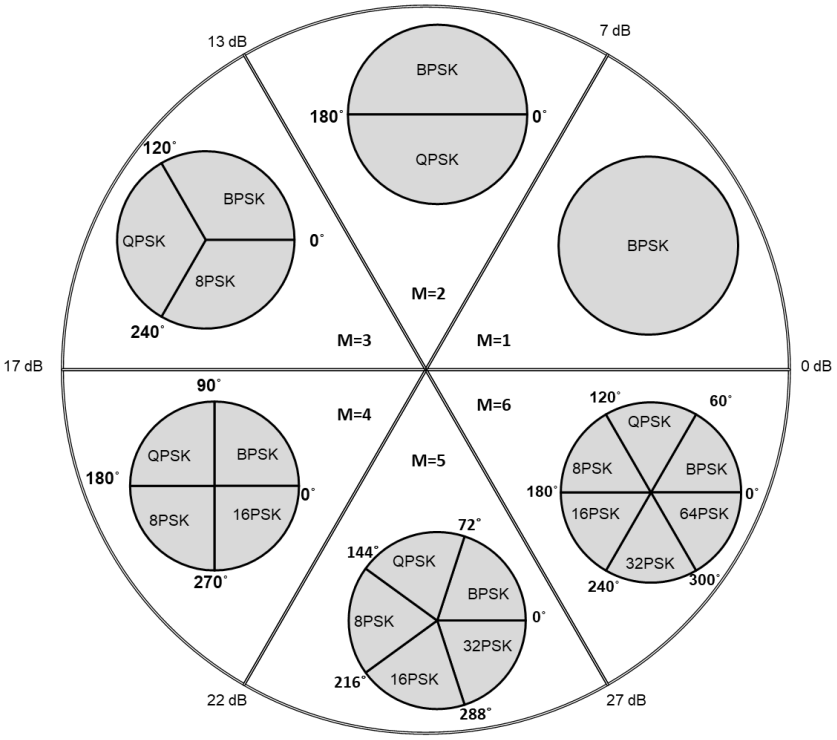

Fig.2.3 Proposed scheme using SNR and Phase for M=6

Fig. 2.3, 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.

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 forrotation and it is computed using estimated phase as mentioned in (5).

2.3 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,

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

ϵ_s is modelled as a uniform random variable in the interval $[-\rho_r, \rho_r]$, 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,

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

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

2.3.1 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,

$$\sigma_1 = \sum_{m=0}^{M-1} \varepsilon_m \left(1 - \left(\int_{\max(-\rho_r, R_{m-1}^U - \gamma(t))}^{\min(\rho_r, R_{m+1}^L - \gamma(t))} f_{\varepsilon_s} d\varepsilon_s . \right)\right) \tag{8}$$

where, ε_m is the probability that the estimated SNR $\gamma(t)$ lies in the region R_m. R_M^U and R_M^L are the upper and lower bounds of R_m respectively. The function $f\epsilon_s$ is the uniform pdf of ϵ_s and is given as,

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

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

Table 2.1 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

2.3.2 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,

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

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

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

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

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

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

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

2.4 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. 2.4 shows the representation of guard interval for SNR estimation and Fig. 4 shows the guard interval for phase estimation.

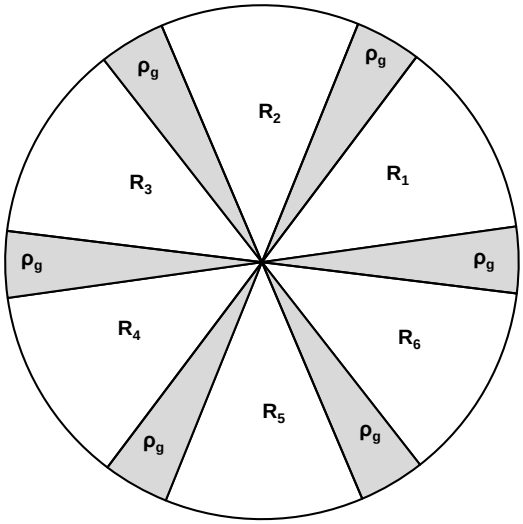

Fig. 2.4 Representation of SNR region of interest with respective guard intervals for M=6

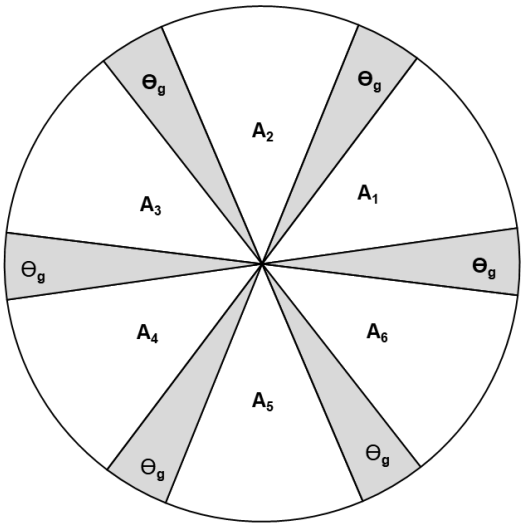

Fig. 2.5 Representation of Phase region of interest with respective guard intervals for M=6

2.5 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

$$SER_R = \sigma_r + (1-\sigma_r)\varepsilon \tag{14}$$

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 (9) and (10), 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., $\sigma_r = 0$ 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

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

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 $|\varepsilon(t)| > \frac{\pi}{2}$.

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

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

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

which can be simplified as follows,

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

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).

2.6 ATTACKER 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.

2.6.1 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].

2.6.2 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}].

