ScuDo

Scuola di Dottorato ~ Doctoral School

WHAT YOU ARE, TAKES YOU FAR

Doctoral Dissertation

Doctoral Program in Electronics and Telecommunications (29^{th}cycle)

Practical Secrecy at the Physical Layer: Key Extraction Methods with Applications in Cognitive Radio

By

Ahmed Badawy

******

Supervisor(s):

Dr. Daniele Trinchero, Supervisor

Dr. Carla-Fabiana Chiasserini, Co-Supervisor

Dr. Tamer Khattab, Co-Supervisor

Doctoral Examination Committee:

Prof. Robert Schober, Referee, IDC, Universität Erlangen-Nürnberg, Germany

Prof. Ahmed Kamal, Referee, ECE Dept., Iowa State University, USA

Prof. Emilio Leonardi, Politecnico di Torino - DET, Italy

Dr. Alessandro Nordio, IEIIT-CNR, Torino, Italy

Prof. Monica Visintin, Politecnico di Torino - DET, Italy

Politecnico di Torino

2017

Declaration

I hereby declare that, the contents and organization of this dissertation constitute my own original work and does not compromise in any way the rights of third parties, including those relating to the security of personal data.

Ahmed Badawy
2017

* This dissertation is presented in partial fulfillment of the requirements for **Ph.D. degree** in the Graduate School of Politecnico di Torino (ScuDo).

I would like to dedicate this thesis to the loving memory of my parents, my loving wife and family.

Acknowledgements

I would like to thank my PhD supervisors Dr. Daniele Trinchero, Dr. Carla-Fabiana Chiasserini and Dr. Tamer Khattab for their continuous help and support during the course of my PhD studies. Without their constant guidance and valuable feedback, I would not have been able to produce this PhD. Special thanks to my doctoral committee for their valuable time and effort in assessing my PhD work.

I would like to thank my wife, Sara, for her continuous encouragement, patience and unwavering love during the past three years. She has been my motivation and inspiration to progress with my PhD studies.

Most of all, I would like to thank God, for the blessings and sound belief in Him, health, and sanity and for putting me in a path that allowed me to meet people that have been kind to me and allowing me the opportunity to reciprocate.

This research was made possible by NPRP 6-150-2-059 grant from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the authors.

Abstract

The broadcast nature of wireless communication imposes the risk of information leakage to adversarial or unauthorized receivers. Therefore, information security between intended users remains a challenging issue. Currently, wireless security relies on cryptographic techniques and protocols that lie at the upper layers of the wireless network. One main drawback of these existing techniques is the necessity of a complex key management scheme in the case of symmetric ciphers and high computational complexity in the case of asymmetric ciphers. On the other hand, physical layer security has attracted significant interest from the research community due to its potential to generate information-theoretic secure keys. In addition, since the vast majority of physical layer security techniques exploit the inherent randomness of the communication channel, key exchange is no longer mandatory. However, additive white Gaussian noise, interference, channel estimation errors and the fact that communicating transceivers employ different radio frequency (RF) chains are among the reasons that limit utilization of secret key generation (SKG) algorithms to high signal to noise ratio levels. The scope of this dissertation is to design novel secret key generation algorithms to overcome this main drawback. In particular, we design a channel based SKG algorithm that increases the dynamic range of the key generation system. In addition, we design an algorithm that exploits angle of arrival (AoA) as a common source of randomness to generate the secret key. Existing AoA estimation systems either have high hardware and computation complexities or low performance, which hinder their incorporation within the context of SKG. To overcome this challenge, we design a novel high performance yet simple and efficient AoA estimation system that fits the objective of collecting sequences of AoAs for SKG.

Cognitive radio networks (CRNs) are designed to increase spectrum usage efficiency by allowing secondary users (SUs) to exploit spectrum slots that are unused by the spectrum owners, i.e., primary users (PUs). Hence, spectrum sensing (SS) is

essential in any CRN. CRNs can work both in opportunistic (interweaved) as well as overlay and/or underlay (limited interference) fashions. CRNs typically operate at low SNR levels, particularly, to support overlay/underlay operations. Similar to other wireless networks, CRNs are susceptible to various physical layer security attacks including spectrum sensing data falsification and eavesdropping. In addition to the generalized SKG methods provided in this thesis and due to the peculiarity of CRNs, we further provide a specific method of SKG for CRNs. After studying, developing and implementing several SS techniques, we design an SKG algorithm that exploits SS data. Our algorithm does not interrupt the SS operation and does not require additional time to generate the secret key. Therefore, it is suitable for CRNs.

Contents

List of Figures

List of Tables

Nomenclature

Acronyms

AAS Adaptive array system

AGM Arithmetic to geomteric mean

AoA Angle of arrival

AWGN Additive white Gaussian noise

BMR Bit mismatch rate

CRN Cognitive radio network

CSD Cyclostationary detection

CUMSUM Cumulative sum

dB Decibels

DoA Direction of arrival

DSP Digital signal processing

EBSS Eigenvlaue based spectrum sensing

ED Energy detection

EGC Equal gain combining

ESPRIT Estimation of signal parameters via rotational invariant technique

EVD Eigenvalue decomposition

FD Full duplex

GLRT General likelihood ratio test

HD Half duplex

HPBW Half power beam width

IFFT Inverse Fourier transform

LDPC Low densitty parity check

LGN Linear cognruential generator

LRT Likelihood ratio test

LS Least squares

MIMO Multiple input multiple output

MLRT Maximum likelihood ratio test

MME Maximum to minimum eigenvalue

MUSIC Multiple signal classification

MVDR Minimum variance distortionless

NIST National institute of standards and technology

OFDM Orthogonal frequency division multiplexing

PFR Peak to floor ratio

PU Primary user

RF Radio frequency

RMSE Root mean squared error

ROC Receiver operating characterstics

RSS Received signal strength

Rx Receiver

SBS Switched beam system

SC Selection combining

SKG Secret key generation

SLC Square law combining

SLS Square law selection

SNR Signal to noise ratio

SPRT Sequential probability ratio test

SRP Secondary random process

SS Spectrum sensing

SSC Switch and stay combining

SSDF Spectrum sensing data falsification

SU Secondary user

Tx Transmitter

UCA Uniform circular array

ULA Uniform linear array

XSBS Cross correlation switched beam system

Chapter 1

Introduction

1.1 Research Motivation

Unlike wired communications where legitimate nodes are connected to the network through cables, the broadcast nature of radio propagation mandates that wireless communications to be accessible to both legitimate and illegitimate nodes. Conventional wireless security such as symmetric ciphers require a complex key management scheme, while asymmetric ciphers have high implementation complexity. Both symmetric and asymmetric ciphering schemes lie at the upper layers of the network. Cryptographic techniques mandate the exchange of encryption keys at one point during the encryption–decryption process. This poses a serious threat to the secrecy of the whole communication session (i.e., becomes a security bottleneck). Minimization of the security risk, stemming from key exchange mechanisms, is the main reason that cryptographic secrecy opts for key reuse (i.e., using the same key for multiple packet encryptions), which introduces another secrecy weakness allowing an eavesdropper to have more chances on guessing the encryption key. In addition, current cryptographic techniques rely on the assumption of limited computational capabilities at the eavesdropper. However, with the fast growth of computational power in modern computers and the rise of quantum computing, restricted computational power assumption at the eavesdropper can be violated.

On the other hand, physical layer security relies on randomness characteristics inherent in communication channels, which are common to the two trusted parties, while being unknown to a potential eavesdropper. Thus, key exchange is no longer

mandatory and key renewal is potentially possible for every packet transmission rendering the secrecy potential higher than upper layers cryptographic methods while maintaining lower computational complexity [1].

The wiretap channel, first presented by Wyner in 1975 [2], models two legitimate nodes communicating through a noisy channel and an adversary receiving a deteriorated version of the exchanged signals between the legitimate parties through a wiretap channel. The paper studied the maximum secured transmission rate between the two legitimate nodes while minimizing the amount of information leaked to the wiretapper, i.e., eavesdropper. The paper concluded that an 'approximately perfect' secret communication between the two legitimate nodes is achievable up to a specified rate without the use of secret keys. This paper presented the early studies on the theoretical aspects of physical layer security.

In relatively recent literature [3–5], researchers started to exploit the randomness in some physical layer characteristics as a potential source for key generation to guarantee information hiding from eavesdroppers or in other words bound the amount of information leaked to un-authorized nodes. These physical layer characteristics have to be common to the two legitimate nodes and not shared with the adversarial users. In other words, an estimation of this physical layer characteristic should be approximately the same if measured from the receivers of either of the legitimate nodes. In addition, the physical layer characteristic used to generate the secret key should be randomly changing. Hence, the physical layer characteristic is also referred to as a *common source of randomness*.

Typically, in the wiretap channel paradigm, the adversary (i.e., eavesdropper), *Eve*, can listen to all communications between the two trusted parties (i.e., communicating nodes), *Alice* and *Bob*. Eve can estimate the channel between itself and both Alice and Bob. In addition, it can estimate the distances between itself and Alice and Bob. Eve can move freely within the field and can visit any of the locations where either Alice or Bob were or will be in the future. Eve, however, can not be in very close proximity (i.e., within few wavelengths) to either Alice or Bob to ensure that the collected signals are not correlated[1]. There is no limitation on the number of the antennas Eve is equipped with nor its computational capabilities. It is assumed that

[1] From a practical perspective this would make the presence of Eve detectable by either Alice or Bob.

Eve is not capable of pursuing denial of service attack, person in the middle attack or jamming attack[2]. Therefore, it is assumed that Eve is a passive adversary.

One main advantage of exploiting channel estimates to generate the secret key is its high key generation rate. However, a major downside of using the channel reciprocity for secret key generation (SKG) is that the additive white Gaussian noise (AWGN) along with interference and estimation errors affect the reciprocity of the channel measurements [6]. Moreover, involved transceivers employ different radio frequency (RF) chains, i.e., chains with different characteristics, and therefore introduce different RF imperfections, which further affect the channel reciprocity. This drawback causes the bit mismatch rate (BMR) between the legitimate nodes to rise, which affects the operation of SKG based on channel estimates, particularly, at low and medium signal to noise ratio (SNR) scenarios. This issue was stated as one of the challenges of physical layer security in [7]. Hence, developing novel SKG algorithms that can operate at medium and low SNR levels is vital.

Cognitive radio networks introduce the idea of dynamic spectrum allocation. They allow for higher spectrum efficiency through dynamically assigning the spectrum access [8]. In cognitive radio networks, secondary user (SU) access the spectrum whenever the primary user (PU) is not using it. Therefore, reliable spectrum sensing is the core for any cognitive radio network. Cognitive radios can work both in opportunistic (interweaved) as well as overlay and/or underlay (limited interference) fashions. Cognitive radio networks typically operate at low SNR (particularly to support overlay/underlay). Securing the communication between legitimate SUs is a challenging issue due to the fact that numerous attacks can be launched against cognitive radio networks. Comprehensive studies on this aspect [9–11] show that two of the major physical layer attacks against cognitive radio networks are spectrum sensing data falsification (SSDF) and eavesdropping. SSDF is performed on a collaborative sensing setup [12]: an attacker sends false spectrum sensing data to other SUs, in case of distributed sensing decision, or to the fusion center [13], resulting in a wrong spectrum access decision.

Conventional techniques to combat SSDF leverage a two-level defense mechanism [14]. The first level authenticates all the collected spectrum sensing results, while the second decides which spectrum sensing result is legitimate. Depending on

[2]The reader is referred to the references within [1] for further information on these types of attacks, called *active attacks*.

whether a fusion center is available or the system is fully distributed, schemes such as the sequential probability ratio test (SPRT) [14], or reputation-based schemes can be exploited [14]. Techniques designed to counteract SSDF, however, require a long processing time for the two stages to occur. Moreover, either a large number of SUs or many successful iterations are needed to achieve a good reputation. Clearly, long processing time might lead to higher probability of missing the opportunity of exploiting empty spectrum slots for SUs. In addition, authentication techniques such as the approach in [15], where cyclo-stationary detection is used to classify and authenticate signals, adds to the complexity and limitations of the system, while failing to prevent a scenario where a malicious node mimics the SU's signal properties.

Exploiting the concepts of physical layer security within the context of cognitive radio network could have numerous advantages over existing security techniques. Therefore, developing novel physical layer security schemes that suits the peculiarity of cognitive radio networks is essential.

1.2 Research Contributions

The main contributions of this dissertation are summarized as follows:

- We survey the most popular common sources of randomness exploited for secret key generation within the context of physical layer security. We present the steps needed to extract a secret key from different physical layer characteristics. In addition, metrics used to evaluate the generated secret key are studied.
- We design a novel SKG algorithm based on combined estimates of channel gain and phase. We create a secondary random process from the estimated channel gain and phase and use it to generate the secret key. The generated secret key through the channel secondary random process has much lower BMR when compared to the key generated through conventional channel gain and phase estimates.
- We develop a novel algorithm that exploits angle of arrival (AoA) as a common source of randomness to generate a secret key. In addition, we design a novel AoA estimation system that has low hardware and computational complexities to be used in the context of secret key generation.

- We develop an algorithm that exploits the combined channel and distance measurements to generate a secret key. We collect channel measurements from lab indoor environment through WARP hardware platform.
- We design spectrum sensing techniques within the context of cognitive radio networks.
- We design a SKG algorithm that exploits general likelihood ratio based spectrum sensing statistics as a base for SKG.

1.3 PhD Research Outcomes

The outcomes for the conducted research during the course of this PhD dissertation are summarized as follows:

1.3.1 Patents

[1] **A. Badawy**, T. Khattab, D. Trinchero, T. Elfouly and A. Mohamed "Method and Apparatus for Simple Angle of Arrival Estimation", US Patent Application No 15268371.

- **A. Badawy**, T. Khattab, D. Trinchero, T. Elfouly and A. Mohamed "Method and Apparatus for Accurate Low Complexity Direction of Arrival (DoA) Estimation of Wireless Radio Frequency Signals," US provisional Patent Application No 62/219,617.

[2] **A. Badawy**, T. Khattab, T. Elfouly, C. Chiasserini, A. Mohamed and D. Trinchero "Method for Generation a Secret Key for Encrypted Wireless Communications," US provisional Patent Application No 62339797 filed on May 20th, 2016.

[3] **A. Badawy**, T. Khattab, T. Elfouly, C. Chiasserini and D. Trinchero "Non-Coherent High performance UWB Receiver'," Submitted Application to University's IP Office.

1.3.2 Journal articles

[1] **A. Badawy**, T. Khattab, D. Trinchero, T. ElFouly and A. Mohamed, "A Simple Cross Correlation Switched Beam System (XSBS) for Angle of arrival Estimation," in IEEE Access, vol. 5, no. , pp. 3340-3352, 2017. This work is presented in Chapter 4

[2] A. Noel, A. Abddouli, **A. Badawy**, T. Elfouly, M. Hossam and M. Shehata "Structural Health Monitoring using Wireless Sensor Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials , vol.PP, no.99, pp.1-22.

[3] **A. Badawy**, T. Salman, T. Elfouly, A. Mohamed, T. Khattab and M. Guizani "Estimating the number of sources: Simple Eigenvalues Based Approaches," Accepted in IET Signal Processing.

[4] **A. Badawy**, T. Elfouly, T. Khattab, A. Mohamed and M. Guizani "Unleashing the secure potential of the wireless physical layer: Secret key generation methods," Elsevier, Physical Communication, Volume 19, June 2016, Pages 1-10, ISSN 1874-4907. This work is presented in Chapter 2.

[5] **A.Badawy**, Elfouly, T., Khattab, T., Chiasserini, C. -F., Mohamed, A., and Trinchero, D. "Robust secret key extraction from channel secondary random process," Wiley, Wireless Communication and Mobile Computing, 16: 1389-1400. doi: 10.1002/wcm.2695. This work is presented in Chapter 3

[6] **A. Badawy**, T. ELfouly, T. Khattab, C.-F. Chiasserini, and D. Trinchero "Exploiting Spectrum Sensing Data to for Key Management", Elsevier, Computer Communications, Volume 97, 1 January 2017, Pages 31-39, ISSN 0140-3664, http://dx.doi.org/10.1016/j.comcom.2016.10.008.
This work is presented in Chapter 5

[7] **A. Badawy**, and R. Wolff, "A hardware based ricean fading radio channel simulator," Springer, Wireless Personal Communications, Volume 93, pp. 615-727, 2017. [Online]. Available: http://dx.doi.org/10.1007/s11277-014-2217-x.

1.3.3 Submitted journal articles

[1] **A. Badawy**, T. Khattab and T. Elfouly "A comprehensive Study on Spectrum Sensing Techniques in Cognitive Radio Networks from Theory to Implementation: A Survey" submitted to Sensors.

1.3.4 Journal articles drafts

[1] **A. Badawy**, T. Khattab, T. Elfouly, C-F Chiasserini and D. Trinchero, "On Non-coherent UWB Receivers: Revamping Single Sample Threshold Detection via Order Statistics," to be submitted to IEEE Communication Letters.

[2] **A. Badawy**, T. Khattab, T. Elfouly, C-F Chiasserini and D. Trinchero, "On Practical Quickest Detection of Primary Users in Cognitive Radio Communications," to be submitted to IEEE Transaction of Cognitive Communication and Networking. This work is presented in Chapter 5

[3] **A. Badawy**, K. Allidina, T. Khattab, M. Elgamal and T. Elfouly, "Performance Analysis of Non-coherent UWB Receiver Under Nakagami Fading Channel in the Presence of Narrowband Interference ," to be submitted to IEEE Transaction on Wireless Communications.

1.3.5 Conference publications

[1] **A. Badawy**, T. Khattab, T. ElFouly, A. Mohamed, and D. Trinchero, "Secret key generation based on channel and distance measurements," in Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2014 6th International Congress on, Oct 2014, pp. 136-142.
This work is presented in Chapter 4

[2] T. Salman, **A. Badawy**, T. Elfouly, T. Khattab, and A. Mohamed, "Non-data aided SNR estimation for QPSK modulation in AWGN channel," in Wireless and Mobile Computing, Networking and Communications (WiMob), 2014 IEEE 10th International Conference on, Oct 2014, pp. 611-616.