2.7 SVD ENCRYPTION PROCESS SYSTEM MODEL

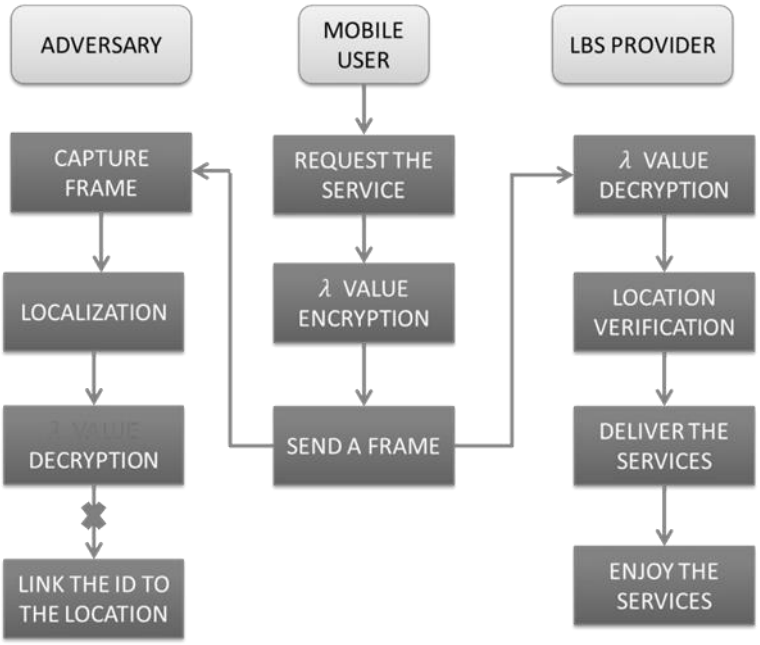

Fig 2.6. System model of SVD encryption process

Fig 2.6. First, mobile user request services from LBS provider by establishing the handshake frame with access points (AP). During handshake phase, provider and user extract CSI information of user and provider respectively which is used for generating secret key and encryption process. Frames sent by user are encrypted using generated secret key and transmitted. After receiving the encrypted frame by the provider, provider decrypts the frame using CSI information which is extracted during handshake phase and then extracts the user's identification (MAC address) and location information from received frames. Afterwards, provider uses CSI information from received frames to verify the truthfulness of the reported users location, to deliver the services to the location authenticated users.

***Algorithm 2**: Proposed Singular value decomposition*

Step 1: Compute the differential CSI vector, $[d_1, ..., d_n]$

where $d_i = c_{i+1} - c_i \quad ,\forall_i = 1, ..., n$

Step 2: Put the differential CSI values into different buckets one by one following the rule,

$d_i \rightarrow$ floor(i/L)th

Step 3: Find the maximum and minimum differential CSI values d_{max} and $d_{min.}$

Step 4: Apply SVD and use SVD applied differential CSI

Step 5: Generate four shape pattern vectors

$$v00 = [\frac{d_{min}}{n}, \ldots, \frac{id_{min}}{n}, \ldots, \frac{Ld_{min}}{n}],$$

$$v01 = [\frac{Ld_{min}}{n}, \ldots, \frac{id_{min}}{n}, \ldots, \frac{d_{min}}{n}],$$

$$v10 = [\frac{d_{max}}{n}, \ldots, \frac{id_{max}}{n}, \ldots, \frac{Ld_{max}}{n}],$$

$$v11 = [\frac{Ld_{max}}{n}, \ldots, \frac{id_{max}}{n}, \ldots, \frac{d_{max}}{n}],$$

Step 6: for each bucket

Step 7: Compute Frechet distances between the bucket and the four shape pattern vectors

Step 8: Find the vector v_i with the smallest distance

Step 9: Add the corresponding bits to k,

Step 10: Generate a vector of CFOs of length, ceil ($\frac{2n}{ML}$)

by multiply each M bits of K with singular values.

Step 11: Hash each generated CFO to singular values.

Step 12: Append each frame with singular value patterns.

CHAPTER 3

RESULTS AND DISCUSSIONS

3.1 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.

3.2 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.

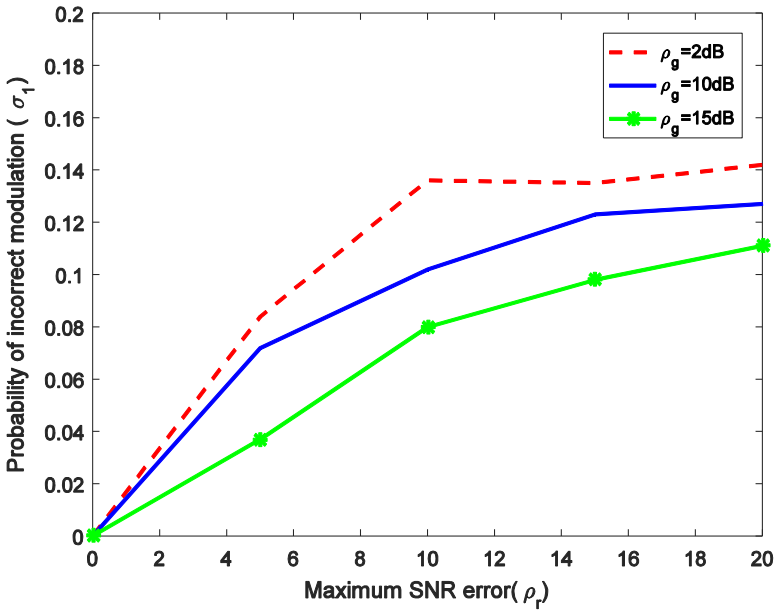

Fig. 3.1 Probability of selecting incorrect modulation type at Rx (σ_r) versus maximum SNR estimation error (ρ_r), for different SNR guard interval widths (ρ_g)

Fig. 3.1 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. 3.2 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.

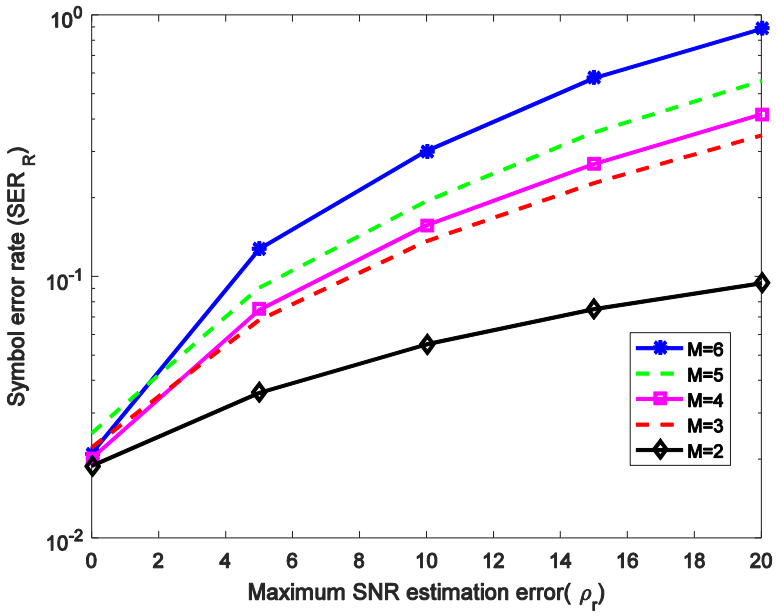

Fig. 3.2 The average SER obtained at receiver Rx versus maximum SNR estimation error (ρ_r) at Rx with a fixed SNR guard interval (ρ_g) = 2dB, for different values of M.

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, $\Theta_g = 5^{\circ}$.

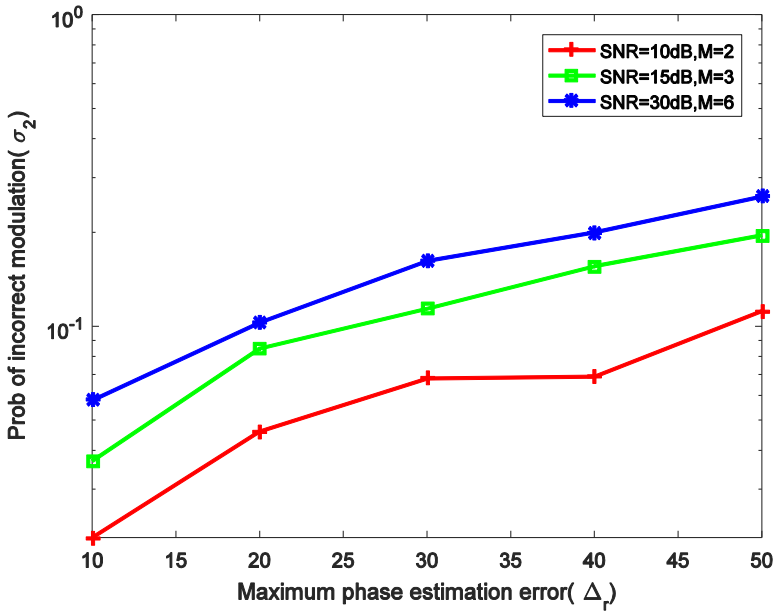

Fig. 3.3 The probability of selecting incorrect modulation type at Rx (σ_r) versus the maximum phase estimation error (Δ_r), for different SNR values.

Fig. 3.3 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. 3.4 shows the system performance in terms of SER for varying maximum phase estimation error at Rx with a fixed phase guard interval $\Theta_g = 5^\circ$ at transmitter. As expected, average SER increases with increase in maximum phase estimation error and with M as well.

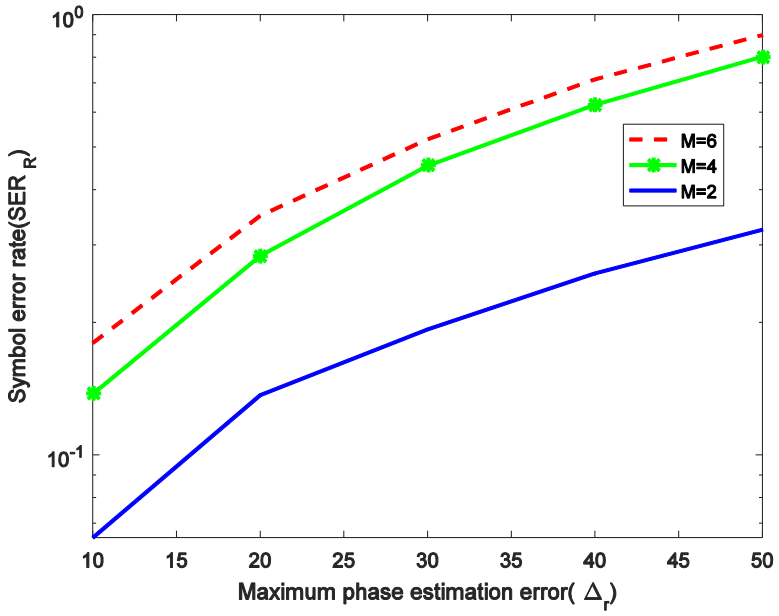

Fig. 3.4 The Average SER obtained at Rx versus maximum phase estimation error (Δ_r) for M=2, 4 & 6. (ρ_g= 2 dB and $\Theta_g = 5^{\circ}$).