[3] **A. Badawy**, T. Khattab, T. M. Elfouly, C.-F. Chiasserini, A. Mohamed, and D. Trinchero, "Secret key generation based on AoA estimation for low snr

conditions," in 2015 IEEE 81st Vehicular Technology Conference (VTC spring 2015), Glasgow, Scotland, May. 2015. This work is presented in Chapter 4

[4] **A. Badawy**, T. Khattab, T. M. Elfouly, C.-F. Chiasserini, A. Mohamed, and D. Trinchero, "Channel secondary random process for robust secret key generation," in IWCMC 2015 Security Symposium (IWCMC 2015 Security Symposium), Dubrovnik, Croatia, Aug. 2015. This work is presented in Chapter 3

[5] T. Salman, **A. Badawy**, T. M. Elfouly, A. Mohamed, and T. Khattab, "Estimating the number of sources: An efficient maximization approach," in IWCMC 2015 Comm & Signal Processing Symposium (IWCMC 2015-Comm & Signal Processing), Dubrovnik, Croatia, Aug. 2015.

[6] **A. Badawy**, T. Khattab, T. Elfouly, C. F. Chiasserini and D. Trinchero, "On the performance of spectrum sensing based on GLR for full-duplex cognitive radio networks," 2016 IEEE Wireless Communications and Networking Conference, Doha, 2016, pp. 1-6. This work is presented in Chapter 5

[7] **A. Badawy**, T. Khattab, T. Elfouly, C. Chiasserini and D. Trinchero "Performance of Eigenvalue Based Spectrum Sensing in Full-Duplex Cognitive Radio Networks," 2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Vancouver, BC, 2016, pp. 1-6.

[8] **A. Badawy**, T. Khattab, D. Trinchero, T. Elfouly and A. Mohamed "A simple AoA Estimation System," 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 2017, pp. 1-6.
This work is presented in Chapter 4

1.4 Dissertation Outline

The rest of the dissertation is organized as follows:

- **Chapter 2** surveys the different common sources of randomness used for SKG. Most common steps used to extract the secret key from the common source of randomness are investigated. Furthermore, both statistical and information theoretic metrics used to evaluate the generated secret key are presented.

- **Chapter 3** presents our novel channel based SKG algorithm. The presented SKG method relies on extracting a secondary random process from combined channel gain and phase estimates. The extracted secondary random process is used for SKG.

- **Chapter 4** introduces our newly developed algorithm that exploits the AoA as a common source of randomness for SKG. AoA based SKG can operate with high efficiency at very low SNR levels. A novel AoA estimation system that uses a single RF receiver is also presented. Moreover, a SKG algorithm based on channel and distance measurements is presented.

- **Chapter 5** presents the basic concepts of different methods for cognitive radio networks. Design and analysis of likelihood ratio based spectrum sensing are presented. In addition, issues and drawbacks of current security schemes in cognitive radio networks are discussed. An algorithm that exploits spectrum sensing data for secret key generation is then presented.

- **Chapter 6** concludes the dissertation and highlights the key findings and directions for future work.

Chapter 2

Secret Key Generation Methods

2.1 Introduction

The objective of this chapter is to present the fundamentals of secret key generation in an explicit way. The flow of this chapter is organized as follows. In Section 2.2, we survey the most common physical layer characteristics used as common sources of randomness to generate the secret key. The steps used to extract the key from the estimated physical layer characteristic is presented in Section 2.3. We then present the metrics used to evaluate the strength of the secret key in Section 2.4. The chapter is concluded in Section 2.5. Our work in this chapter is presented in [16].

2.2 Common Sources of Randomness

Several characteristics of the physical layer link between the two communicating legitimate nodes, Alice and Bob, are shared only between them, while the eavesdropper, Eve, can only measure these characteristics between itself and each node separately as depicted in Figure 2.1. The measures available to Eve may be (or may be not) correlated to the characteristics shared between Alice and Bob. The most commonly used physical layer characteristic as a common source of randomness is channel randomness. Received signal strength can also be used for SKG. However, exploiting distance as a reciprocal physical layer characteristic is limited due to reasons provided in the discussion below.

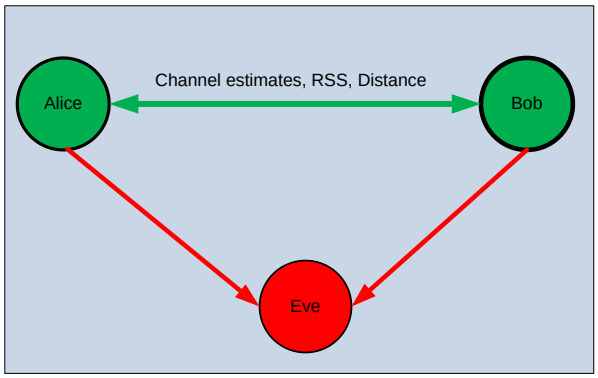

Fig. 2.1 Common physical layer characteristics used for secret key generation between two authorized nodes Alice and Bob and an eavesdropper, Eve, listening to the communication between them.

2.2.1 Channel estimates

One well known property of the communication channel is the reciprocity of its effects. When two antennas communicate by radiating the same signal through a linear and isotropic channel, the received signals by each antenna will be identical. This is mainly because of the reciprocity of the radiating and receiving antenna pattern [17, 18].

Most current physical layer security techniques are based on the channel reciprocity assumption. One of the pioneering work on secret key generation based on channel reciprocity was presented in [3]. They concluded that the maximum size of the generated secret key mainly depends on the mutual information between the channel estimates at the two legitimate nodes. They also derived an expression for the mutual information for a general multipath channel. The most common feature of the channel characteristics that is widely used is the channel gain; mainly because of its ease of extraction [19, 20]. In [19], the authors studied the channel probing rate effect on the secret key rate for different doppler shifts. They found that secret key rate increases as the probing rate increases and saturates at 20 KHz probing rate for the worst case doppler shift they assumed of 100 Hz. The smaller the doppler shift the smaller the probing rate required to saturate the secret key rate. In [20], the authors observed that as the carrier frequency increases, the probing rate should increase to achieve a suitable key rate. This is mainly because the channel's temporal variation increases at higher carrier frequencies.

In [21], the authors studied the theoretical limits of the SKG when Eve's channel is correlated with Alice-Bob's channel. Furthermore, they developed a quantization mechanism to mitigate errors by exploiting guard band to separate decision areas. This guard band based technique is further developed in [22]. SKG algorithms are also further investigated under a multiple input multiple output (MIMO) scheme as in [23], the authors developed a SKG technique that exploits the eigenvalues of the composite round trip channel to generate the secret key. In addition, a SKG technique that uses the precoding matrix in MIMO OFDM system is presented in [24], while the authors in [25] present a SKG algorithm in massive MIMO system when the eavesdropper launches a pilot contamination attack.

Secret key generation algorithms in relay assisted channels are presented in [26, 27], while [28] studies SKG when the relays are untrusted. In [27], it was assumed that there is no direct channel between the two communicating nodes, Alice and Bob. Their SKG technique showed a key rate that is larger than the rate of the direct channel.

Others exploit the channel phase to generate the secret key as in [29–32]. Unlike the channel gain, the channel phase is uniformly distributed. The authors in [29] and [30], which were published in 1996 and 1998, respectively, were able to generate a *long* key as compared to the conventional cryptographic techniques from the estimated channel phase, while in [31], they extend their system to the use of relay nodes. In [33], the authors developed a quantization algorithm to exploit channel phase in SKG.

One main advantage of exploiting channel estimates to generate the secret key is its high key generation rate. However, a main drawback of exploiting the channel reciprocity to generate secret keys is that the additive white Gaussian noise (AWGN) at both receivers, interference, estimation errors and the fact that involved transceivers could employ different RF chains affect the reciprocity of the channel measurements. Also, both nodes must collect the measurement simultaneously [6].

2.2.2 Received signal strength

Other reciprocal (common) parameters such as received signal strength (RSS), which is a measure of the received signal's power, can be used as a common source of randomness to generate the secret key [4]. Available results show that it would

require a signal to noise ratio (SNR) of at least 20 dB to generate a secret key with appropriate agreement. A practical implementation of RSS based secret key generation, presented in [34] shows that it would require a highly mobile scenario to generate a secret key with acceptable entropy, i.e., key randomness. In IEEE 802.11, RSS is exploited for SKG [35, 36] and also in IEEE 802.15.4 [37–39].

RSS is a very common metric that requires a simple circuitry to be extracted. Nevertheless, its practical utilization as a common source of randomness is limited because its key bit generation rate is very low, particularly, for mobile scenarios [40].

2.2.3 Distance

A recent physical layer security technique that is based on the distance reciprocity to generate secret key bits is presented in [5]. SKG based on distance is best suited for mobile scenarios. The authors in [5] studied the theoretical achievable secret key bit rate in terms of the observation noise variance at the legitimate nodes and the eavesdropper. They also tested their algorithm using of-the-shelf radios. Most of the currently deployed localization techniques exploit the RSS to estimate the distance between the two communicating nodes [41]. Estimating the distance based on RSS requires an accurate modelling of the channel between the nodes. Moreover, it has a low estimation accuracy. This implies that the secret key generated based on distance will have a high BMR. There are other techniques to perform distance measurements which are based on the time of arrival (TOA). Although distance measurements based on TOA has a higher accuracy than RSS based, it requires clock synchronization between the two nodes. Nevertheless, TOA based distance estimation error is high at low SNR (< 0 dB).

SKG based on distance estimation is useful for mobile scenarios where either or both of the two nodes are moving, therefore, the distance between the two legitimate nodes changes. On the other hand, a secret key generated based on the distance between the two communicating nodes is susceptible to be recovered by an eavesdropper that is equipped with angle of arrival (AoA) estimation capabilities. In this case, the eavesdropper estimates the AoA for both signals received from the two nodes as well as the distances between itself and the two nodes. The eavesdropper then easily estimates the distance between the two nodes. Once the distance between the nodes is estimated, the secret key is recovered by the eavesdropper.

2.3 Secret Key Generation Steps

The steps to generate the secret key from the physical layer characteristics are based on whether a single or multiple common sources of randomness are used to extract the key. It is inherited that both Alice and Bob have already agreed on the common source(s), which will be used to generate the key. The vast majority of the current research work exploits only a single common source of randomness, i.e., 1-D. We explore the possibility of exploiting combined multiple common sources of randomness and show how the technique used to extract the secret key will differ. We first present the steps needed to extract the key exploiting 1-D common source of randomness followed by the addition needed to extract the key in case of multiple common sources of randomness.

2.3.1 Exploiting 1-D common source of randomness to extract the key

A block diagram of the steps needed to extract the key from a single common source of randomness is shown in Figure 2.2. The block diagram includes all the necessary steps involved in the process of secret key generation. The two legitimate nodes start by an initializing phase followed by estimating the underlining common randomness. Quantization, encoding, information reconciliation and privacy amplification steps are followed to convert the common randomness into a bit stream. The output of the block diagram is the secret key, which both legitimate nodes use to encrypt the transmitted data. The detailed steps are:

Initialization

This step is also known as *beacon exchange*. Both Alice and Bob start to exchange signal from which the physical layer characteristic will be estimated. Multiple beacon exchange might be needed based on the required length and rate of the key.

Common Source of Randomness Estimation

Based on the received signal from the other legitimate node, both Alice and Bob estimate the physical layer characteristic. For example, when exploiting channel randomness to generate the secret key, Alice and Bob could use the received signal, in this case the pilot signal, along with a channel estimation technique such as least squares or minimum mean square to obtain the channel estimates.

Quantization & Encoding

Now that we have the common sources of randomness estimated at both Alice and Bob, the third step is to convert them into a bit stream suitable for the secret key generation. The conventional secret key length is between 128 and 512 bits [19]. The most popular technique for quantization is the uniform quantization. When using n_q bits as the number of quantization bits, there will exist 2^{n_q} levels to quantize the common sources of randomness. The quantized decimal valued are then converted into bits. Moreover, the authors in [42–44] use a multi bit quantization technique, which uses multiple thresholds and which differ based on the selection of the threshold, to reduce the quantization error. Although uniform quantization is easy to implement, increasing the quantization bit number, dramatically degrades the performance of the algorithm since the bit mismatch rate between the two communicating nodes increases. In [45], an encoding algorithm is proposed to tackle this problem where each uniformly quantized value is encoded with multiple values, n_e bits. Moreover, Gray coding can be used to reduce the BMR.

Information Reconciliation

The generated bit streams at Alice and Bob will have some discrepancy, particularly at very low SNR levels. This is due to several reasons such as interference, noise and hardware limitations. A reconciliation protocol such as the one presented in [46] can be used to minimize the discrepancy. Both Alice and Bob first permute their bit streams in the same way. Then they divide the permuted bit stream into small blocks. Alice then sends permutations and parities of each block to Bob. Bob then compares the received parity information with the ones he already processed. In case of a parity mismatch, Bob changes his bits in this block to match the received ones. Another

approach for information reconciliation is presented in [47], where the reconciliation step is treated as a source coding with side information problem. In this case, Alice compresses her collected common source of randomness data and Bob decodes them with the aid of his correlated collected data. Their reconciliation procedure can accomplish security rates comparable to the theoretical limits. Their method relies on multilevel coding and optimized low-density parity-check (LDPC) codes, where Alice applies a labeling function on its generated bit stream then produces supplementary information for Bob by calculating syndromes of the bit stream.

Privacy Amplification

Although information reconciliation protocol leaks minimum information, the eavesdropper can still use this leaked information to guess the rest of the secret key. Privacy amplification solves this issue by reducing the length of the outputted bit stream. The generated bit stream is shorter in length but higher in entropy. To do so, both Alice and Bob apply a universal hash function selected randomly from a set of hash functions known by both Alice and Bob. Alice sends the number of the selected hash function to Bob so that Bob can use the same hash function.

2.3.2 Exploiting multiple common sources of randomness to extract the key

In some cases, it is possible to collect multiple common sources of randomness simultaneously such as channel gain and phase, channel real and imaginary coefficients [48], linear combination of channel estimates in multiple antenna scenario [49], RSS and distance, if distance estimation is based on RSS.

If multiple common sources of randomness were estimated and the nodes intend to exploit them to generate the secret key, the steps to generate the secret key are the same as in Figure 2.2 with a block added either at the raw data level after *Estimation of Phy Layer Characteristic* block or at the bit level after the *Encoding* block. The responsibility of this block is to combine the multiple common sources of randomness. We shall call the step of combining the multiple common sources of randomness as the Fusion Operation.

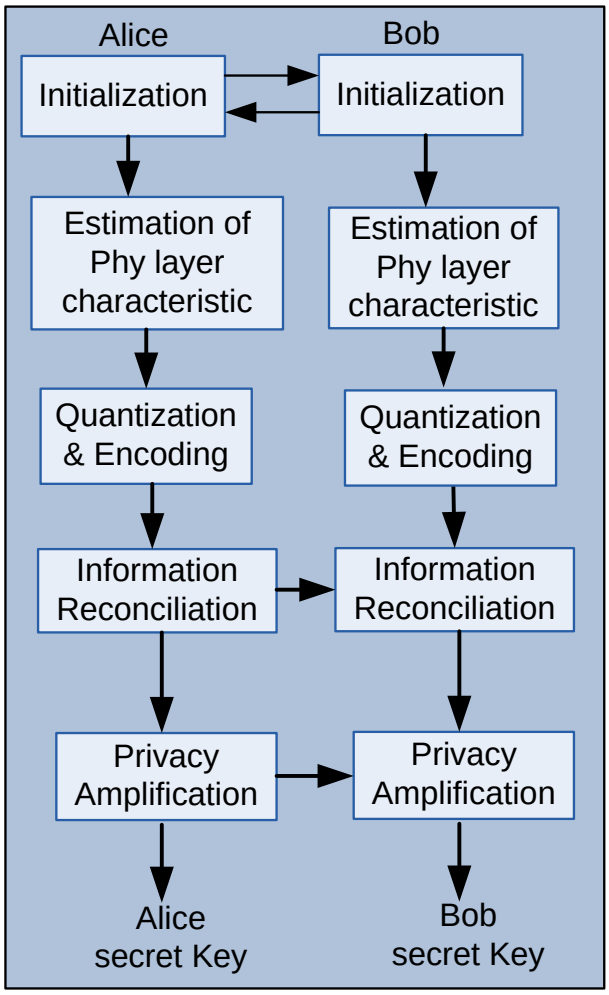

Fig. 2.2 Secret key generation steps in case of 1-D common source of randomness

2.4 Metrics to Evaluate the Generated Secret Key

We present the most commonly used metrics to evaluate the generated secret key, which can be categorized into two main categories: information theoretic metrics and statistical metrics.

2.4.1 Information theoretic metrics

We present three important information theoretic metrics, which are the secret key rate, the secret key capacity and the outage secret key capacity.

Secret key rate

The concept of secret key rate, R, was first presented in the pioneering work of Maurer in 1993 [50]. He derived the upper and lower bounds on the secret key rate considering that the two legitimate nodes, Alice and Bob, have unlimited access to a public channel, which Eve can listen to. Both Alice and Bob observe n independent and identically distributed random variable X and Y, respectively. X and Y are denoted by $X = (X_1, ...X_n)$ and $Y = (Y_1, ...Y_n)$. At any instant of time i, the corresponding observations at Alice and Bob X_i and Y_i are highly dependant. These observations are their estimates of the common source of randomness. On the other hand, Eve observes a sequence of observation denoted by Z. The upper bound on the generated secret key as defined by Maurer is given by:

$$S(X;Y||Z) \leq \min\left[I(X;Y), I(X;Y|Z)\right] \tag{2.1}$$

where $I(X;Y)$ is the mutual information between X and Y and $I(X;Y|Z)$ is the mutual information between X and Y given Z. The lower bound is given by

$$S(X;Y||Z) \geq \max\left[I(Y;X) - I(Z;X), I(X;Y) - I(Z;Y)\right] \tag{2.2}$$

Secret key capacity

The supremum of the secret key rate is considered the secret key capacity C_s. Although, secret key capacity in general is still an open problem, Maurer defined it

as:

$$\begin{aligned} C_s &= \max_{P_X} S(X;Y||Z) \\ &\leq \min\left[\max_{P_X} I(X;Y), \max_{P_X} I(X;Y|Z)\right] \end{aligned} \tag{2.3}$$

where P_X is the probability density function of X.

Secrecy entropy

Entropy is a measure of the level of randomness of the generated key. Within the context of SKG, the higher the entropy, the more random the generated key. Within information theory context, entropy quantifies the uncertainty in a random variable or random process. The maximum achievable entropy rate occurs when the random variable follows a uniform distribution.

2.4.2 Statistical metrics

The statistical tests applied on the secret key generated based on a physical layer characteristic are borrowed from the conventional cryptography test. As stated in [51] "Each statistical test determines whether the sequence possesses a certain attribute that a truly random sequence would be likely to exhibit; the conclusion of each test is not definite, but rather probabilistic." The National Institute of Standards and Technology (NIST) (US Department of Commerce) [52] provides tools (Public key interpretability test suite certification path validation [53]) to evaluate the statistical metrics of the generated secret key. The tools are developed to evaluate the performance of conventional cryptographic techniques, however the generated key through a physical layer characteristic can be tested using the provided tools by NIST. There are five basic statistical tests presented in [51]. We add a more recent test applied on the generated secret key, which is the bit mismatch rate between the key generated at Alice and Bob. For a generated secret key s of length N bits, the six tests are:

Frequency test

The objective of this test is to determine if the number of 1's and 0's are approximately the same, as predicted for a random binary sequence.

Serial test

The objective of this test is to determine if the number of occurrences of the two bit subsequences 00, 01, 10, and 11 are approximately the same, as predicted for a random binary sequence.

Poker test

To apply the poker test, the generated key s is divided into k non-overlapping subsequences of length m. The objective of this test is to determine if the number of occurrences of each of the subsequences of length m is approximately the same, as predicted for a random binary sequence. If the length of the subsequence $m = 1$, the poker test reduces to the frequency test.

Runs test

Each run is represented as subsequence of the generated key s consisting of consecutive 0's or consecutive 1's. The subsequence of consecutive 0's is referred to as *gap*, while the subsequence of 1's is referred to as *block*. The objective of this test is to check if the number of runs of different lengths is as predicted for a random binary sequence. The expected number of runs (either gaps or blocks) of length j in the generated key s of length N is $e_j = (N - i + 3)2^j$.

Autocorrelation test

The objective of this test is to examine the correlation between the generated secret key s and a shifted version of itself.

Bit mismatch rate

The objective of this test is to estimate the bit mismatch between the two sequences generated at Alice and Bob. The BMR should be less than a threshold to meet reliability criteria.

2.5 Conclusion

In this chapter, we presented the most widely exploited common sources of randomness for SKG. Channel gain is commonly used due to its high key generation rate. On the other hand, channel phase follows a uniform distribution and it is expected that the key generated through channel phase will have higher entropy rate. RSS is also commonly used due to its ease of implementation. However, SKG based on RSS suffers from low key generation rate. Distance as a common source of randomness can be exploited only in case of high mobility on the assumption that the eavesdropper is not equipped with AoA estimation capabilities.

Furthermore, we presented the common steps used in the process of SKG. In addition, both information theoretic and statistical metrics used to evaluate the strength of the generated secret key were also investigates. BMR, secrecy entropy and key rate are most widely accepted metrics for the generated secret key.

Chapter 3

Channel Secondary Random Process for Secret Key Generation

3.1 Introduction

As we stated earlier, a major downside of using the channel reciprocity for SKG is that the AWGN at both receivers affects the reciprocity of the channel measurements [6]. This drawback causes the bit mismatch rate (BMR) between the legitimate nodes to rise, which affects the operation of SKG based on channel estimates, particularly, at low and medium signal to noise ratio (SNR) scenarios. As a matter of fact, this major drawback was stated as one of the challenges of physical layer security in [7].

To address the latter drawback of physical layer security techniques, we design a robust SKG technique to mitigate the effect of AWGN. We propose a SKG technique, which we apply on the estimated channel gain only, channel phase only and combined gain and phase, which enhances the performance of the SKG system at low and medium SNR levels. In our technique, the estimated channel is considered our primary random process, from which we derive a secondary random process (SRP) that is then used to generate the secret key. The primary random process, which is either the estimated channel gain or phase, is compared to a preset threshold. The locations of the realizations at which the primary random process exceeds the threshold are stored. The moving differences, which are the differences between each two adjacent locations, are the realizations of our SRP. Those realizations are then used to generate the secret key. The main reason for using the locations, i.e.,

x-axis indices as the core for SKG rather than the gain (amplitude) or phase values, i.e, y-axis points is that it is very likely that those locations are less affected by the AWGN. In other words, due to AWGN, unlike those locations, the y-axis values, whether they are channel gain or phase values, may differ at both communicating receivers, which causes high BMR. Hence, our rational behind creating a SRP that is based on those locations. We derive a closed form expression for the probability mass function of those realizations. Our proposed technique improves the BMR drastically and achieves a longer key length than the conventional techniques. The entropy rate achieved through our technique is comparable to that achieved by conventional techniques. In addition, we numerically compute the conditional probabilities used in secret key capacity estimation.

The rest of this chapter is organized as follows: In Section 3.2 the system model is presented. Our proposed channel SRP for SKG technique is presented in Section 3.3. The properties of our generated SRP are discussed in Section 3.4. The capacity of our SRP secret key is presented in Section 3.5. We evaluate the performance of our solution in Section 3.6. The chapter is then concluded in Section 3.7. Our work in this chapter is presented in [54] and [55].

3.2 System Model

We assume that Alice and Bob use orthogonal frequency division multiplexing (OFDM) system for transmission/reception. In particular, consider an OFDM system where each OFDM symbol consists of N orthogonal subcarrier. After modulating the input serial data streams, a serial to parallel converter converts serial data symbols to parallel streams. N_t pilots, denoted by x_t, are then inserted for the measurement of channel conditions. This results in a vector $X[k]$ for $k = 0, 1, ..., N-1$. $X[k]$ is then used as input to an N-point Inverse Fast Fourier Transform (IFFT). The time domain signal is now:

$$x[n] = \text{IFFT}\{X[k]\} \qquad n = 0, 1, 2, \cdots, N-1. \tag{3.1}$$

A guard interval of length N_d, also known as cyclic prefix, is appended according to:

$$x_f[n] = \begin{cases} x[n+N], & n = -N_d, -N_d+1, \cdots, -1, \\ x[n], & n = 0, 1, \cdots, N-1. \end{cases} \tag{3.2}$$

$x_f[n]$ is then passed through a parallel to serial converter and digital to analog converter, and it is then transmitted to the other node. The received signal at Alice and Bob is given by:

$$y_f^A[n] = x_f^B[n] \otimes h[n] + w_A[n], \tag{3.3}$$
$$y_f^B[n] = x_f^A[n] \otimes h[n] + w_B[n], \tag{3.4}$$

where x_f^B is the transmitted signal from Bob to Alice, x_f^A is the transmitted signal from Alice to Bob, h is a random process that describes the wireless channel between Alice and Bob and w_A and w_B are the additive white Gaussian noise (AWGN) at Alice and Bob's receivers, respectively. Note that the pilots, also known as training signals or reference signal, within x_f^A and x_f^B are identical. The guard interval is then removed from the received signal yielding $y[n] = y_f[n]$ for $n = 0, 1, \cdots, N-1$. $y[n]$ is then passed through an N-point FFT yielding the frequency domain signal $Y[k] = \text{FFT}\{y[n]\}$ $k = 0, 1, ..., N-1$. The pilots, whose locations are already known, are then extracted from $Y[k]$ yielding Y_t, where $t = 1, \cdots, N_t$. Note that the signal exchange between Alice and Bob is performed during the coherence time of the channel.

For simplicity, we estimate the channel through the least squares (LS) estimator in the frequency domain. The LS estimator minimizes the squared error as [56]:

$$\hat{H} = \arg\min ||Y_t - X_t H||. \tag{3.5}$$

The estimated channel at both Alice and Bob can be given by:

$$\hat{H}_{LS}^A = (X_t)^{-1} Y_t^A, \tag{3.6}$$
$$\hat{H}_{LS}^B = (X_t)^{-1} Y_t^B, \tag{3.7}$$

where X_t is the diagonal matrix defined as $X_t = \text{diag}(x_1, \cdots, x_{N_t})$ and Y_t has a dimension of $N_t \times 1$. Since the entries $(x_1, \cdots, x_{N_t})$ are non-zero, the matrix X_t is invertible. The estimated channel at the pilot locations are then interpolated to estimate the

channel across the entire OFDM symbol. The estimated channel gains at Alice and Bob $|\hat{H}^A_{LS}|$ and $|\hat{H}^B_{LS}|$ as well as the phases, which are the angles of $\hat{H}^A_{LS}$ and $\hat{H}^B_{LS}$, are the common sources of randomness which are typically used to generate the secret key and from which we will derive our SRP.

In our adversary model, we assume that an eavesdropper (Eve) can listen to all the exchanged signals between the two legitimate communicating nodes (Alice) and (Bob). Moreover, Eve can estimate the channel between itself and both Alice and Bob. However, Eve can not be within a few wavelengths of either of the two communicating nodes, Alice and Bob, which ensures that her estimated channel between either of them is independent of that between Alice and Bob. In addition, we assume that Eve is a passive adversary, that is not interested in active attacks.

3.3 Proposed SRP Technique

We design a simple SKG technique exploiting, *indirectly*, the estimated channel. Our technique can be applied on the channel gain only, phase only or a combination of the channel gain and phase as we will show later. It is assumed that Alice and Bob have exchanged signals within the coherence time of the channel. They then have estimated the channel using (3.6) and (3.7). They applied an interpolation technique on their channel estimates at the pilot locations to estimate the channel across the entire OFDM symbol. It is worth noting that our technique is not exclusive to OFDM systems, rather it can be applied on the estimated channel in presence of any other system.

3.3.1 Creating a secondary random process

Due to the reciprocity of the channel, the channel estimates at Alice and Bob, $\hat{H}^A_{LS}$ and $\hat{H}^B_{LS}$, are supposed to be identical. However, because of the AWGN added at the two receivers, $\hat{H}^A_{LS}$ and $\hat{H}^B_{LS}$ are not identical. To address the BMR issue explained earlier, we generate a *secondary* random process from the channel estimates. This SRP is then used as common source of randomness to generate the secret key. The steps, which can be applied on the estimated channel gain or phase, are reported below. The steps are reported for the channel gain and apply similarly to the phase.

For simplicity, we limit the description below to the case in which they are applied to the estimated channel gain. The steps to generate our SRP are:

1. Both Alice and Bob use their estimated channel gain to estimate a threshold (γ_g) as:

$$\gamma_g^A = \mathbb{E}[|\hat{H}_{LS}^A|] + \alpha \, \text{std}(|\hat{H}_{LS}^A|) \tag{3.8}$$
$$\gamma_g^B = \mathbb{E}[|\hat{H}_{LS}^B|] + \alpha \, \text{std}(|\hat{H}_{LS}^B|), \tag{3.9}$$

   where $\mathbb{E}[.]$ is the mean operation, std$(.)$ is the standard deviation operation and α is a design parameter $\in [-1:1]$. The design parameter α decides how far the threshold from the mean with a percentage of the standard deviation. For example, when $\alpha = 0$, $\gamma_g^A = \mathbb{E}[|\hat{H}_{LS}^A|]$. For $\alpha \neq 0$, the threshold moves away from the mean. Hence, covering a wide range of possible thresholds.

2. Both Alice and Bob compare their channel gain, recursively to the preset thresholds γ_g^A and γ_g^B, respectively.

3. If the channel estimate is higher than the preset threshold, the location, i.e, the index (x-axis) is stored in a vector S initialized to all zeros. Alice and Bob estimate their vectors as S_g^A and S_g^B.

4. Alice and Bob then estimate the moving difference of their estimated locations J_g^A and J_g^B for channel gain, which are computed as:

$$J_g^A[i] = S_g^A[i+1] - S_g^A[i], \quad i = 1,...,N-1, \tag{3.10}$$
$$J_g^B[i] = S_g^B[i+1] - S_g^B[i], \quad i = 1,...,N-1. \tag{3.11}$$

A flow chart of the SRP of the channel gain is presented in Figure 3.1 for Alice. The realizations in the vectors J_g^A and J_g^B constitute the entries of our *secondary* random process. In other words, we have created two SRPs, one for the channel gain and another for the channel phase. These SRPs are considered our new common sources of randomness which are then used by Alice and Bob to generate the secret key. In Section 3.6, we provide an example of our SRP. Alice and Bob can use SRP extracted from channel gain only, channel phase only or a combination of the two for the SKG. Once the SRP is created, the secret key can be generated using the steps presented in Chapter 2. Algorithm 1 summarizes the steps used to generated the secret key. In

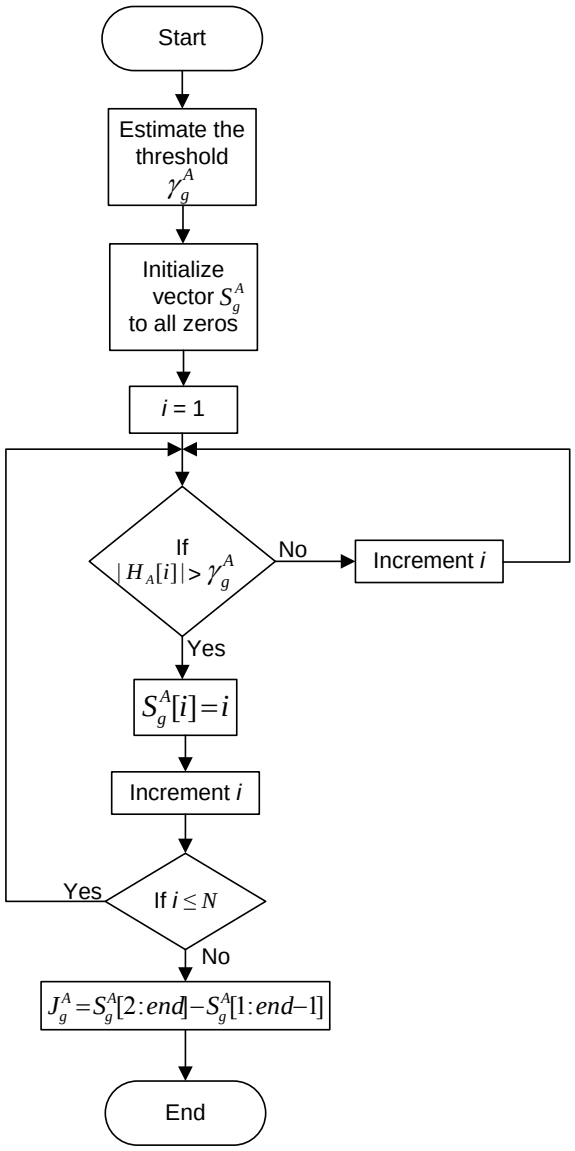

Fig. 3.1 Flow chart of SRP creation for channel gain at Alice.

line 2, (3.8) and (3.9) are used to estimate the threshold, which is then used in lines 4 to 10 to compare the gain values to. The moving difference is estimated in line 11. The rest of the algorithm contains the quantization, information reconciliation and privacy amplification steps.

Algorithm 1 SRP SKG Technique for Channel Gain

1: **Step 1: Creating secondary random process**
2: Alice and Bob estimate their thresholds using (3.8) and (3.9), respectively.
3: Both Alice and Bob apply the following steps on $|\hat{H}^A_{LS}|$ and $|\hat{H}^B_{LS}|$.
4: **for** *i = 1: length*$(|\hat{H}^A_{LS}|)$ **do**
5: **if** $|\hat{H}_{LS}| > \gamma_g$ **then**
6: $S[i] = i$
7: **else**
8: $S[i] = 0$
9: **end if**
10: **end for**
11: Both Alice and Bob estimate $J^A_g = S^A_g[i+1] - S^A_g[i]$ and $J^B_g = S^B_g[i+1] - S^B_g[i]$.
12: **Step 2: Uniform Quantization**
13: Alice and Bob use n_q bits to quantize J^A_g and J^B_g.
14: Alice and Bob convert their quantized values into bitstreams.
15: **Step 3: Information Reconciliation**
16: Alice and Bob permute the bit streams and divide them into small blocks.
17: Alice sends the permutation and parities to Bob.
18: Bob compares the received parity information with his own.
19: In case of mismatch, Bob corrects his bits accordingly.
20: **Step 4: Privacy Amplification**
21: Alice sends the number of the hash function to Bob.
22: Alice and Bob apply the hash function to the bit stream.

3.4 Properties of SRP

In this section, we study the characteristics of our generated SRP. The first step in our SRP creation is to compare the estimated channel gain or phase to a preset threshold. This process can be considered as independent and identically distributed Bernoulli trials. For the channel gain, the success is defined as $|\hat{H}_{LS}[i]| > \gamma_g$ and the failure defined as $|\hat{H}_{LS}[i]| \leq \gamma_g$. The probability of success for the channel gain, p_g, is given

by

$$\begin{aligned} p_g &= Pr(|\hat{H}_{LS}[i]| > \gamma_g) \\ &= 1 - q_g \\ &= 1 - Pr(|\hat{H}_{LS}[i]| \leq \gamma_g), \end{aligned} \tag{3.12}$$

where q_g is the probability of failure. The channel gain follows a Rayleigh distribution with probability density function defined as:

$$f(r) = \frac{r}{\Omega^2} \exp\left(-\frac{r^2}{2\Omega^2}\right), \quad \text{for} \quad r \geq 0 \tag{3.13}$$

where r is the envelope amplitude of the received signal and $2\Omega^2$ is the average power of multipath signal prior to envelope detection. Hence,

$$p_g = \exp\left(-\frac{\gamma_g^2}{2\Omega^2}\right). \tag{3.14}$$

Similarly, for channel phase, the success is defined as $\angle\hat{H}_{LS}[i] > \gamma_{ph}$ and the failure defined as $\angle\hat{H}_{LS}[i] \leq \gamma_{ph}$, where γ_{ph} is the threshold for the channel phase. The probability of success for the channel phase is

$$\begin{aligned} p_{ph} &= Pr(\angle\hat{H}_{LS}[i] > \gamma_{ph}) \\ &= 1 - q_{ph} \\ &= 1 - Pr(\angle\hat{H}_{LS}[i] \leq \gamma_{ph}), \end{aligned} \tag{3.15}$$

where q_{ph} is the probability of failure. The channel phase, θ, follows a uniform distribution with probability density function defined as:

$$f(\theta) = \frac{1}{2\pi}, \quad \text{for} \quad 0 \leq \theta \leq 2\pi \tag{3.16}$$

Hence,

$$p_{ph} = 1 - \frac{\gamma_{ph}}{2\pi}. \tag{3.17}$$

Remember that the vectors S_g and S_{ph} are initialized to all zeros. We search for the locations at which the estimated channel gain or phase exceeds the threshold. These locations are the nonzero entries in S_g and S_{ph}. They are estimated as the number of trials, v, needed to achieve u successes. Therefore, these locations, V_g, follow a negative binomial (NB) distribution according to $V_g \sim \mathscr{NB}(u_g, p_g)$ for the channel gain and $V_{ph} \sim \mathscr{NB}\left(u_{ph}, p_{ph}\right)$ for the channel phase. The probability mass function of V_g is given by:

$$\begin{aligned} l_g(v_g, u_g) &= Pr(V_g = v_g) \\ &= \begin{pmatrix} v_g - 1 \\ u_g - 1 \end{pmatrix} (1 - p_g)^{v_g - u_g} p_g^{u_g}. \end{aligned} \tag{3.18}$$

$l_{ph}(v_{ph}, u_{ph})$ is defined similarly for the channel phase. Thus, the probability of overwriting the initial zero in S_g is given by (3.18) and the probability that it remains zero is $l'_g(v_g, u_g) = 1 - l_g(v_g, u_g)$. Also $l'_{ph}(v_{ph}, u_{ph})$ is described in the same manner. The entries in the vectors J_g and J_{ph} are the moving differences between each two consecutive entries in S_g and S_{ph}, respectively. Hence, each entry in J_g and J_{ph} has four possibilities as follows. We present the cases for the channel gain only. The four cases for the channel phase are similar with the probabilities assigned to the channel phase vector entries.