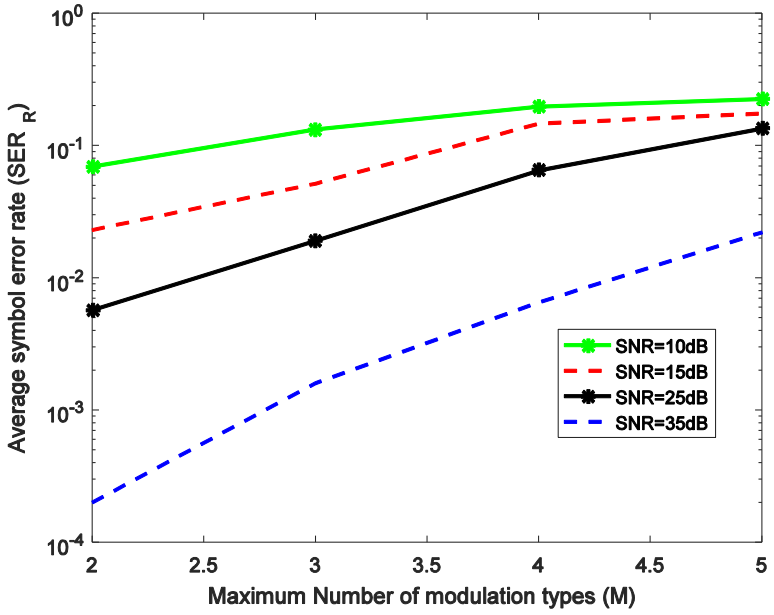

Fig.3.5 The Average SER obtained at Rx versus Maximum number of modulation types (M), for different SNR values

Fig.3.5 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.

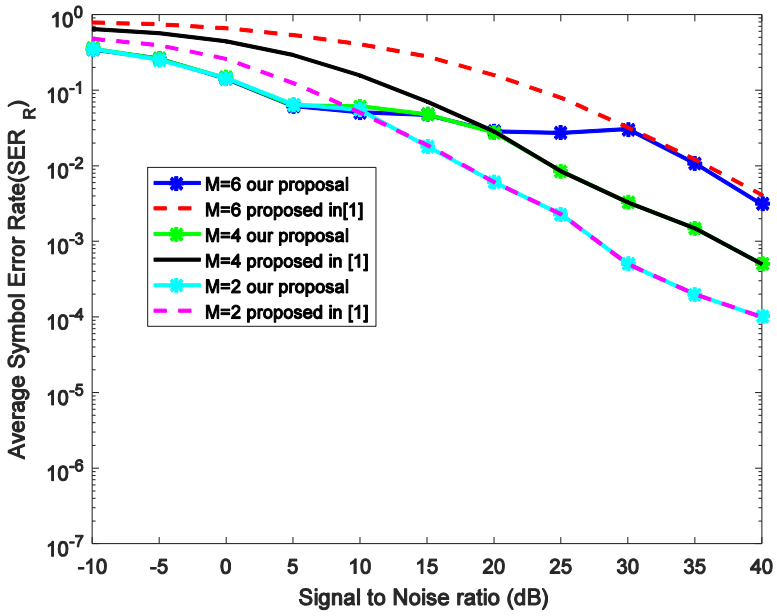

Fig.3.6 The Average SER obtained at Rx versus SNR for M = 2 & 4, for proposed and existing schemes

Fig.3.6 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 $\rho_g = \rho_r$ and $\Theta_g = \Theta_r$ 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

3.3 PERFORMANCE AGAINST ATTACKERS

The immunity of the proposed technique with two different types of attackers has been analysed. 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.

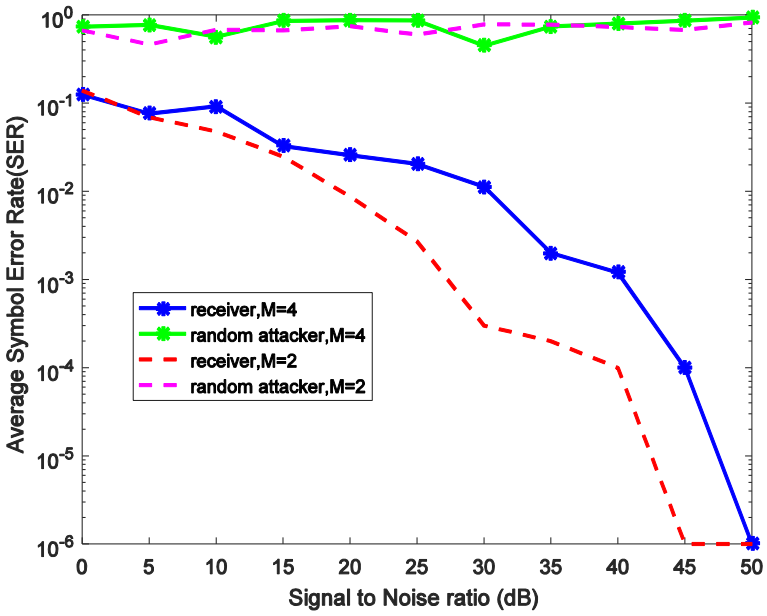

Fig. 3.7 The Average SER versus SNR for Rx and random attacker for M = 2 & 4.

Fig. 3.7 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.