- Case 1: the two consecutive entries in S_g are zeros. Consequently, the entry in J_g is zero with probability $l'_g(v_g, u_g)\ l'_g(v_g + 1, u_g)$.
- Case 2: the two consecutive entries in S_g are the values of the NB random variables (v_g and $v_g + 1$). Consequently, the entry in J_g is 1 with probability $l_g(v_g, u_g)\ l_g(v_g + 1, u_g + 1)$.
- Case 3: the first (out of the two producing J_g entry) entry is zero and the second is a value of the NB random variable. Consequently, the entry in J_g is the same value of the NB random variable (v_g) with probability $l'_g(v_g, u_g)\ l_g(v_g + 1, u_g + 1)$.
- Case 4: the first entry is a value of the NB random variable and the second is zero. Consequently, the entry in J_g is the negative of the value of the NB random variable ($-v_g$) with probability $l_g(v_g, u_g)\ l'_g(v_g + 1, u_g)$.

To find a closed form expression for the probability mass function of each entry in J_g, which we denote by $P(J_g[i] = j_g)$, we use the Lagrange interpolating polynomial formula [57]. Lagrange interpolating polynomial method finds the polynomial of degree $\leq n_{lg} - 1$ which passes through n_{lg} points $((x_{lg_1}, y_{lg_1}), (x_{lg_2}, y_{lg_2}), \cdots, (x_{lg_{n_{lg}}}, y_{lg_{n_{lg}}}))$. It is defined as

$$D(x_{lg}) = \sum_{i_{lg}=1}^{n_{lg}} T_{lg}(x_{lg}), \tag{3.19}$$

with

$$T_{lg}(x_{lg}) = y_{lg_{i_{lg}}} \prod_{\substack{k_{lg}=1 \\ k_{lg} \neq i_{lg}}}^{n_{lg}} \frac{x_{lg} - x_{lg_{k_{lg}}}}{x_{lg_{i_{lg}}} - x_{lg_{k_{lg}}}}. \tag{3.20}$$

Using the four cases explained above, the probability mass function of each entry in J_g for $j_g \in \{-v_g, 0, 1, v_g\}$ can be given by

$$\begin{aligned}
&P(J_g[i] = j_g) \\
&= \frac{l_g(v_g, u_g) l_g(v_g + 1, u_g + 1) j_g (v_g + j_g)(v_g - j_g)}{(v_g - 1)(v_g + 1)} \\
&- \frac{l'_g(v_g, u_g) l'_g(v_g + 1, u_g)(j_g - 1)(v_g + j_g)(v_g - j_g)}{v_g^2} \\
&+ \frac{l_g(v_g, u_g) l'_g(v_g + 1, u_g) j_g (v_g - j_g)(j_g - 1)}{2v_g^2(v_g + 1)} \\
&+ \frac{l'_g(v_g, u_g) l_g(v_g + 1, u_g + 1) j_g (v_g + j_g)\ (j_g - 1)}{2v_g^2(v_g - 1)}.
\end{aligned} \tag{3.21}$$

The probability mass function of each entry in J_g is zero otherwise. The mean, $\mathbb{E}[J_g[i]]$, is then:

$$\begin{aligned}
\mathbb{E}[J_g[i]] &= \sum_{j_g} j_g \, P(J_g[i] = j_g) \\
&= l_g(v_g, u_g)\ l_g(v_g + 1, u_g + 1) \\
&+ v_g\ l'_g(v_g, u_g)\ l_g(v_g + 1, u_g + 1) \\
&- v_g\ l_g(v_g, u_g)\ l'_g(v_g + 1, u_g),
\end{aligned} \tag{3.22}$$

and

$$\begin{aligned}\mathbb{E}\left[J_g^2[i]\right] &= \sum_{j_g} j_g^2\, P(J_g[i]=j_g)\\ &= l_g(v_g,u_g)\; l_g(v_g+1,u_g+1)\\ &+ v_g^2\; l'_g(v_g,u_g)\; l_g(v_g+1,u_g+1)\\ &+ v_g^2\; l_g(v_g,u_g)\; l'_g(v_g+1,u_g). \end{aligned} \tag{3.23}$$

Hence, the variance of $J_g[i]$ can be given by:

$$\begin{aligned}\mathrm{var}\,[J_g[i]] &= \mathbb{E}\left[J_g^2[i]\right] - \left[\mathbb{E}\left[J_g[i]\right]\right]^2\\ &= l_g(v_g,u_g)\; l_g(v_g+1,u_g+1)\\ &+ v_g^2\; l'_g(v_g,u_g)\; l_g(v_g+1,u_g+1)\\ &+ v_g^2\; l_g(v_g,u_g)\; l'_g(v_g+1,u_g)\\ &- \Big(l_g(v_g,u_g)\; l_g(v_g+1,u_g+1)\\ &+ v_g\; l'_g(v_g,u_g)\; l_g(v_g+1,u_g+1)\\ &- v_g\; l_g(v_g,u_g)\; l'_g(v_g+1,u_g)\Big)^2. \end{aligned} \tag{3.24}$$

The probability mass function for the channel phase, $P(J_{ph}[i]=j_{ph})$ is defined similarly.

3.5 Secret Key Capacity

Since the entries in our generated SRPs are independent and identically distributed (i.i.d.), our secret key rate after the information reconciliation and privacy amplification exhibits the same generic results presented in [50]. The upper and lower bounds for the channel gain SRP are given by [50]:

$$\begin{aligned}R_g^U\left(J_g^A[i];J_g^B[i]||J_g^E[i]\right) \leq \min\Big[&I(J_g^A[i];J_g^B[i]),\\ &I(J_g^A[i];J_g^B[i]|J_g^E[i])\Big], \end{aligned} \tag{3.25}$$

$$R_g^L(J_g^A[i];J_g^B[i]||J_g^E[i]) \geq \max\Bigg[I(J_g^B[i];J_g^A[i]) - I(J_g^E[i];J_g^A[i]),I(J_g^A[i];J_g^B[i]) - I(J_g^E[i];J_g^B[i])\Bigg], \tag{3.26}$$

where $I(J_g^A[i];J_g^B[i])$ is the mutual information between $J_g^A[i]$ and $J_g^B[i]$ and $I(J_g^A[i];J_g^B[i]|J_g^E[i])$ is the mutual information between $J_g^A[i]$ and $J_g^B[i]$ given $J_g^E[i]$ for the eavesdropper, Eve. The supremum of the secret key rate is considered the secret key capacity C_g:

$$\begin{aligned} C_g &= \max_{P(J_g^A[i])} I(J_g^A[i];J_g^B[i]||J_g^E[i]) \\ &\leq \min\Bigg[\max_{P(J_g^A[i])} I(J_g^A[i];J_g^B[i]), \\ &\quad \max_{P(J_g^A[i])} I(J_g^A[i];J_g^B[i]|J_g^E[i])\Bigg]. \end{aligned} \tag{3.27}$$

However, in the definitions above, it was assumed that Eve has access to the primary random process, i.e., channel estimates. In order for Eve to collect correlated channel measurements, she has to be within a half wavelength apart from either Alice or Bob. In other words, Eve has to place herself within a close proximity (typically a few centimeters) of either of them to obtain useful channel estimates, which is very unlikely to occur. Therefore, as in [48], we disregard the feasibility of eavesdropping. Consequently, the secret key capacity for the channel gain SRP can be given by

$$C_g = \lim_{N\to\infty} \frac{1}{N} I\left(J_g^A[i];J_g^B[i]\right). \tag{3.28}$$

The mutual information is defined as

$$\begin{aligned} &I\left(J_g^A[i];J_g^B[i]\right) = \\ &\sum_{j_g^A\in[-v_g,0,1,v_g]} \sum_{j_g^B\in[-v_g,0,1,v_g]} \Bigg[P\Bigg(J_g^A[i]=j_g^A, \\ &J_g^B[i]=j_g^B\Bigg)\log\left(\frac{P(J_g^A[i]=j_g^A,J_g^B[i]=j_g^B)}{P(J_g^A[i]=j_g^A)P(J_g^B[i]=j_g^B)}\right)\Bigg], \end{aligned} \tag{3.29}$$

Table 3.1 $P\left(J_g^A[i]=j_g^A|J_g^B[i]=j_g^B\right)$

j_g^A \ j_g^B	$-v_g$	0	1	v_g
$-v_g$	p_g^o	p_g^{e1}	p_g^{e1}	p_g^{e2}
0	p_g^{e1}	p_g^o	p_g^{e2}	p_g^{e1}
1	p_g^{e1}	p_g^{e2}	p_g^o	p_g^{e1}
v_g	p_g^{e2}	p_g^{e1}	p_g^{e1}	p_g^o

where $P\left(J_g^A[i]=j_g^A,J_g^B[i]=j_g^B\right)$ is the joint probability mass function of $J_g^A[i]$ and $J_g^B[i]$, while $P(J_g^A[i]=j_g^A)$ and $P(J_g^B[i]=j_g^B)$ are the probability mass functions of $J_g^A[i]$ and $J_g^B[i]$, respectively, which are defined by (3.21). $P\left(J_g^A[i]=j_g^A,J_g^B[i]=j_g^B\right)$ can be given by

$$P\left(J_g^A[i]=j_g^A,J_g^B[i]=j_g^B\right)= P\left(J_g^A[i]=j_g^A|J_g^B[i]=j_g^B\right)P(J_g^B[i]=j_g^B). \tag{3.30}$$

Since the two vectors $J_g^A[i]$ and $J_g^B[i]$ are highly correlated, the probability that the entry at J_g^B is identical to the entry at J_g^A is high. We denote this probability by p_g^o. It is defined as $p_g^o=P\left(J_g^A[i]=j_g^B|J_g^B[i]=j_g^B\right)$[1]. The probability that an error occurred, i.e., the entry at J_g^B is different from the entry J_g^A is defined as $p_g^e=P\left(J_g^A[i]\neq j_g^B|J_g^B[i]=j_g^B\right)$. The error can happen in two cases. The first case occurs if either one of the entries in S_g^A, which are used to generate the entry J_g^A, is different from its counterpart in S_g^B. We denote this probability by p_g^{e1}. The second case occurs if the two entries in S_g^A are different from their counterparts in S_g^B. We denote this probability by p_g^{e2}. The relation between the three probabilities follow $p_g^o>p_g^{e1}>p_g^{e2}$ at medium and high SNR levels. Based on these probabilities, we define $P\left(J_g^A[i]=j_g^A|J_g^B[i]=j_g^B\right)$ for all possible values of j_g^A and j_g^B in Table 3.1. Similarly, the secret key capacity for the channel phase, C_{ph}, is defined in the same manner with the probabilities p_{ph}^o, p_{ph}^{e1} and p_{ph}^{e2}. We compute the values of both channel gain and phase probabilities in Section 3.6.

[1]Even if the two entries of S_g^A and S_g^B were different and resulted in $J_g^A[i]=j_g^B|J_g^B[i]=j_g^B$, we still consider that as a success since j_g^B is the value that will be used to generate the secret key and it should be equal at both Alice and Bob. However, we would like to state that having the two entries in S_g^A and S_g^B different and resulting in a success shall constitute a very small percentage of p_g^o because the two vectors S_g^A and S_g^B are highly correlated.

Table 3.2 Simulation parameters

Parameter	Value
No. of subcarriers	1024
No. of FFT point	1024
Subcarrier spacing	15 KHz
Number of pilots	16.7%=171
Cyclic prefix length	25%=256
Modulation scheme	QPSK
Channel type	Rayleigh
Doppler shift	100 Hz
Chan. Estimation	LS
Interpolation type	Linear
α	-0.2
m for Level crossing	4
n_q	8 bits
Number of iterations	10000

3.6 Performance Evaluation

To evaluate the performance of our technique, we simulate an entire OFDM system and estimate the channel using the LS estimator. Table 3.2 summarizes our simulation parameters for the subsequent figures. We simulate the conventional channel gain and phase techniques, level crossing technique, and proposed SRP technique for channel gain only and for channel phase only. Then we obtain the combined SRP by concatenating bitstreams from channel gain and phase SRPs. Our combined vectors are given by

$$J_c^A = [J_g^A[1], J_p^A[1], J_g^A[2], J_p^A[2], \cdots, J_g^A[N], J_p^A[N]], \tag{3.31}$$

$$J_c^B = [J_g^B[1], J_p^B[1], J_g^B[2], J_p^B[2], \cdots, J_g^B[N], J_p^B[N]]. \tag{3.32}$$

We first present an example of our generated SRP. To show the effect of our proposed SRP technique on the BMR, we simulate all techniques up to the quantization and bitstream generation step. For a fair comparison, the level crossing technique is

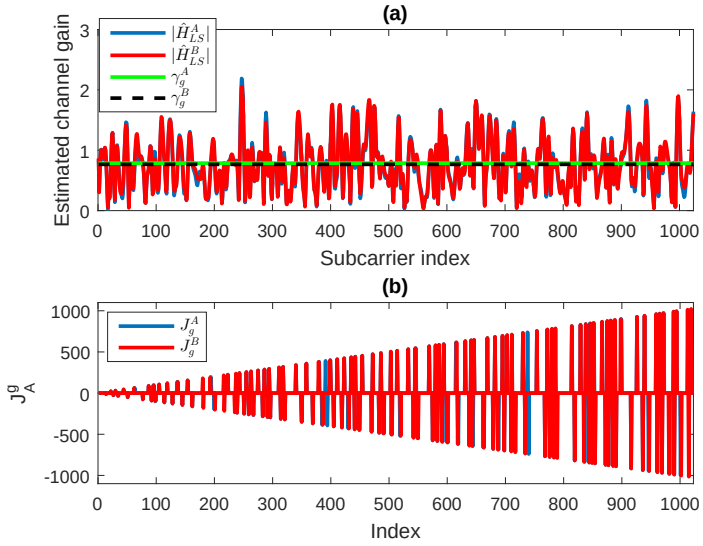

Fig. 3.2 (a) Estimated channel gain at Alice and Bob with γ_g^A and γ_g^B at SNR = 20 dB and (b) our estimated J_A and J_B.

simulated without the information reconciliation step. In other words, channel estimates at the locations G_A and G_B are quantized and converted into bitstreams. We plot the BMR for all techniques. We then compute the secret key capacity probabilities for both channel gain and phase SRPs. Afterwards, we estimate the entropy rate of the generated key for our techniques versus existing techniques. The secret key length is then presented.

3.6.1 SRP

In Figure 3.2-(a), we plot the estimated channel gain at both Alice and Bob, for SNR = 20 dB and the thresholds estimated from (3.8) and (3.9). We then follow the steps in Section 3.3.1 to estimate J_g^A and J_g^B and plot them in Figure 3.2-(b). The estimated channel gain at Alice and Bob is almost identical with some discrepancy in the value of the gain (y-axis) due to the effect of the AWGN. Note that SNR = 20 dB can be considered a moderately high SNR level. The effect of AWGN at lower SNR levels is more severe as can be seen in Figure 3.3, which is simulated at SNR = 3dB. On the other hand, since our SRP depends on the locations (x-axis), the effect of AWGN on our channel gain SRP is tolerable. The same conclusion is drawn for the channel phase SRP.

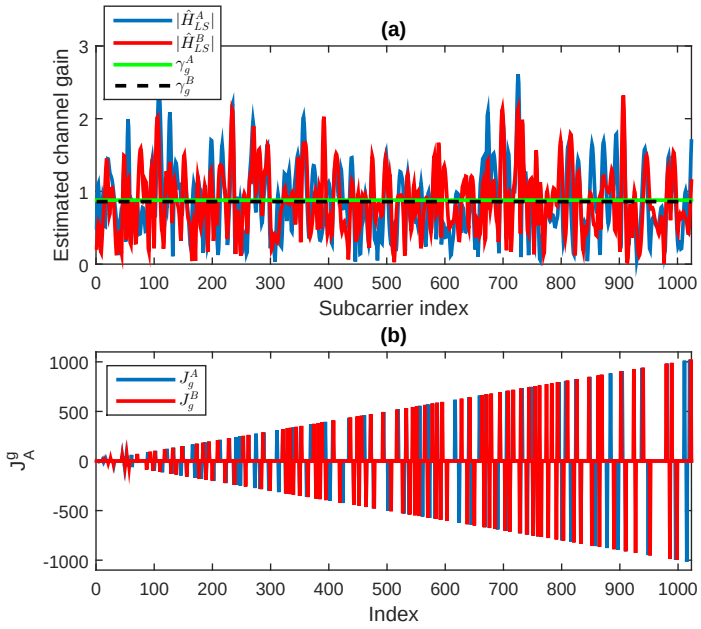

Fig. 3.3 (a) Estimated channel gain at Alice and Bob with γ_g^A and γ_g^B at SNR = 3dB and (b) our estimated J_A and J_B.

3.6.2 BMR

We plot the BMR between the secret keys generated at Alice and Bob for all the techniques in Figure 3.4. Our proposed SRP techniques drastically improve the BMR achieving a BMR that is ranging from 10-15% at low and high SNR levels to 25% at medium SNR levels less than that of the conventional channel gain and phase. In addition to that, our proposed SRP is achieving a BMR that is ranging from 12% at low SNR levels to 40% at medium and high SNR levels less than that of the level crossing technique. It is worth noting that on average the worst BMR achieved is 0.5 which is equivalent to random guessing. The level crossing technique is performing the worst; achieving the highest BMR, which indicates that the strength of the level crossing algorithm comes from the information reconciliation step. The combined SRP technique achieves a BMR that is average between the SRP channel gain and phase. Also, as expected, as the SNR increases, the BMR for all techniques improves.

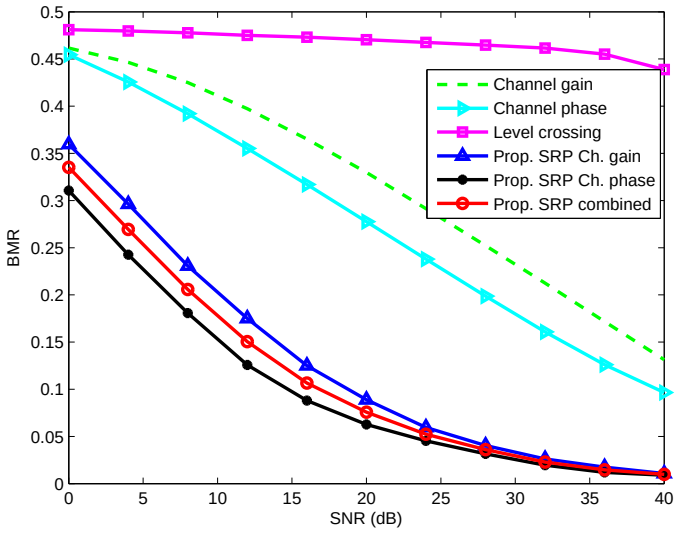

Fig. 3.4 BMR as a function of SNR for our scheme vs. existing techniques.

3.6.3 Probabilities for secret key capacity

We compute the probabilities, p_g^o, p_g^{e1} and p_g^{e2} numerically in Figure 3.5 for the channel gain SRP and p_{ph}^o, p_{ph}^{e1} and p_{ph}^{e2} in Figure 3.6 for the channel phase SRP for SNR ranging from 0 to 40 dB. As expected, since $J_g^A[i]$ and $J_g^B[i]$ are highly correlated, p_g^o is much higher than p_g^{e1} and p_g^{e2}, particularly at medium and high SNR levels. As SNR increases, p_g^o increases, while p_g^{e1} and p_g^{e2} decrease. In addition, $p_g^{e1} > p_g^{e2}$ at medium and high SNR levels since it is more likely for one entry in S_g to change rather than the two entries. The same result is obtained for the channel phase. Note that $p_g^o + 2\ p_g^{e1} + p_g^{e2} = 1$. In addition $p_{ph}^o > p_g^o$ at low SNR levels, which suggests exploiting the channel phase SRP over channel gain SRP at low SNR levels should be preferred.

3.6.4 Entropy

Entropy is a measure of the level of randomness of the generated key. For example, for our SRP channel gain, the entropy of a secret key generated from Alice's estimated channel gain is defined as $\mathscr{H}(J_g^A[i]) = \log\left(1/P(J_g^A[i])\right)$. The average entropy is then $\mathbb{E}[\mathscr{H}(J_g^A)]$. As expected from Figure 3.2-(b), the average entropy of our SRP secret key will be less than that of the channel gain. We plot the achieved

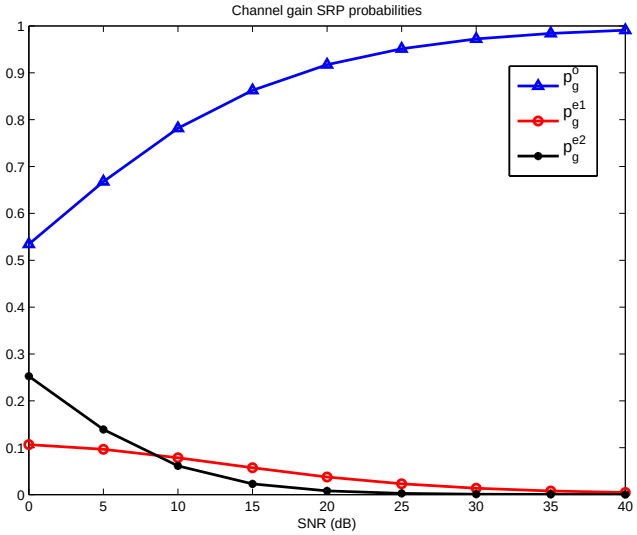

Fig. 3.5 Probabilities for channel gain SRP.

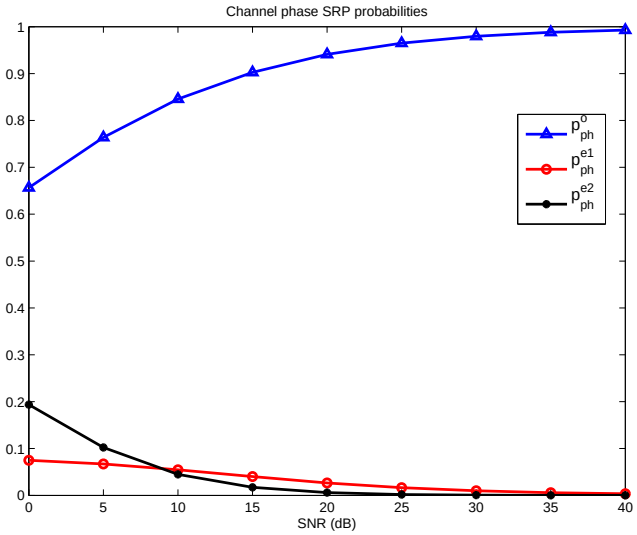

Fig. 3.6 Probabilities for channel phase SRP.

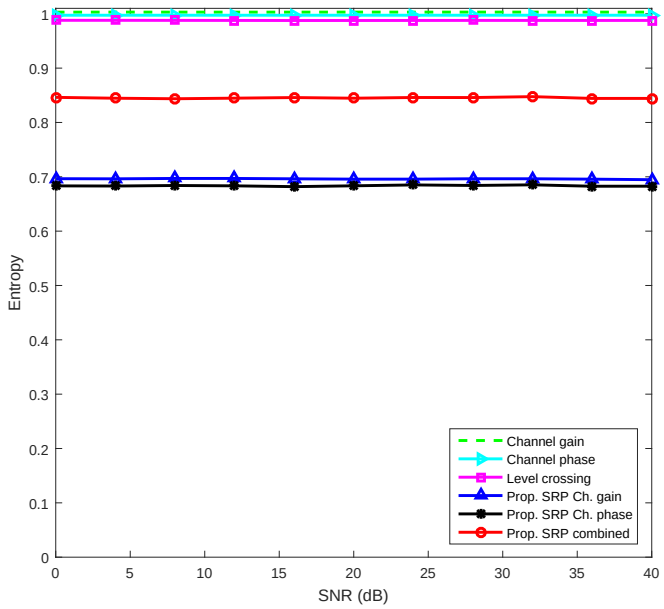

Fig. 3.7 Entropy as a function of SNR for our scheme vs. existing techniques.

entropy rate of all techniques in Figure 3.7. Our entropy rate for the channel gain is consistent with the results obtained in [58]. Our SRP channel gain and phase exhibit less entropy than all other techniques. To address this drawback, we proposed the combined channel gain and phase SRP algorithm, which improved the entropy rate of the generated secret key. We sacrifice a bit of entropy (15%) to greatly improve the BMR. Also, it is worth nothing that the combined SRP technique does not increase the complexity of the system since both channel gain and phase can be calculated from the channel estimates. In addition to that, it only requires a simple concatenation operation.

The reduction in entropy resulting from our method which is associated with significant reduction in BMR has the advantage that less exchange of messages is needed in the subsequent phases of information reconciliation and privacy amplifications. Knowing that more exchange of messages for information reconciliation results in more side information available to Eve, which in turn will mean less entropy of the final key after privacy amplification [59], we can argue in a qualitative manner that we achieve a performance very close to classical key extraction methods in terms of final key entropy. However, in this work we are not addressing the subsequent phases mentioned above and we stop at showing that BMR is reduced.

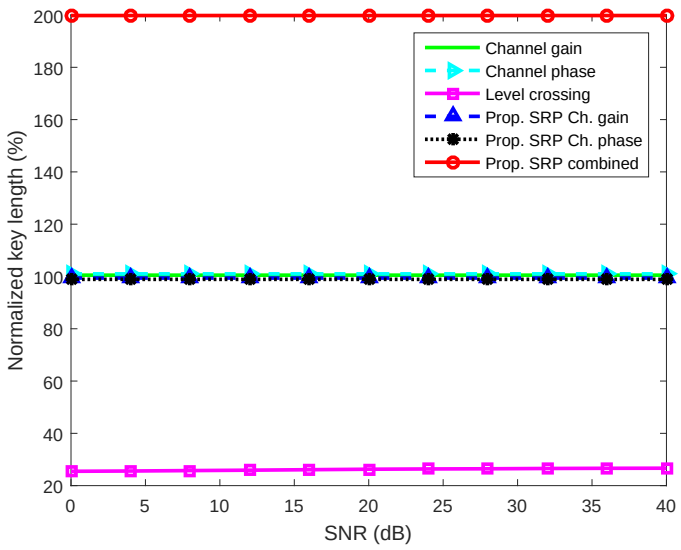

Fig. 3.8 Normalized key length as a function of SNR for our scheme vs. existing techniques.

3.6.5 Key length

Figure 3.8 shows the simulated key length of all techniques normalized to the length of the secret key generated through the conventional channel gain technique. Our proposed SRP channel gain and phase is achieving approximately the same key length as of that of the channel gain and phase techniques, while SRP combined is achieving twice that length. On the contrary, the level crossing technique is performing the worst achieving a normalized key length of 30%. This implies that for the level crossing rate technique to achieve a reasonable key length, the frequency of channel propping should increase which decreases the throughput of the system.

3.7 Conclusion

We designed a simple yet robust technique to extract a secret key from a secondary random process that is derived from the channel estimates. Our SRP technique can be applied on the channel gain only, channel phase only as well as a combination of the two. We derived a closed form expression for the probability mass function of an entry of the SRP vector and simulated our technique using a complete OFDM system. Compared to existing techniques, our SRP solution provided a drastic improvement in the BMR, and achieved comparable entropy and a much longer key length in

the case of the combined SRPs. We computed the conditional probabilities used to estimate the secret key capacity for both the channel gain and phase SRP. In addition, our SRP solution is easy to implement and does not increase the complexity of the system.

Chapter 4

Novel Common Sources of Randomness

4.1 Introduction

In Chapter 3, we designed a novel technique to exploit channel estimates to create a SRP with the objective of mitigating the effect of AWGN and hence increasing the dynamic range of the SKG system. However, for low SNR levels, i.e., SNR < 0 dB, existing SKG techniques will fail to generate a secret key with appropriate BMR. This is mainly because channel estimation is highly affected by AWGN.

To address this latter drawback, we design a novel algorithm that exploits angle of arrival (AoA) between the two communicating nodes. AoA estimation techniques can accurately function even at very low SNR level. To the best of the authors' knowledge, exploiting the AoA as a common source of randomness has not been presented in the literature before.

Although AoA estimation techniques can operate with high accuracy at low SNR levels, they require more hardware and computational complexity than single antenna systems. This is mainly because AoA estimation techniques employ antenna array systems. We start this chapter by conducting a thorough literature review on existing AoA estimation techniques so as to determine the advantages and drawbacks of existing techniques and decide on the appropriateness of these techniques within the context of SKG. In Section 4.2 we design a novel AoA estimation technique that enjoys low hardware and computational complexity, hence appropriate for SKG. In

Section 4.3, we present our AoA based SKG technique. Some of our work in this chapter is presented in [60] and [61].

Furthermore, we investigate fusing multiple common sources of randomness for SKG in Section 4.4. In particular, we implement least square channel estimation technique on WARP [62] hardware platform to estimate channel gain. In addition, we estimate the distance between the Alice and Bob and use both channel gain and distance measurements for SKG. This chapter is then concluded in Section 4.5.

4.1.1 Literature review on AoA estimation techniques

Angle of arrival (AoA) estimation is a process that determines the direction of arrival of a received signal by processing the signal impinging on an antenna array. Estimating the AoA is a crucial step in many military and civilian applications, particularly related to security. Applications of estimating the AoA include beamforming, tracking [63], localization and physical layer secrecy [60].

The subject of AoA has been extensively studied in the literature [64–68]. From a system perspective, one can categorize AoA estimation systems into two main categories [64]: **(i) Switched beam system (SBS)** which uses a fixed number of beams to scan the azimuth plane. The AoA is the angle of the beam with the highest received signal strength (RSS). SBS is easy to implement since it requires a single receiver radio frequency (RF) chain and no baseband signal processing, however, it fails at low signal to noise ratio (SNR) levels, and **(ii) Adaptive array system (AAS)** which can steer the beam in any desired direction using baseband signal processing. AAS requires M receiver RF chains to estimate the AoA using baseband processing, where M is the number of antennas. AAS can operate at SNRs lower than SBS, but has higher hardware and computational complexities.

AoA estimation using AAS can be divided into two main techniques: **(1) Classical AoA techniques** based on one of two main methods: *Delay and Sum*, also known as *Bartlett* [69] and *Minimum Variance Distortionless Response (MVDR)*, also known as *Capon* [70]. In Bartlett, the AoA is estimated by steering the beams electronically and estimating the power spectrum of the received signal looking for the angle(s) corresponding to peak(s) in the spatial power spectrum. The main drawback of the Bartlett technique is that signal impinging with angular separation less than $2\pi/M$ can not be resolved. The Capon technique relatively solves the

angular resolution drawback of the Bartlett method at the cost of more baseband processing to perform matrix inversion [70], and **(2) Subspace techniques** based on the concept of orthogonality of signal subspace to noise subspace. The most widely investigated method in this group is multiple signal classification (MUSIC) [71, 72]. MUSIC provides high angular resolution while operating at low SNR levels. This comes at the cost of requiring full a priori knowledge of the number of sources and the array response, whether measured and stored or computed analytically [73]. The signal and noise subspaces are distinguished through an eigen decomposition operation on the covariance matrix of the received signal. This operation requires a substantial computational complexity. Another technique that is subspace based is the Estimation of Signal Parameters via Rotational Invariant Technique (ESPRIT) [74, 75]. Although ESPRIT has lower computational complexity relative to the MUSIC technique since it does not require a sweeping through all possible array response, it puts a constraint on the structure of the antenna array. ESPRIT requires that the antenna element to be clustered in doublet with identical displacement vector.

Recent publications [76, 77] exploit the newly developed concept of co-prime arrays to estimate the AoA. In addition, Kalman filtering is used in [78] in the first stage to estimate the sources, while QR decomposition is needed in the second stage to estimate the AoA. Although Kalman filter based techniques may have lower computational complexity than MUSIC, they have high computational and hardware complexity when compared to SBS.

Due to its attractive simplicity, several attempts have been performed to integrate SBS with other theories to estimate the AoA as presented in [79]. Their methodology is based on neural network, in which the AoA problem is transferred into a mapping problem. This requires a priori knowledge of the number of sources as well as the multiple access scheme adopted between them. It is also assumed that a power control scheme is implemented such that the source powers are equal. Such requirements and assumptions limit the deployment of the system to very few scenarios. Exploiting the power ratio between adjacent beams to estimate the AoA is presented in [80]. A table driven SBS system is presented in [81]. All of these variant techniques do not tackle the drawbacks of the conventional SBS, but rather make its implementation easier. In [82, 83] exploit sectorized antennas along to improve the performance of SBS.

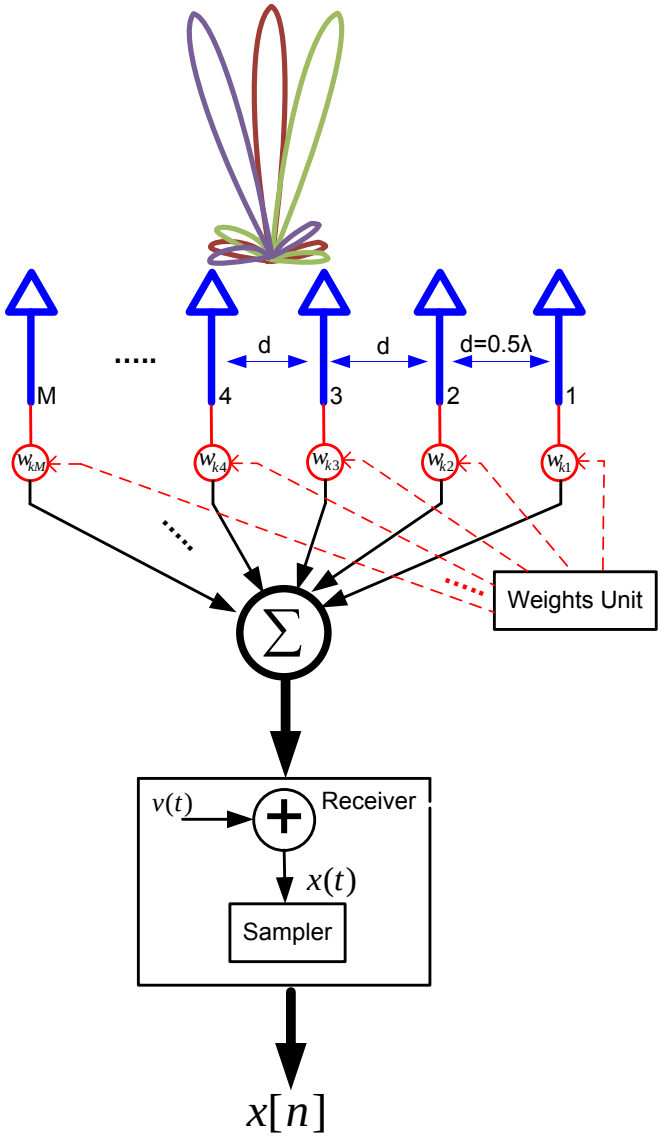

Fig. 4.1 Proposed cross correlation switched beam system for M antenna elements.