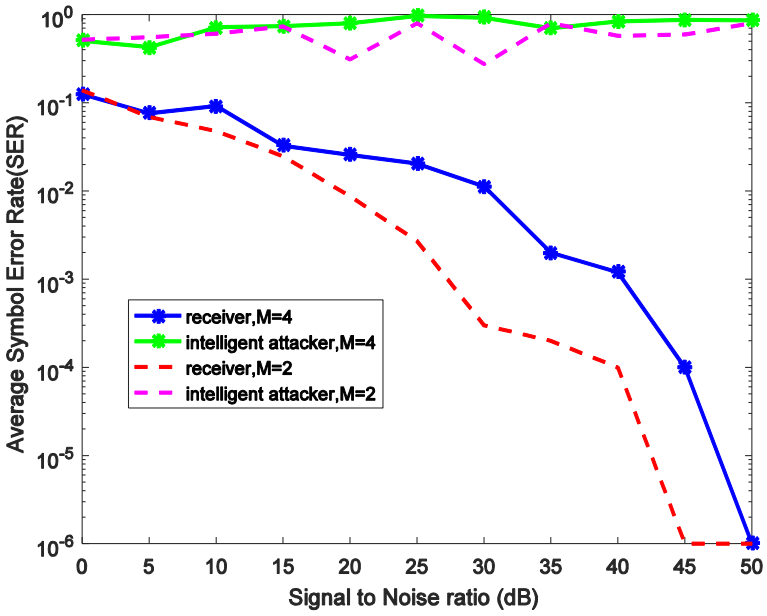

Fig. 3.8 The Average SER versus SNR for Rx and intelligent attacker for M = 2 & 4.

Similarly, the proposed technique is analysed with intelligent attacker who is assumed to possess some level of intelligence to estimate the SNR and phase. Fig. 13 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.

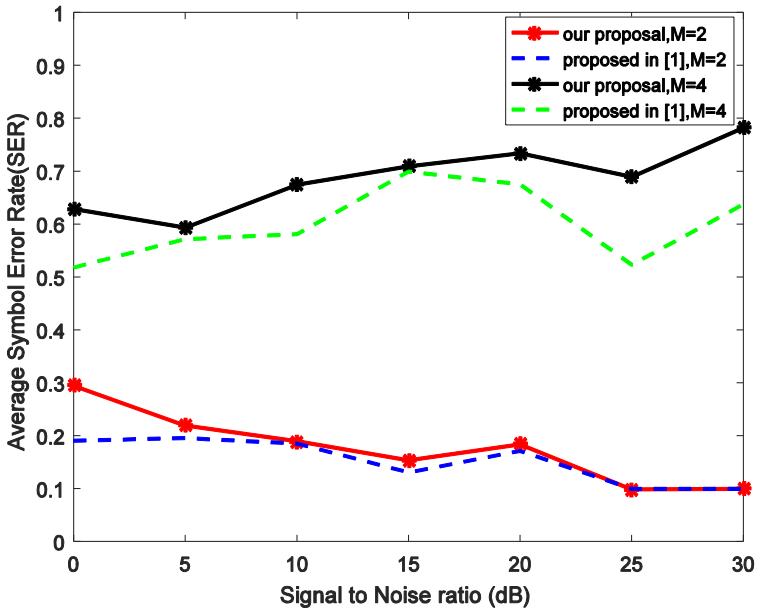

Fig. 3.9 The Average SER for random attackers versus SNR for M = 2 & 4.

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. 3.9, 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 and phase to start demodulation. Due to the three layers of adaptation, the random attacker's probability of selecting incorrect modulation is very high, resulting in high SER. 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 $[-\rho_{int}, \rho_{int}]$ and $[-\Delta_{int}, \Delta_{int}]$ 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˚].

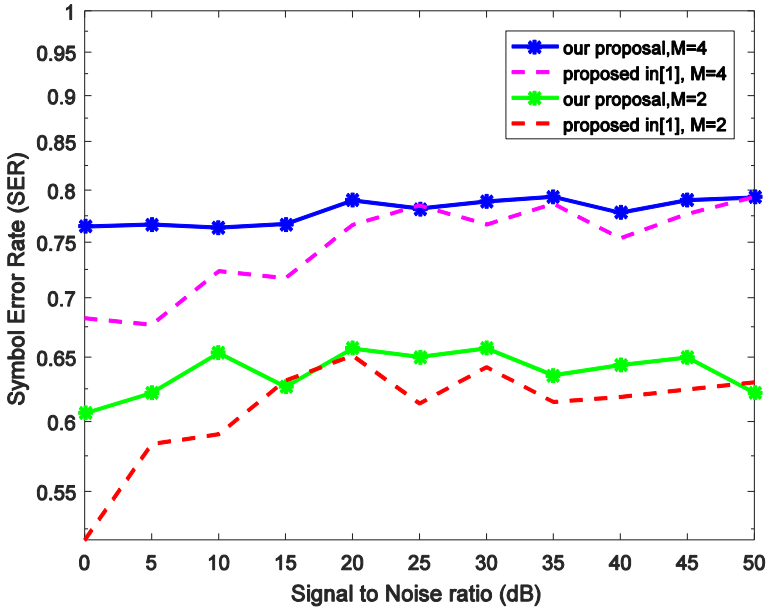

Fig. 3.10 The Average SER for intelligent attackers versus SNR for M= 2 & 4.

In Fig.3.10, 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.