4.2 Novel AoA Estimation Technique

We design a new simple AoA estimation system to estimate the AoA. Our system goes through two phases of operation. In the first phase, we select a single antenna element from the antenna array, while the rest of antenna elements are switched off, to collect an omni-directional signal. In the second phase our system switches the beam across the azimuth angular domain of interest. The received signal from each beam is then cross correlated with the omni-directional signal collected earlier in the first phase. The cross correlation between the omni-directional signal and the signals received from the switched beams is the highest at the true AoA and relatively negligible otherwise. Our contributions in this work as compared to available literature are as follows:

- We design an intuitive, novel, low complexity and hardware friendly two-phase cross correlation based AoA estimation system that is based on SBS to detect the angles of transmitters.
- We provide the mathematical modelling and analysis of our proposed system.
- We address some practical aspects related to our proposed system.
- We compare the performance of the proposed system with the MUSIC algorithm (famous for being one of the best performing state-of-the-art for low SNR) and show that our proposed solution performs better, particularly for low SNRs.
- We also compare the computational complexity of our approach with MUSIC and conclude that our approach has lower hardware and computational complexities.

Since our system is based on beam switching, it requires a single receiver which reduces the hardware complexity tremendously. Also, the computational complexity of estimating the cross correlation coefficient is so trivial when compared to estimating the eigen decomposition of the autocovariance function used in MUSIC. At the same time, our proposed system can estimate the AoA at low SNR levels which is very convenient for the application of SKG at low SNR levels. To the best of the authors' knowledge using the cross correlation coefficient between an omni-directional signal and directed beam signal to estimate the AoA has not been

presented in the literature before. It is worth noting that our system can be used for generic AoA estimation and not limited to the application of SKG.

The concept of using the cross-correlation function to extract features of a signal, or to detect its presence, can be found in many applications. One of the most relevant applications is passive radar systems [84, 85], which exploit the transmitters of opportunity, such as television signals, to detect an airborne target. In passive radar systems, a cross correlation between a reference signal from the first receiver and a directional signal from the second is applied to estimate bistatic range and doppler shift of the target. The AoA has to be estimated before that at the second receiver to place a null in the direction of the reference signal [84, 85] such that the received directional signal is the reflection from the airborne target.

4.2.1 System model for AoA estimation

In our system model, we assume that the transmitter sends a signal $s(t)$. The receiver at the other node is equipped with an SBS presented in Figure 4.1 consisting of M antenna elements, separated by a fixed separation d and operating at frequency f. Our antenna array has an array response vector (steering vector) $\mathbf{a}(\phi) \in \mathbb{C}^M$ given by

$$\mathbf{a}(\phi_k) = [w_{k1}, w_{k2}, ..., w_{kM}], \tag{4.1}$$

where ϕ is the azimuth angle, $\mathbb{C}$ is the set of complex numbers and w_{km} for $m \in [1:M]$ are the weights applied across the antenna array elements such that the steering vector $\mathbf{a}(\phi)$ is pointing to an azimuth angle ϕ_k. The received and sampled signal, $x[n]$, in the vector notation for the k^{th} beam, $\mathbf{x_k}$, is

$$\mathbf{x_k} = \mathbf{a}(\phi_k)\mathbf{S} + \mathbf{v}, \tag{4.2}$$

where $\mathbf{x_k}$ (with dimensions $1 \times N$) is the signal received from the k^{th} beam (beam pointing at angle ϕ_k) for $k \in [1:K]$, K is the total number of generated beams, N is the total number of collected samples, $\mathbf{S}$ is the sampled version of the transmitted signal (with dimensions $M \times N$) as seen by the M elements of the antenna array and $\mathbf{v}$ is the additive white Gaussian noise (AWGN) (with dimensions $1 \times N$).

The weights are updated to change ϕ_k in order to scan the angular space of interest. The steering vectors, $\mathbf{a}(\phi)$, for linear, circular or planar array formations

can be calculated analytically. It is worth noting that once the steering vector is set, the operation of our proposed system is independent of the antenna array formation. For a uniform linear array (ULA) with uniform excitation, $\mathbf{a}(\phi)$ is given by [64]:

$$\mathbf{a}(\phi) = \left[1, e^{j\beta dcos(\phi)}, e^{j\beta 2dcos(\phi)}, ..., e^{j\beta(M-1)dcos(\phi)}\right], \tag{4.3}$$

where $\beta = \frac{2\pi}{\lambda}$ is the wave number, λ is the wavelength and ϕ ranges between $[0 : \pi]$. For a uniform circular array (UCA), $\mathbf{a}(\phi)$, is given by [64]:

$$\begin{aligned}\mathbf{a}(\phi) = \quad & [e^{j\beta r\cos(\phi-\phi_1)}, e^{j\beta r\cos(\phi-\phi_2)}, \\ & \cdots, e^{j\beta r\cos(\phi-\phi_M)}],\end{aligned} \tag{4.4}$$

where $\phi_m = 2\pi m/M, m \in [1 : M]$, ϕ ranges between $[0 : 2\pi]$ and r is the radius of the antenna array. The elevation angle is assumed to be 90 degrees in 1-D AoA estimation techniques. For a linear array of M elements with uniform excitation, the total number of orthogonal beams that can be generated is M, i.e., $K = M$. However, using non-uniform excitation such as Dolph-Chebyshev or Taylor [86], it is possible to generate more orthogonal beams for the same number of antenna elements, M, i.e., $K > M$, as will be discussed later.

We assume that the our scanning time is much less than the time it takes the transmitter to move from one location to the next. In addition, we assume that the transmitter continues to transmit highly correlated signal during our scanning time. This can be safely assumed since the scanning time should not exceed few milliseconds.

4.2.2 Review of MUSIC algorithm

Since we compare our results to the MUSIC algorithm, a brief derivation follows for completeness. We chose to compare our results to MUSIC for two main reasons. The first is that MUSIC is one of literature's best performing AoA estimation algorithms [87, 88]. In addition, MUSIC is one of the most popular AoA estimation algorithms. MUSIC requires M receiver RF chains to down convert the received signals from the M antenna elements to the baseband in order to estimate the AoA. Hence, the definition and dimensions of the transmitted signal matrix is different than our SBS system above. The received signal, $\mathbf{X}$, is a matrix with dimensions

$M \times N$. The MUSIC algorithm operates on the autocovariance function of the received signal matrix $\mathbf{X}$, with dimensions $M \times N$, which is denoted by $\mathbf{R}_{XX}$. Let $\mathbf{A} = [\mathbf{a}^T(\phi_1), \cdots, \mathbf{a}^T(\phi_L)]$, with dimensions $M \times L$, and $(.)^T$ denotes the transpose operation. Also, let $\mathbf{s}(t) = [s_1(t), \cdots, s_L(t)]^T$. We have [87]

$$\mathbf{X} = \mathbf{AS} + \mathbf{V}, \tag{4.5}$$

where $\mathbf{S}$ and $\mathbf{V}$ have dimensions of $L \times N$ and $M \times N$, respectively. After an eigenvalue decomposition (EVD) on $\mathbf{R}_{XX}$, it can be written as [87]

$$\begin{aligned} \mathbf{R}_{XX} &= \mathbf{A}\mathbf{R}_{SS}\mathbf{A}^H + \sigma^2 I \\ &= \mathbf{U}_S \Lambda_S \mathbf{U}_S^H + \mathbf{U}_V \Lambda_V \mathbf{U}_V^H, \end{aligned} \tag{4.6}$$

where $\mathbf{R}_{SS}$ is the autocovariance matrix of the transmitted signal, σ^2 is the noise variance, $(.)^H$ denotes the hermitian operation, $\mathbf{I}$ is the $M \times M$ unitary matrix, $\mathbf{U}_S$ and $\mathbf{U}_V$ are the signal and noise subspaces unitary matrices and Λ_S and Λ_V are diagonal matrices of the eigenvalues of the signal and noise. The spatial power spectrum for the MUSIC technique is given by [71, 89]:

$$P_{\text{MUSIC}}(\phi) = \frac{1}{\mathbf{a}^H(\phi) P_V \mathbf{a}(\phi)}, \tag{4.7}$$

where $P_V = U_V U_V^H$. For MUSIC, number of sources is a prerequisite. If the number of sources is not known a priori, it should be estimated prior to AoA estimation and fed to MUSIC.

4.2.3 Cross-correlation switched beam system (XSBS)

The existing high performance AoA estimation techniques either have a low resolution problem or require extensive computational complexity to estimate the AoA. Moreover, they require M receivers to implement the AoA estimation technique which increases the hardware complexity tremendously. On the other hand, although conventional SBSs have low hardware and computational complexities, they fail to operate at medium and low SNR levels.

We propose a novel cross-correlation based SBS (XSBS) AoA estimation technique. Our XSBS benefits from the low hardware complexity of the conventional

SBS, which requires a single receiver, yet does not sacrifice the resolution or performance at medium and low SNR levels. Moreover, our XSBS requires low computational complexity to estimate the AoA since it is based on estimating the cross correlation between two collected one dimensional vector of samples. With such low hardware and computational complexity, our XSBS will consume less power which will be very beneficial, particularly, if implemented on a portable device. Furthermore, XSBS requires neither prior information on the number of the sources nor the sources to be uncorrelated.

Our XSBS can be implemented within the conventional AoA estimation paradigm, where a receiver tries to estimate the AoA of a transmitter that is trying to communicate with. However, our XSBS can be very advantageous within the paradigm of SKG. In this case, sequence of AoAs are estimated at Alice and Bob to be used as a common source of randomness.

In the following, we provide a detailed description of the operation of our proposed XSBS alongside the corresponding basic mathematical modelling of the system.

4.2.4 XSBS design

XSBS goes through two phases to estimate the AoA as follows.

- **Phase I**: the *Weights Unit* depicted in Fig. 4.1 controls the RF switches such a single antenna element is turned on, while the remaining antenna elements are switched off. In the selected antenna element branch, the applied weight is unity gain and zero phase shift. Assuming approximate omni-directional pattern for individual antenna elements, XSBS then acquires N samples to collect the signal $\mathbf{x}_o$.

- **Phase II**: In this phase the omni-directional signal collected in the first phase, i.e., $\mathbf{x}_o$, becomes our reference signal. The *Weights Unit* sends the sets of weights $\mathbf{a}(\phi_k)$, for $k \in [1:K]$. The set $\mathbf{a}(\phi_k)$ steers the main beam of the antenna array to the direction ϕ_k. XSBS then acquires N samples to collect the signal $\mathbf{x}_k$. A cross correlation operation between our reference signal $\mathbf{x}_o$ and the k^{th} beam signal is applied. The cross correlation coefficient (R_{ko}) is calculated for K beams. The AoA is the index $\hat{\phi}_k$ with the highest R_{ko}.

4.2.5 Cross correlation estimation

In the second phase of estimating the AoA, XSBS cross correlates the omni-directional reference signal, $\mathbf{x_o} = [x_o[1], \cdots, x_o[n], \cdots, x_o[N]]$, with the directed beam signals, $\mathbf{x_k} = [x_k[1], \cdots, x_k[n], \cdots, x_k[N]]$, for $k \in [1:K]$ through the region of interest as in (4.2). The cross correlation coefficient between the reference signal and the k^{th} signal is given by

$$R_{ko} = \frac{1}{N}\Big(\mathbf{x_k}\ \mathbf{x_o^H}\Big). \tag{4.8}$$

The cross correlation between the omni-directional reference signal and the signals received from the switched beams is the highest at the true AoA and relatively negligible otherwise. To show that, we provide the derivation below. The received signal from the k^{th} beam if k is the true AoA is

$$x_k^{Tr}[n] = G_k s[n+\tau] + v[n+\tau], \tag{4.9}$$

where G_k is the directive antenna array gain and τ is a random time shift. The received signal from the k^{th} beam if k is not the true AoA is $x_k^F[n] = v[n+\tau]$. The cross correlation function in the case of the true AoA, R_{ko}^{Tr}, can be written as

$$\begin{aligned}
R_{ko}^{Tr} &= \frac{1}{N}\sum_{n=1}^{N} x_k^{Tr}[n]\ x_o^H[n] \\
&= \frac{1}{N}\sum_{n=1}^{N}\Big[\left(G_k\ s[n+\tau] + v[n+\tau]\right)\left(G_o\ s^H[n] + v^H[n]\right)\Big] \\
&= \frac{G_o G_k}{N}\sum_{n=1}^{N} s[n+\tau]\ s^H[n] + \frac{G_k}{N}\sum_{n=1}^{N} s[n+\tau]\ v^H[n] \\
&+ \frac{G_o}{N}\sum_{n=1}^{N} v[n+\tau]\ s^H[n] + \frac{1}{N}\sum_{n=1}^{N} v[n+\tau]\ v^H[n].
\end{aligned} \tag{4.10}$$

The cross correlation function in the case that k is not the true AoA, R_{ko}^{F}, can be written as

$$\begin{aligned} R_{ko}^{F} &= \frac{1}{N}\sum_{n=1}^{N} x_k^F[n] x_o^H[n] \\ &= \frac{1}{N}\sum_{n=1}^{N} (v[n+\tau]) \left(G_o\, s^H[n] + v^H[n]\right) \\ &= \frac{G_o}{N}\sum_{n=1}^{N} v[n+\tau]\; s^H[n] + \frac{1}{N}\sum_{n=1}^{N} v[n+\tau]\; v^H[n]. \end{aligned} \tag{4.11}$$

With R_{ss} being the autocorrelation function of $s[n]$, R_{sv} the cross correlation between $s[n]$ and $v[n]$, and $s[n]$ and $v[n]$ are stationary processes, (4.10) can be written as

$$R_{ko}^{Tr} = G_o G_k\, R_{ss}[\tau] + G_k\, R_{sv}[\tau] + G_o\, R_{vs}[\tau] + \sigma^2, \tag{4.12}$$

where σ^2 is the noise variance. (4.11) can be written as

$$R_{ko}^{F} = G_o R_{vs}[\tau] + \sigma^2. \tag{4.13}$$

Since $s(t)$ and $v(t)$ are uncorrelated, R_{sv} and R_{vs} can be considered negligible. Consequently, (4.12) and (4.13) reduce to:

$$R_{ko}^{Tr} = G_o G_k R_{ss}[\tau] + \sigma^2, \tag{4.14}$$

$$R_{ko}^{F} = \sigma^2. \tag{4.15}$$

From (4.14) and (4.15), one can see that $R_{ko}^{Tr} > R_{ko}^{F}$. As the transmitted power increases, $R_{ko}^{Tr} \gg R_{ko}^{F}$.

4.2.6 Addressing practical aspects

In this section, we address some practical aspects of our proposed XSBS. We start by presenting a schematic of XSBS, which details the required components needed to implement XSBS. Then, we proceed to discuss incorporating non-uniform excitation in order to increase the total number of orthogonal generated beams.

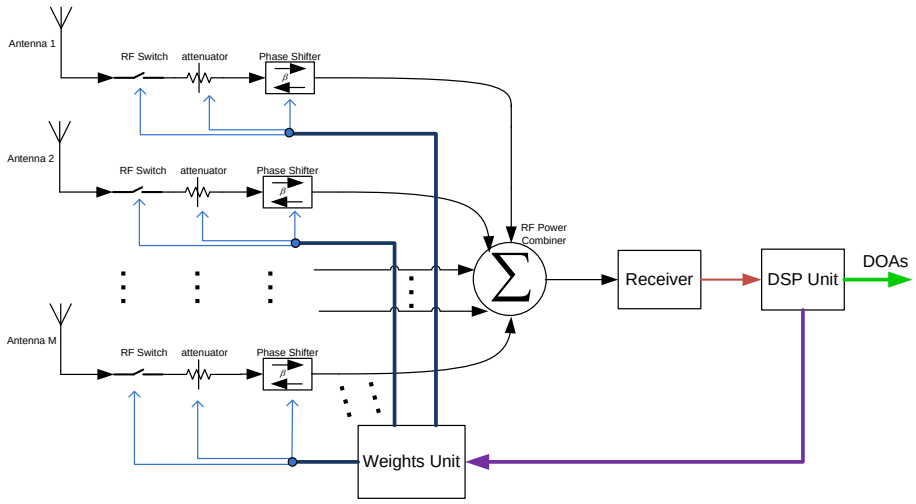

Fig. 4.2 Schematic of proposed XSBS.

Schematic of XSBS

Fig. 4.2 shows the schematic of XSBS. Each antenna is connected to an RF switch, attenuator and phase shifter. Signals from all antenna branches are combined using an RF combiner/divider. A receiver circuitry is then followed to down-convert the collected signal into baseband in order to be processed by the digital signal processing (DSP) unit, which triggers the weights unit to send the pre-calculated weights to the attenuators and phase shifters in order to steer the main beam of the antenna array. The RF switches are added, primarily, because of Phase I of XSBS operation. During this phase, the omni-directional signal, $\mathbf{x_0}$, should be collected from a single antenna branch. RF switches are used to turn on the selected branch and turn off the unwanted ones. This minimizes the leaked signal from the unwanted branches, which could be leaked through the attenuators and phase shifters. During Phase II of XSBS operation, all the RF switches are turned on.

Number of generated orthogonal beams

Orthogonal beams indicate that the peak of the current beam is located at a minima of the two adjacent beams. Hence, when collecting a signal from one beam (assuming a signal is impinging from the direction of the peak), no signal is leaked from its adjacent ones. M is a key factor in determining the resolution of our XSBS. The higher the number of antenna elements, the smaller the half power beam width

(HPBW) of the antenna array beam. Hence, our AoA location grid (assuming orthogonal beams) can become finer and finer, i.e., covering more and more locations as required. A smaller HPBW leads to a better resolution. It is possible to generate as many non-orthogonal beams as possible. For example, for ULA, it is possible to generate 180 beams. However, this approach will increase the scanning time significantly. When using orthogonal beams, the signal impinging on directions that are not the peak location, will be detected by two adjacent beams with different powers. We will show in Sec 4.2.7, that by simply using weighted average, we can detect all AoAs with almost same accuracy. In weighted average the two adjacent peaks are compared and if for example, they are approximately equal, then the signal is impinging at a direction, which is the mid-angle between the two adjacent peaks. On the contrary, a higher M will increase the hardware complexity of XSBS since they will require more weight adjustment components.

Using a non-uniform excitation such as Dolph-Chebyshev excitation, it is possible to generate more *orthogonal* beams using the same M antenna elements. In this case, for ULA , the array response vector $\mathbf{a}(\phi)$ is defined by the Chebyshev polynomial of degree $M-1$, $T_{M-1}(y)$, in the scaled variable y as [86]:

$$\mathbf{a}(\phi) = T_{M-1}(y), \qquad y = y_0 \cos\left(\frac{\beta d \cos(\phi)}{2}\right). \tag{4.16}$$

The scale factor, y_0, is estimated as $y_0 = \cosh\left(\frac{\cosh^{-1}(R)}{M-1}\right)$, where $\cosh^{-1}(.)$ is the inverse hyperbolic cosine function, R is the main lobe to side lobe ratio. The elements of the weight vector $\mathbf{a}(\phi_k)$ for a fixed k and $m \in [1:M]$ can be calculated by creating the z-transform of the array response factor from its zeros and then applying an inverse z-transform. The $M-1$ zeros of $T_{M-1}(y)$ are [86]:

$$y_i = \cos\left(\frac{(i-1/2)\pi}{M-1}\right), \quad \text{for} \quad i = 1,2,...,M-1. \tag{4.17}$$

Let $\psi = \beta d \cos(\phi)$, the pattern zeros are [86]:

$$\psi_i = 2\ \cos^{-1}\left(\frac{y_i}{y_0}\right), \qquad Z_i = 2\exp[j\psi_i], \tag{4.18}$$

where $\cos^{-1}(.)$ is the inverse cosine function, $j = \sqrt{-1}$. The z-transform of the array factor, $A(Z)$, is then [86]:

$$A(Z) = Z^{-(M-1)/2} \prod_{i=1}^{M-1} (Z - Z_i). \tag{4.19}$$

The coefficients, $\mathbf{a_c}$ of dimension $1 \times M$, of the inverse z-transform of $A(Z)$ are the weight vector , which is steered towards ϕ_k to generate $\mathbf{a}(\phi_k)$ by $\psi_k = \beta d \cos\phi_k$, then $\mathbf{a}(\phi_k) = \mathbf{a_c} \exp[j * \psi_k]$.

Sequential vs. binary search

XSBS sequentially scans the angular region of interest to collect K directed signals. XSBS then estimates the cross correlation coefficient for the K beams. This sequential search for the highest peak leads to a longer operation time to detect the AoA. Therefore, quick estimation of the AoA is a key parameter in a efficient AoA system. We propose to use binary search for the peak location rather than sequential, which has two benefits. In binary peak location search, the angular region of interest is divided into two equal regions. The cross correlation coefficient is estimated for the two signals collected from the two regions. The half with the higher cross correlation coefficient is then divided into two equal halves and so on. To do so, the *Weights Unit* adjust the weights accordingly. A subset of the antenna array can be used to achieve this target since lower number of antenna array elements leads to higher HPBW. The rest of the antenna array elements will be switched off using the RF switches. The first benefit of binary search is that it reduces the number of cross correlation estimation from K to $\log_2 K$. For example, for our simulation below with $K = 32$ beams, binary peak search requires the estimation of only 5 beams rather than 32 as in the case of sequential search. The second benefit is that it significantly increases the main lobe to side lobe ratio (R) such that almost no signal is leaked through a side lobe. We start by high HPBW and then reduce it as we get closer to the target. With high HPBW required, the main lobe to side lobe ratio can be very high.

RF receiver architecture

As we stated earlier, unlike MUSIC, which requires M RF receivers, XSBS requires a single RF receiver to down convert the signal to the baseband. With appropriate selection of the receiver architecture, it is possible to improve the estimation accuracy and the noise floor. There exists several receiver architectures including heterodyne and direct conversion receivers. One main drawback of heterodyne receivers is the well known image frequency issue [90]. Typically, the mixing operation is followed by a filter to get rid off the image. However, in order to reduce the image noise, we can either increase the intermediate frequency in order for the filter to apply more attenuation on the image or tolerate more loss in the filter. On the other hand, direct conversion receiver architecture have several advantages over heterodyne architecture such as simplified hardware design, higher power efficiency and lower cost [91]. Therefore, configurable direct conversion receiver architecture could be advantageous within the context of hiding transmitters due to it is low power consumption and improved noise floor.

4.2.7 Performance evaluation of XSBS

First we present results for XSBS's angular resolution. XSBS AoA estimation performance is then compared to MUSIC in terms of peak to floor ratio (PFR), root mean square error (RMSE) and 3-dB success rate for single transmitter case. We then compare the spatial resolution and RMSE of XSBS and MUSIC for two transmitters.

XSBS practical aspects

We start by analyzing the resolution of XSBS; we plot the steered antenna array beam for $M = 17$, separation $d = 0.5\lambda$, $R = 15$ dB, with Dolph-Chebyshev non-uniform excitation in Fig. 4.3. The achieved HPBW is approximately 6 degrees with a total of $K = 32$ *orthogonal* beams scanning the 180 degrees[1]. As M increases, the resolution of XSBS improves since the HPBW decreases.

[1]Fig. 4.3 is plotted using the MATLAB toolbox of [86].

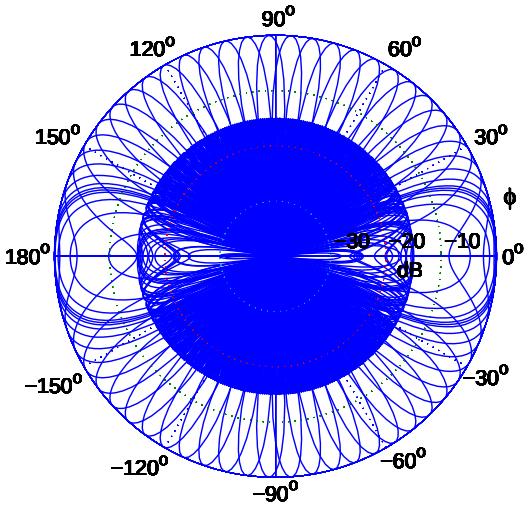

Fig. 4.3 Beam switching antenna array for $M = 17$ with Dolph-Chebychev excitation, $R = 15$ dB and $d = 0.5\lambda$ with a total of 32 orthogonal beams with HBPW = 6 degrees.

XSBS AoA estimation

In the following we evaluate the performance of XSBS AoA estimation with respect to different aspects. We present the PFR as an intuition that XSBS can correctly estimate the true AoA. We compare RMSE and 3-dB success rate of XSBS. We show how XSBS performs when two sources are impinging on the antenna array. The simulation settings in the subsequent figures is as follows. We simulate XSBS with linear antenna array with Dolph-Chebyshev excitation using $M = 17$. MUSIC uses uniform linear antenna array with $M = 16$. We plot the normalized cross correlation coefficient (4.8) to represent the spatial power, versus the azimuth angle ϕ. We assume strong line of sight with block fading (i.e channel is almost constant during the whole processing time).

As we stated in the System Model, we can safely assume that the transmitter continues to transmit a highly coherent signal during the scanning time of XSBS. For example, for a number of beams $K = 32$ and if we collect $N = 1000$ samples from each direction and for a sampling frequency of 5 MHz, the total scanning time is 6.4 milliseconds. Moreover, we proposed binary search approach that reduces the number of required scans from K to $\log_2 k$. For the provided example, the number of scans reduces to 5, which reduces our scanning time to 1 millisecond.

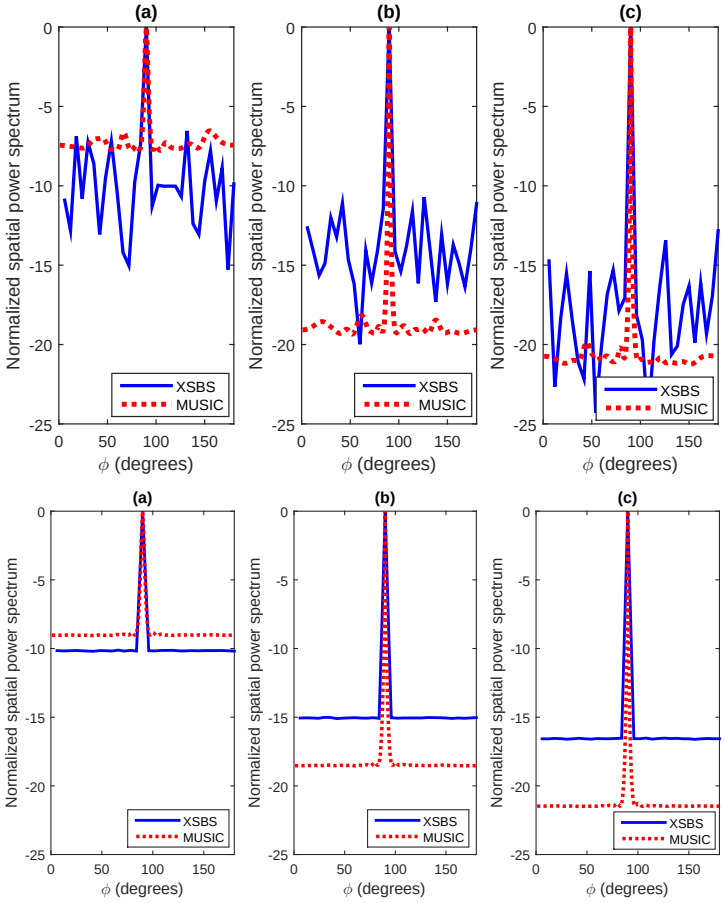

Fig. 4.4 PFR for XSBS vs. MUSIC for single run (top) and average of 1000 iterations (bottom) at SNR = -10 dB for different number of samples (a) $N = 100$, (b) $N = 1000$ and (c) $N = 2000$ samples.

Peak to floor ratio

In Fig. 4.4, we simulate XSBS and MUSIC at SNR = -10 dB for $N = 100$, 1000 and 2000 samples for a signal with arriving angle $\phi_k = 90^\circ$ for a single run (top) and an average of 1000 iteration (bottom). It is shown that XSBS can accurately determine the correct AoA by having the highest peak at the location of the incident angle. Increasing the number of samples improves the performance of XSBS. XSBS achieves PFR = 8 dB, 15 dB and 17 dB for $N = 100$, 1000 and 2000 samples, respectively. MUSIC has a higher PFR achieving PFR = 10 dB, 18 dB and 22 dB for $N = 100$, 1000 and 2000 samples, respectively.

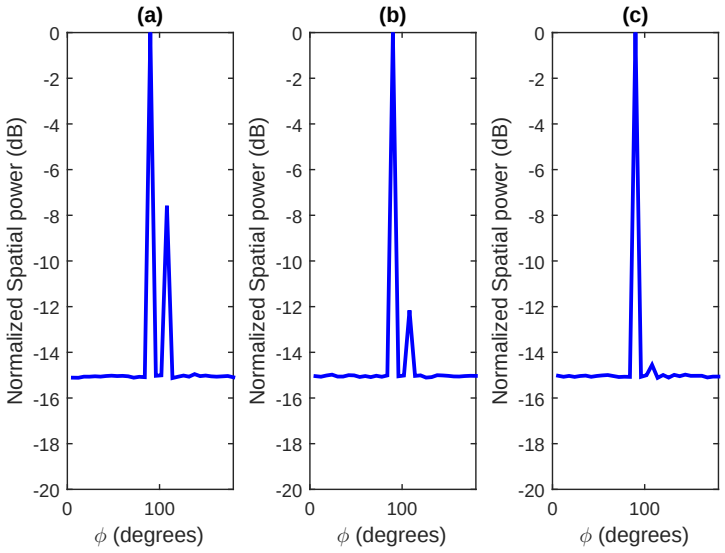

Fig. 4.5 Effect of main lobe to side lobe ratio on the performance of XSBS for $N = 1000$ samples at SNR = -10 dB (a)$R = 15$ dB, (b) $R = 25$ dB and (c)$R = 30$ dB .

Effect of main lobe to side lobe ratio

As we stated earlier, the main lobe to side lobe ratio (R) is a design parameter. When using binary search, we start by high HPBW, for which it is possible for R to be very high such that the signal is received through the main lobe only. However, as we get closer to the location of the incident angle, we must reduce the HPBW of the main lobe, which results in signal getting leaked through a side lobe. This mainly occurs during the last cross-correlation estimation step. In Fig. 4.5, we simulate the scenario of the last binary search step for different values of $R = 15, 25$ and 30 dB. The results are the average of 10000 iterations. The true AoA is 90° and a signal is leaked through a side lobe directed at 108°. Even in the worst case scenario, i.e., $R = 15$ dB, XSBS still can correctly estimate the correct AoA with approximately 8 dB difference between the correct peak and the peak caused due to the side lobe issue.

RMSE versus incident angle

In Fig. 4.6, we plot the RMSE of XSBS and MUSIC for $N = 100$ samples at SNR = -10 dB with the incident angle spanning the 180°. This shows that aside from the poor performance towards the sides of the antenna array, which is common behavior

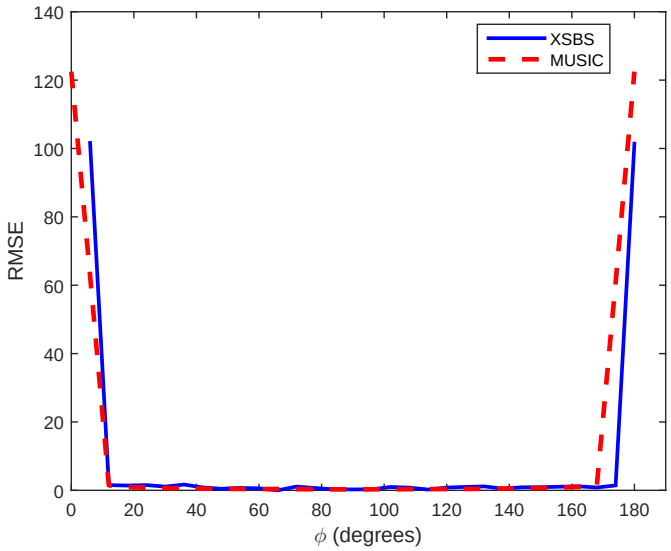

Fig. 4.6 RMSE versus incident AoA for $N = 100$ samples at SNR = -10 dB.

between XSBS and MUSIC, the performance of XSBS is consistent regardless of the location of the incident angle.

In Fig. 4.7, we plot the RMSE for XSBS when the transmitter signal is impinging at angles 85°, 86°, 87°, 88°, 89° and 90° versus SNR for $N = 100$ samples. The received signal is received by the two adjacent orthogonal beams at 84° and 90°. As can be seen by comparing the peaks at the two adjacent beams, we can get very comparable performance for any received AoA using weighted average.

Performance for a single transmitter

Fig. 4.8 depicts the RMSE of XSBS and MUSIC versus SNR (in steps of 2 dB) for different number of samples. XSBS achieves a comparable RMSE to MUSIC with approximately 2 dB performance gap in favor of MUSIC. For example, for $N = 1000$ samples XSBS requires SNR > -16 dB to achieve RMSE of approximately zero, while MUSIC requires SNR > -18.

Fig. 4.9 presents the 3-dB success rate versus SNR for XSBS and MUSIC for different number of samples. The 3-dB success rate is defined as the rate at which the estimated angle is the correct angle with the difference between the first peak (success) and the following peak (false) is at least 3 dB. The 3-dB difference between

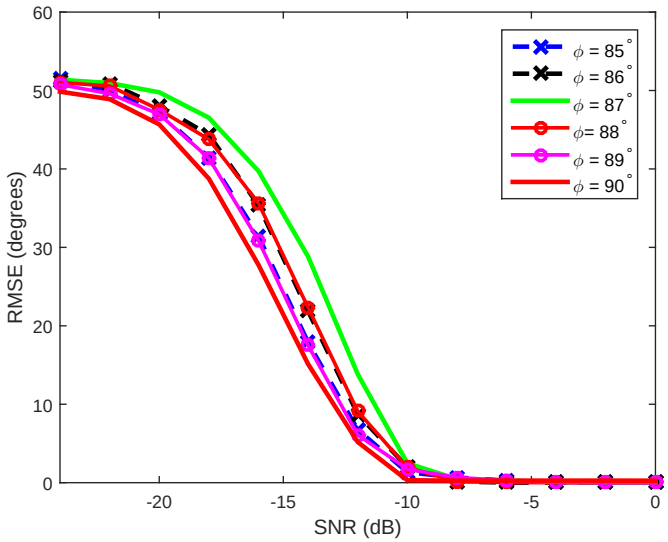

Fig. 4.7 RMSE for XSBS versus SNR for $\phi = 85°, 86°, 85°, 88°, 89°$ and $90°$ for $N = 100$ samples .

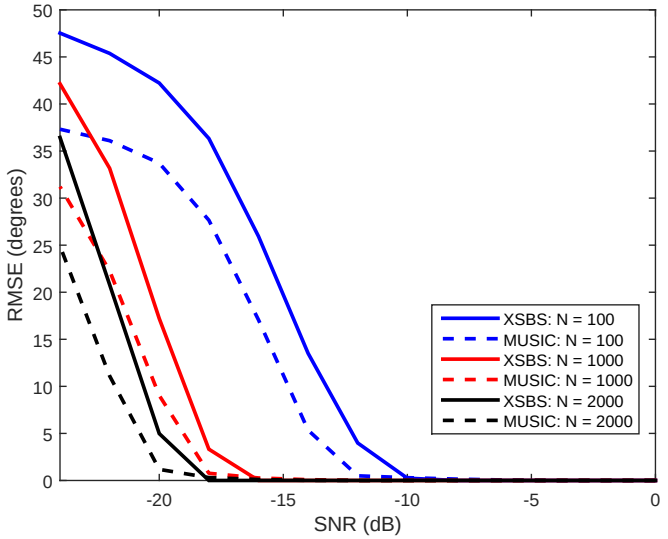

Fig. 4.8 RMSE of XSBS and MUSIC vs. SNR for different number of samples for single transmitter.

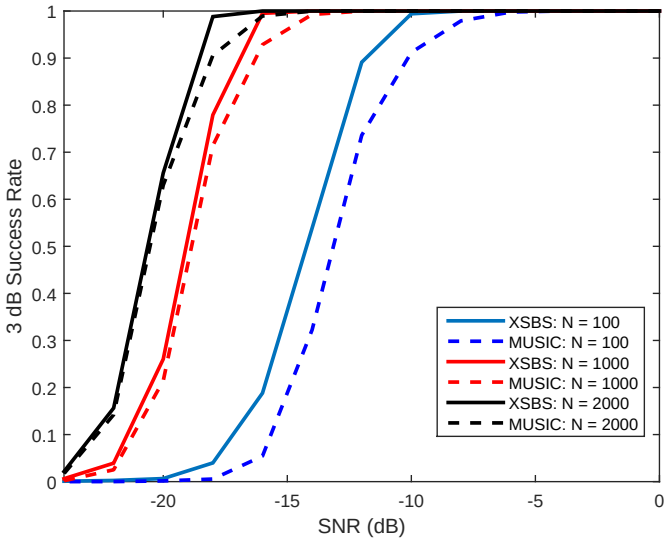

Fig. 4.9 3-dB success rate for XSBS and MUSIC vs. SNR for different number of samples for single transmitter.

the correct peak and the false peak ensures that the AoA estimation process can be performed efficiently with lower probability of error. On the contrary of the RMSE, XSBS outperforms MUSIC with respect to the 3-dB success rate. This indicates that if the threshold is set at 3-dB level, XSBS will have lower probability of error than MUSIC.