3.4 PERFORMANCE OF SINGULAR VALUE ENCRYPTION

There are two metrics, i.e., mismatch rate and leakage, to evaluate the performance of singular value encryption. Mismatch rate is defined to be ratio of mismatched bits between the secret keys independently generated by the user and the provider. Mismatch rate measures the robustness of the encryption scheme. The probability of each curve pattern is computed by counting its frequency in repeated experiments. The secret bits with higher entropy contain more information, and are harder for the adversary to infer. Leakage measures the amount of information learned by the adversary. In our evaluation, leakage is defined to be the ratio of matched bits between the sender (the user or provider and the adversary. An encryption scheme with lower leakage is more secure.

3.4.1 BITS MISMATCH RATE (BMR)

- Ratio of number of bits unmatched between the secret key independently generated by USER and PROVIDER to the total number of bits.
- Measures the robustness of encryption scheme.
- Low BMR provides more security.

3.4.2 LEAKAGE

- Ratio of matched bits between user or provider and adversary.
- Encryption scheme with lower leakage is more secure.

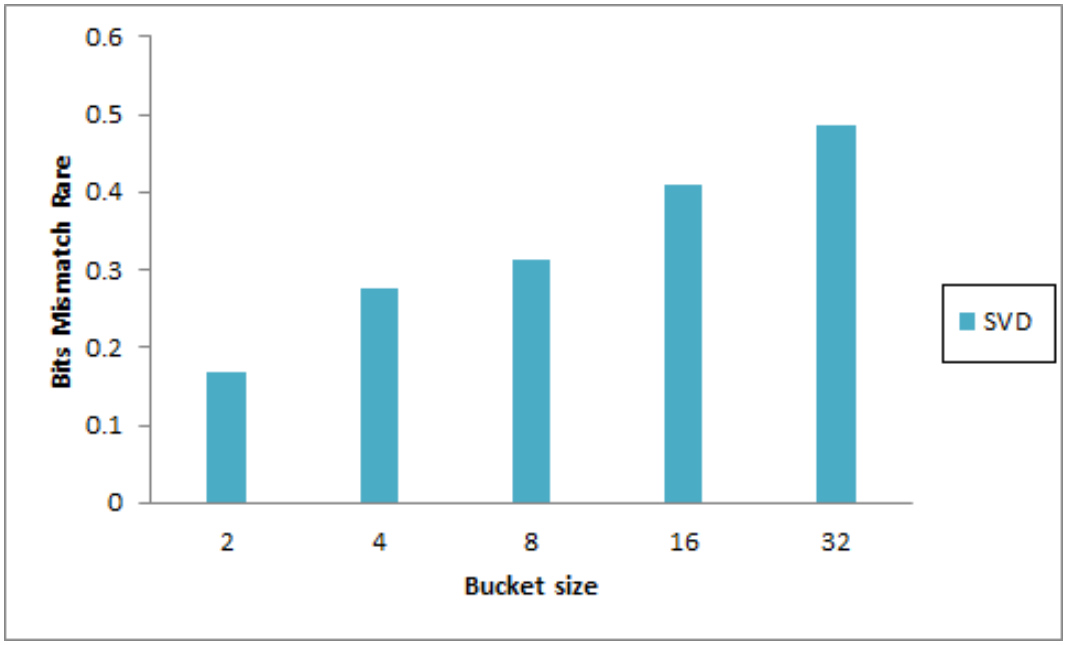

Fig. 3.11 Mismatch rate under different numbers of buckets- SVD Encryption

To verify the robustness of the SVD encryption, Measuring the mismatch rate of different schemes in Fig.3.11 the mismatch rate of SVD achieves low mismatch rate when the number of buckets is no more than 5, while the mismatch rate of SVD is significantly higher when the number of buckets grows to 10. The reason is that when the number of buckets is large, the entropy of bucket is quite small, implying low uncertainty in the bits generated by buckets. Hence, the security level of SVD in the case of large number of buckets is low. To validate the security level provided by SVD, experiments where the user and the provider are placed at a fixed distant (5 m) while the adversary is placed at various distances apart from the sender. The number of buckets is fixed to be 5. As shown in Fig.3.12, more information is leaked to the adversary with smaller distance. This is quit intuitive as nearer adversary shares more similar multipath profiles and channel responses.

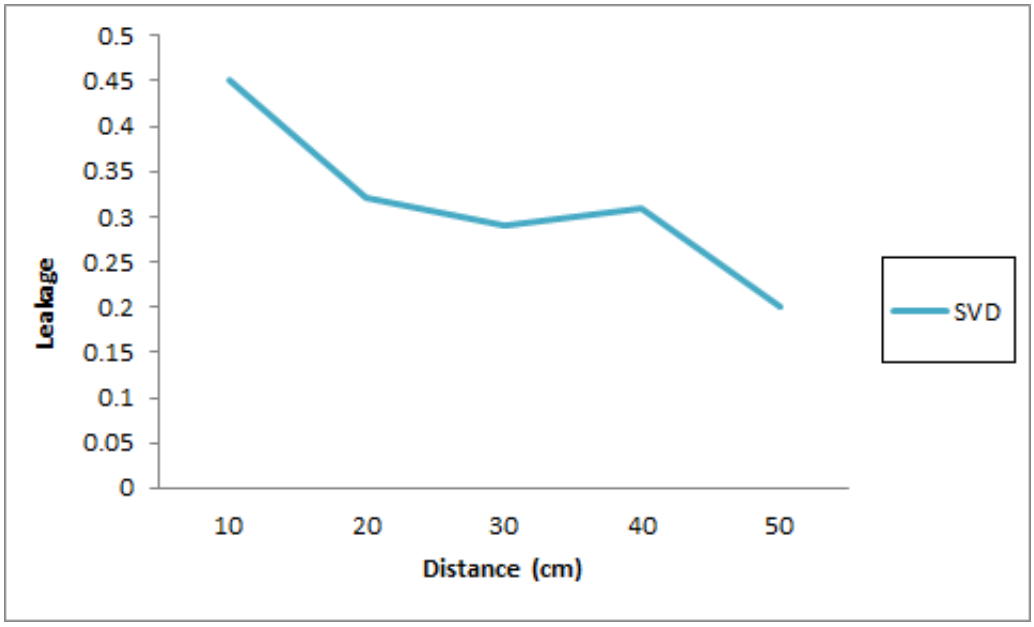

Fig. 3.12 Information leakage to the adversary with different distances- SVD Encryption

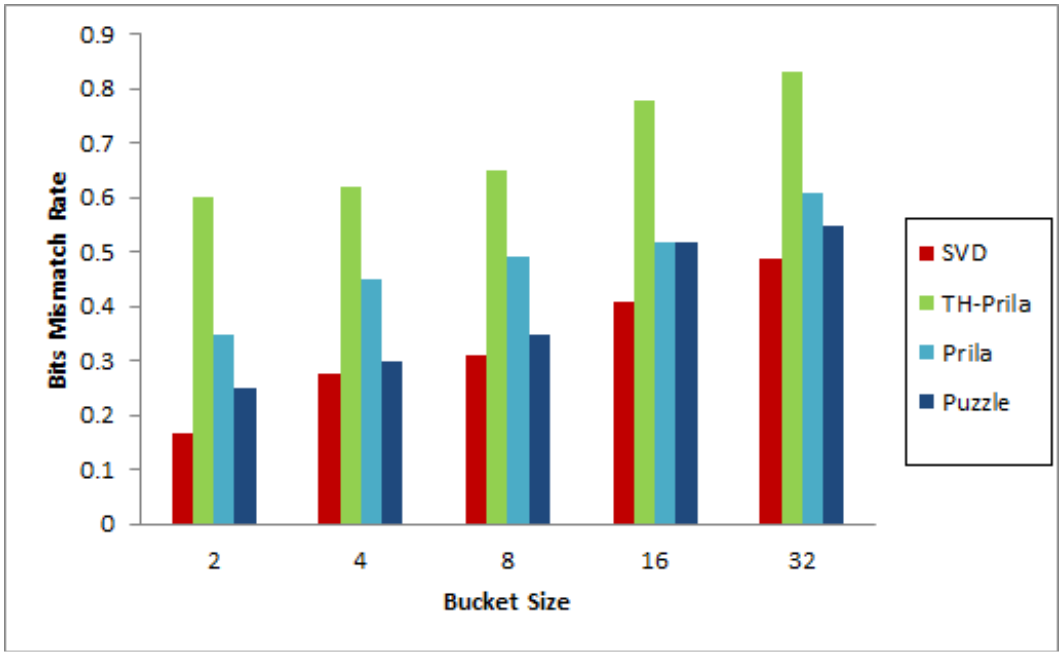

Fig. 3.13 Comparison of Mismatch rate under different numbers of buckets

SVD achieves comparable mismatch rate with Prila when the number of Fig.3.13 Mismatch rate under different numbers of buckets. Fig.19 Information leakage to the adversary with different distances, buckets is no more than 5, while the mismatch rate of SVD is significantly higher than that of Prila when the number

of buckets grows to 10. The reason is that when the number of buckets is large, the entropy of Prila is quite small, implying low uncertainty in the bits generated by Puzzle. Hence, the security level of Puzzle in the case of large number of buckets is low. Moreover, PriLA outperforms TH-PriLA in mismatch rate while enjoying comparable entropy, which implies that TLDC is more robust than the threshold-based approach. To validate the security level provided by SVD, experiments where the user and the provider are placed at a fixed distant (5 m) while the adversary is placed at various distances apart from the sender. The number of buckets is fixed to be 5. As shown in Fig.3.14, more information is leaked to the adversary with smaller distance. This is quit intuitive as nearer adversary shares more similar multipath profiles and channel responses. Besides, both SVD and PriLA leak less information compared to puzzle in all cases demonstrated. On average, SVD leaks lesser information compared to Puzzle.

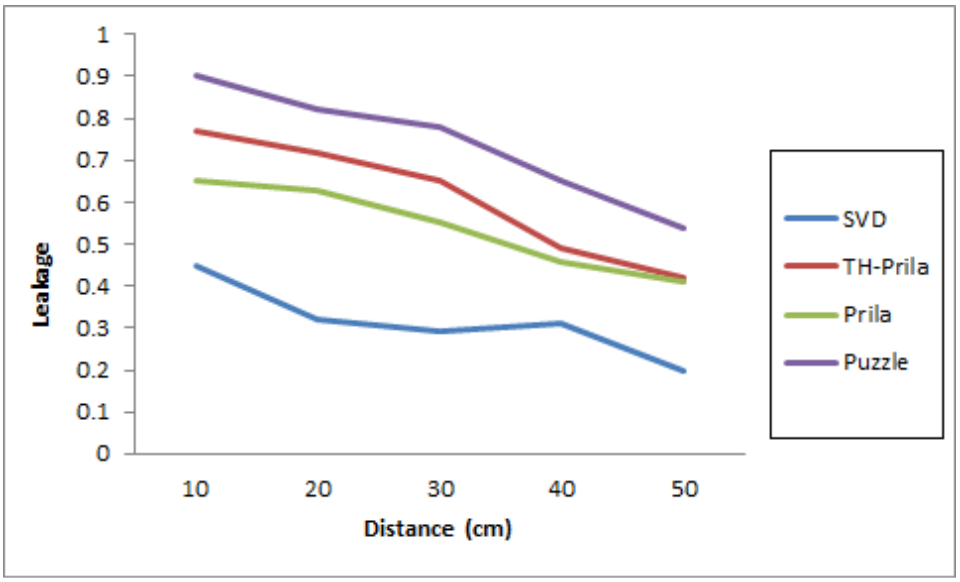

Fig. 3.14 Comparison of Information leakage to the adversary with different distances

CHAPTER 4

CONCLUSION

A new physical layer security scheme to enhance the confidentiality of the transmitted message from transmitter to receiver and against attackers and location authentication for LBS services has been proposed and analysed in this project. In this proposed scheme, four layers of security such as location authentication, 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, authentication and SER performance than the existing physical layer security schemes.

CHAPTER 5

REFERENCES

[1] Saud Althunibat, Victor Sucasas, Jonathan Rodriguez ,"A Physical-Layer Security Scheme by Phase-Based Adaptive Modulation" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 66, NO. 11, NOVEMBER 2017.

[2] L. Xiao, L. J. Greenstern, N. B. Mandayam and W. Trappe, "Channel-based spoofing detection in frequency-selective rayleigh channels," IEEE Trans. Wireless Commun., vol. 8, no. 12, pp. 5948-5956, Dec. 2009.

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

[4] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," IEEE Wireless Commun., vol. 18, no. 2, pp. 66-74, Apr. 2011.

[5] D. Shan, K. Zeng, W. Xiang, P. Richardson and Y. Dong, "PHY-CRAM: physical layer challenge-response authentication mechanism for wireless networks," IEEE J. Sel. Areas in Commun., vol. 31, no. 9, pp. 1817-1827, Sept. 2013.

[6] W. Hou, X. Wang, J.-Y. Chouinard and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," IEEE Trans. Commun., vol. 62, no. 5, pp. 1658-1667, May 2014.

[7] Y. Liu, S. C. Draper and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," IEEE Trans. Inf. Forens. Security, vol. 7, no. 5, pp. 1484-1497, Oct. 2012.

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

[9] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks,"in Proc. IEEE Conf. Comput. Commun., 2011, pp. 1422–1430.

[10] X. Li and E. P. Ratazzi, "MIMO transmissions with informationtheoretic secrecy for secret-key agreement in wireless networks," in Proc. IEEE Mil.

Commun. Conf. (MILCOM), vol. 3. Atlantic City, NJ, USA, Oct. 2005, pp. 1353–1359.

[11] C.P¨opperetal.,"Investigationofsignalandmessagemanipulationsonthe wireless channel," in Proc. Eur. Symp. Res. Comput. Security, Sep. 2011, pp. 40–59.

[12] T. Xiong, W. Lou, J. Zhang, and H. Tan, "MIO: Enhancing wireless communications security through physical layer multiple inter-symbol obfuscation,"IEEETrans.Inf.ForensicsSecurity,vol.10,no.8,pp.1678– 1691, Aug. 2015.

[13] M.I.Husain,S.Mahant,andR.Sridhar,"CD-PHY:Physicallayersecurity in wireless networks through constellation diversity," in Proc. IEEE Mil. Commun. Conf., Oct./Nov. 2012, pp. 1–9.

[14] L. Tang, J. A. Ambrose, S. Parameswaran, and S. Zhu, "Reconfigurable convolutional codec for physical layer communication security application," in Proc. IEEE Mil. Commun. Conf., Baltimore, MD, 2014, pp. 82– 87.

[15] L. Tang, J. A. Ambrose, A. Kumar, and S. Parameswaran, "Dynamic reconfigurable puncturing for secure wireless communication," in Proc. Design, Autom. Test Europe Conf. Exhib., Grenoble, 2015, pp. 888–891.

[16] G.Zang,B.Huang,L.Chen,andY.Gao,"Onetransmissionschemebased on variable MSK modulator for wireless physical layer security," in Proc. Int. Conf. Wireless Commun. Signal Process., Nanjing, 2015, pp. 1–5.

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

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

[19] A. Ijaz, A.B. Awoseyila, B.G. Evans, "Signal-to-noise ratio estimation algorithm for adaptive coding and modulation in advanced digital video broadcasting–radar cross section satellite systems", *IET Communications*, vol. 6, pp. 1587, 2012, ISSN 17518628.

[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, Vol. 2 Issue 3, March 2015.

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

[22] Y. El Hajj Shehadeh and D. Hogrefe, “An optimal guard intervals based mechanism for key generation from multipath wireless channels,”InProc. 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, VOL. 15, NO. 2, FEBRUARY 2016

[25] K. Wu, J. Xiao, Y. Yi, D. Chen, X. Luo, and L. M. Ni, “CSI-based indoor localization,” IEEE Trans. Parallel Distrib. Syst., Jul. 2013.4. J. Xiong and K. Jamieson, “Array track: A fine-grained indoor location system,” in Proc. USENIX Symp. Netw. Syst. Des. Implement. (NSDI), 2013

[26] Z. Zhu and G. Cao, “Toward privacy preserving and collusion resistance in a location proof updating system,” IEEE Trans. Mobile Comput., vol. 12, no. 1, pp. 51–64, Jan. 2013.

[27] J. Brassil, P. Manadhata, and R. Netravali, “Traffic signature-based mobile device location authentication,” IEEE Trans. Mobile Comput., vol. 13, no. 9, pp. 2156–2169, Sep. 2014