Performance for two transmitters

We evaluate the performance of XSBS versus MUSIC when two signals are impinging on the antenna array. The two sources for MUSIC are uncorrelated while we use un-coherent signals for the two sources for XSBS. In Fig. 4.10, we plot the RMSE for XSBS and MUSIC for two sources versus SNR for different number of samples. The degradation in performance for MUSIC and XBSS due to the second source is approximately 2 dB.

In Fig. 4.11, we compare the multi-source resolution of XSBS to the multi-source resolution of MUSIC. It is shown that the resolution of MUSIC highly depends on the received SNR and number of samples while for XSBS, it depends mainly on the HPBW of the main lobe, which is determined based on the number of antenna

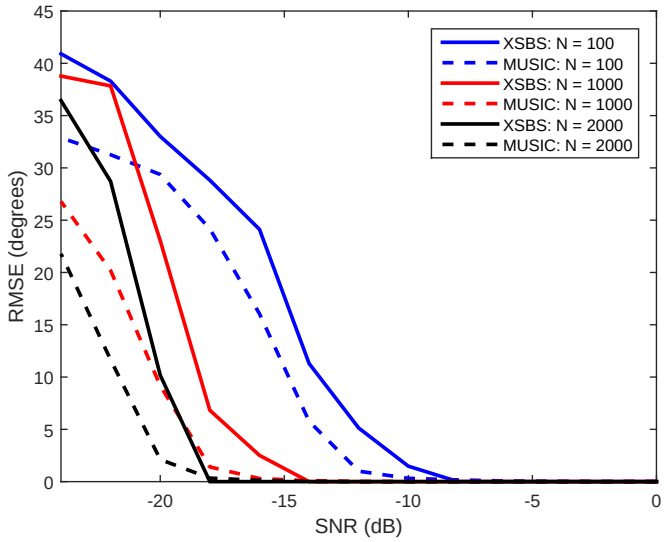

Fig. 4.10 RMSE XSBS vs. MUSIC for two sources at angles $\phi_1 = 90^\circ$ and $\phi_2 = 114^\circ$ using $N = 1000$ samples for: (a) SNR = -10 dB and (b) SNR = -20 dB.

elements M and the type of excitation. For example for $N = 1000$ samples, the resolution of MUSIC is about 8°, while the resolution of XSBS is 12°.

4.2.8 Complexity comparison

Table 4.1 Comparison between MUSIC and XSBS

Item	MUSIC	XSBS
Number of receivers	M	1
EVD	Yes	No
Number of sources	Must be known a priori	Not needed
Correlation between sources	Must be uncorrelated	Works for both correlated and uncorrelated
Maximum number of sources	$M-1$	K
Computational Complexity	$\mathscr{O}\left(M^2N+M^3+JM\right)$	$\mathscr{O}\left(MN\right)$

Complexity analysis provides a qualitative measure of system power consumption as well as real-time processing abilities both on software and hardware subsystems which are critical in dynamic environment such as battlefield.

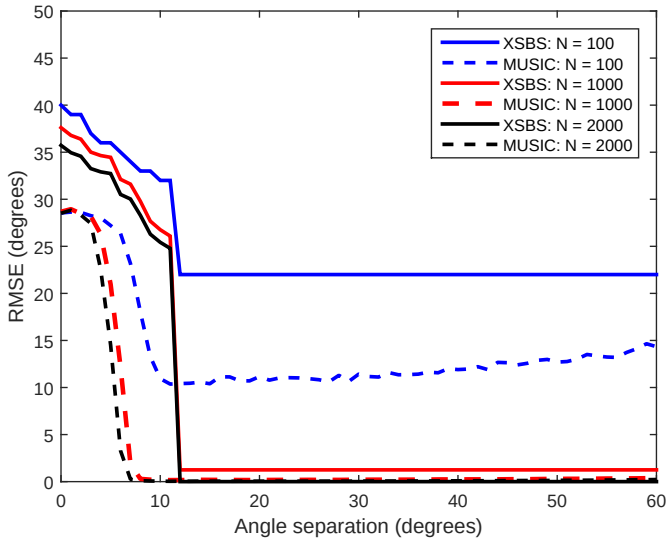

Fig. 4.11 Resolution of MUSIC vs. XSBS for different number of samples at SNR = -15 dB.

For MUSIC, there are three major computational steps needed to estimate the AoA. The first one is the autocovariance function, which requires multiplication of two matrices with sizes $M \times N$ and $N \times M$. The exact number of floating-point operations (flops) needed for this matrix multiplication is $M^2(2N-1)$. The complexity of the first step is $\mathcal{O}\left(M^2N\right)$. The second step is the EVD operation, which has a complexity of $\mathcal{O}\left(M^3\right)$ [92]. The third step is obtaining the spatial pseudo-spectrum, which has a complexity of $\mathcal{O}(JM)$ [89], with J being the number of spectral points of the total angular field of view. Therefore, the complexity of MUSIC is given by $\mathcal{O}\left(M^2N+M^3+JM\right)$. In [92], the complexity of MUSIC is given by $\mathcal{O}\left(M^2N+M^2P\right)$, with P being the number of potential AoAs. In [93], the EVD is simplified using the fast decomposition technique [94], which reduces the complexity of MUSIC to $\mathcal{O}\left(M^2P+M(M-P)J+(M-P)J\right)$.

For XSBS, (4.8) is applied on two vectors each has a dimension of $1 \times N$. The vector multiplication in (4.8) for each $k \in [1:K]$ requires N multiplications and $N-1$ additions. Therefore, for K beams, the exact number of flops is $K(2N-1)$. Hence, the complexity of XSBS is $\mathcal{O}(KN)$. For non uniform excitation, $K \approx 2M$, which reduces the complexity to $\mathcal{O}(MN)$. Consequently, the computational complexity of XSBS is considerably less than the complexity needed in the first step of MUSIC only. In Table 4.1, we present a comparison between XSBS AoA estimation and

MUSIC in terms of different criteria. It is clear that XSBS has lower hardware and computational complexities and less stringent requirements than MUSIC.

4.3 Secret Key Generation Based on AoA

To generate a secret key based on AoA, the estimated AoA has to be common at both Alice and Bob. In other words, both Alice and Bob estimate the same AoA. To do so, Both Alice and Bob agree only once on a selected reference, let it be the North, along with a rotation direction, let it be Clockwise as shown in Fig. 4.12 (a). In this case, the estimated AoA at Alice ϕ_1 is:

$$\phi_1 = \phi_c, \tag{4.20}$$

where ϕ_c is the common AoA and the estimated AoA at Bob ϕ_2 is:

$$\phi_2 = \phi_c + \pi \tag{4.21}$$

Therefore, Bob estimates the common AoA, simply, by subtracting π from its estimated AoA ϕ_2. Another approach is that Alice uses the selected reference, let it be the North and Bob uses the opposite reference which is in this case the South. The rotation direction for Both is still the same, let it be Clockwise. As shown in Fig. 4.12 (b), the estimated AoAs are:

$$\phi_1 = \phi_2 = \phi_c. \tag{4.22}$$

Once Alice and Bob have agreed on the reference direction, they start collecting sequences of the AoA. They then use Algorithm 2 to extract the secret key from these sequences. Algorithm 2 follows same steps for SKG except at the beginning from lines 1 to 5, where Alice and Bob agree on the reference and rotation direction and then estimate the AoA sequence. Note that since estimation error as well as the effect of AWGN is minimal on the estimated AoA, at SNR $>$ 0 dB, it is possible not to use the information reconciliation and the privacy amplification steps.

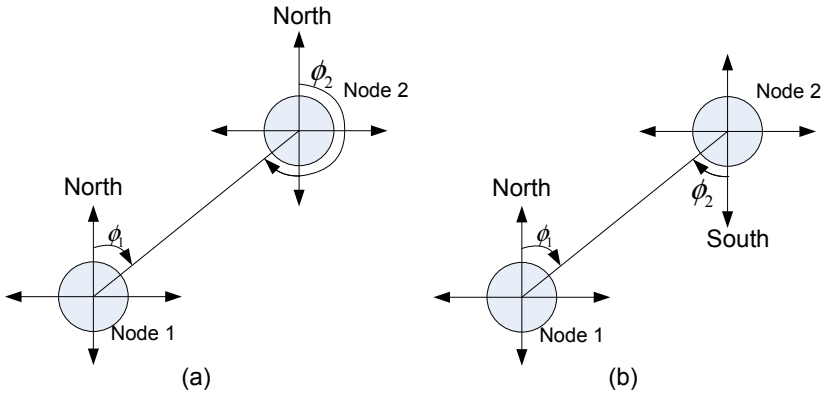

Fig. 4.12 AoA estimation reference: (a) Both have the same reference, let it be the North and (b) Alice has the reference as the North and Bob has the reference as the South.

Algorithm 2 Secret key generation algorithm exploiting AoA.

Step 0: Initialization
Alice and Bob agree on the reference and the rotation direction from which they estimate the AoA.
Step 1: AoA Estimation
Alice and Bob estimate the common source(s) of randomness, ϕ_c, or ϕ_c and θ_c, each using its implemented technique.
Step 2: Uniform Quantization & Encoding
Alice and Bob quantize the ϕ_c or ϕ_c and θ_c using n_{quan} bits to convert the decimal values into bits.
Alice and Bob encode each uniformly quantized value with multiple values n_{encod}.
Step 5: Information Reconciliation (Optional for very low SNR)
Alice and Bob permute the bit stream and divide them into small blocks.
Alice sends the permutation and parities to Bob.
Bob compares the received parity information with his.
In case of mismatch, Bob corrects his bits accordingly.
Step 6: Privacy Amplification (Optional for very low SNR)
Alice sends the number of the hash function to Bob.
Alice and Bob apply the hash function to the bit stream.

Table 4.2 RMSE for MUSIC vs. XSBS for different number of samples.

SNR (dB)	RMSE (degrees)					
	N= 100		N= 1000		N= 2000	
	MUSIC	XSBS	MUSIC	XSBS	MUSIC	XSBS
-0	0	0	0	0	0	0
-5	0	0	0	0	0	0
-10	0	0	0	0	0	0
-15	11	19	0	0	0	0
-20	34	42	9	17	1	5

4.3.1 Performance evaluation for AoA SKG

Fig. 4.8 presents the RMSE for both the MUSIC as well as the XSBS versus SNR for different number of samples. Table 4.2 summarizes the RMSE values for both MUSIC and XSBS for different number of samples at different SNR values. From Table 4.2, one can see that both the MUSIC and the XSBS have a low RMSE at low SNR levels.

We use the estimated RMSE to generate random angles and use them as the seed to generate the secret key. We compare the BMR of the generated keys based on AoA with the BMR of the most commonly used physical layer characteristics which are the channel gain and phase. For a fair comparison between the different common sources of randomness, we first scale the sequence of information collected to the same scaling level such that all common sources of randomness used below, i.e., channel gain, channel phase and AoA fluctuate within the same levels.

4.3.2 MUSIC vs. XSBS

In Fig. 4.13 we compare the performance of the MUSIC algorithm versus the XSBS in generating the secret key. It can be seen that the algorithm based on MUSIC outperforms XSBS based algorithm, which was expected since the RMSE for the XSBS is slightly higher than that for the MUSIC. Both MUSIC and XSBS based SKG algorithms can operate without the need for information reconciliation and privacy amplification steps and using a low number of samples ($N = 100$ samples) for SNR $10 >$ dB. This is a significant improvement in SKG techniques since non of the existing channel based algorithms can operate with an acceptable BMR at such

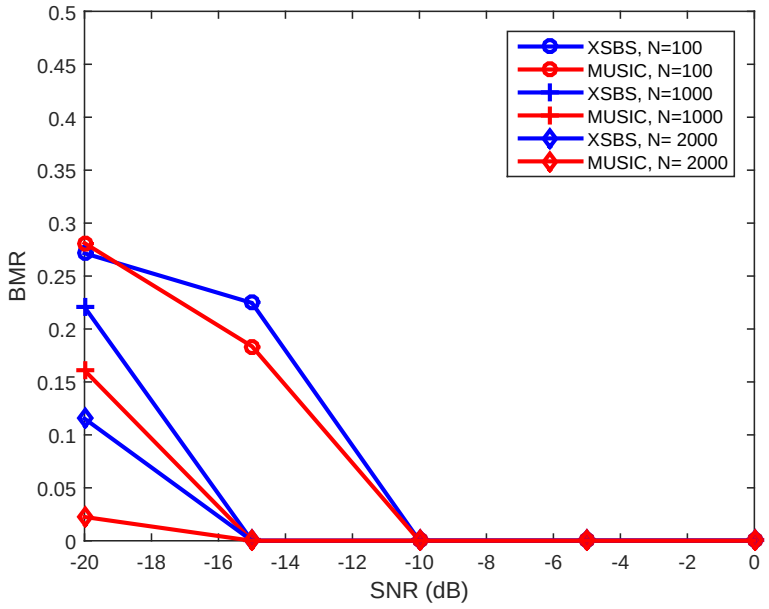

Fig. 4.13 BMR for MUSIC and XSBS vs. SNR for different number of samples.

low SNR levels. In fact, most existing SKG algorithms assume an operation SNR range that higher than 15 dB.

4.3.3 Effect of number of quantization bits

In Fig. 4.14, we compare the BMR of our XSBS based AoA SKG algorithm to channel gain and phase based algorithms up to the quantization and encoding steps versus SNR for different number of quantization bits. As can be seen, our AoA based SKG algorithm has significantly improved the BMR. In fact, channel gain and phase based SKG cannot operate at such low SNR range. In addition, another advantage of our AoA based SKG algorithm is that it removes the need for information reconciliation and privacy amplification steps making it suitable for applications that require a quicker key generation time.

It is shown from Fig. 4.14 that as the number of quantization bits increases, the performance of our algorithm slightly deteriorates. This is expected since as the number of quantization bits increases, more levels are added. Therefore a smaller mismatch or error between the estimated AoAs will lead to more mismatched bit.

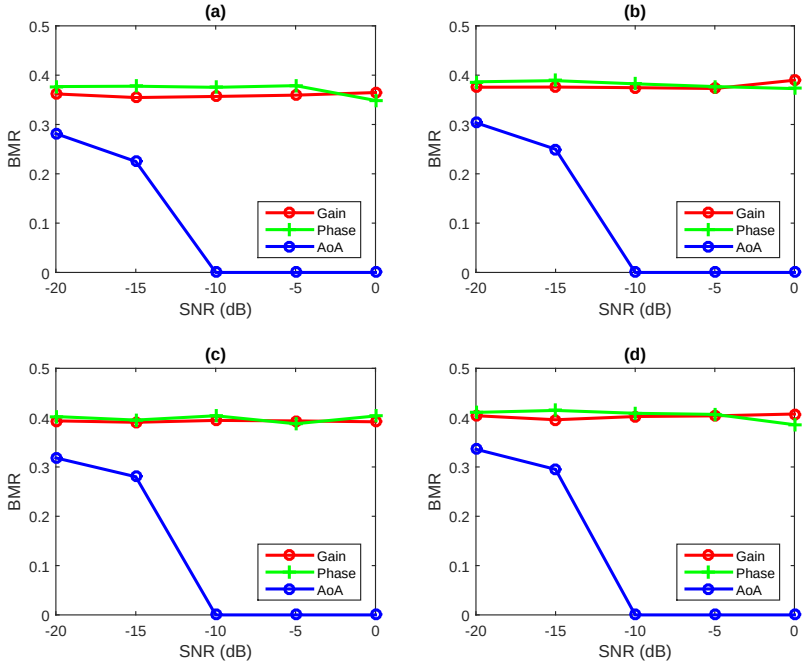

Fig. 4.14 BMR for the AoA based algorithm vs. channel based for (a) $n_q = 6$ and (b) $n_q = 7$ (c) $n_q = 8$ (d) $n_q = 9$.

4.4 Secret Key Generation Based on Channel and Distance Measurements

In this section, we investigate the possibility of fusing multiple common sources of randomness for SKG. In particular, we exploit channel gain and distance between the two communicating nodes. We implement channel gain and distance estimation techniques on WARP hardware platform.

4.4.1 Channel gain measurements

As stated earlier, the channel gain is the most common channel characteristic to generate the secret key. The received signal by Alice and Bob can be given by:

$$y_A = x(t)h(t) + n_A(t) \tag{4.23}$$

$$y_B = x(t)h(t) + n_B(t) \tag{4.24}$$

where $x(t)$ is the transmitted signal, $h(t)$ is the channel and $n_A(t)$ and $n_B(t)$ are AWGN at Alice and Bob's receivers, respectively. Then the estimated channel gain $|\widehat{h}(t)|$ by Alice and Bob's receiver are:

$$|\widehat{h}_A(t)| = |h(t)| + z_A(t) \tag{4.25}$$

$$|\widehat{h}_B(t)| = |h(t)| + z_B(t) \tag{4.26}$$

Where $z_A(t)$ and $z_B(t)$ are noise in estimation of $|h(t)|$ at Alice (A) and Bob (B), respectively. $|\widehat{h}_A(t)|$ and $|\widehat{h}_B(t)|$ are highly correlated. Since Eve listens to all the communication between Alice and Bob, the received signal at Eve's receiver for both signals can be given by:

$$y_E^A = x(t)|h_E^A(t)| + n_E(t) \tag{4.27}$$

$$y_E^B = x(t)|h_E^B(t)| + n_E(t) \tag{4.28}$$

where $|h_E^A(t)|$and $|h_E^B(t)|$ are the channel gains between Alice and Eve (E); and Bob and Eve, respectively. Since it is assumed that Eve can not be less than half wavelength near from either Alice or Bob, $|h_E^A(t)|$ and $|h_E^B(t)|$ are independent from $|\widehat{h}_A(t)|$ and $|\widehat{h}_B(t)|$.

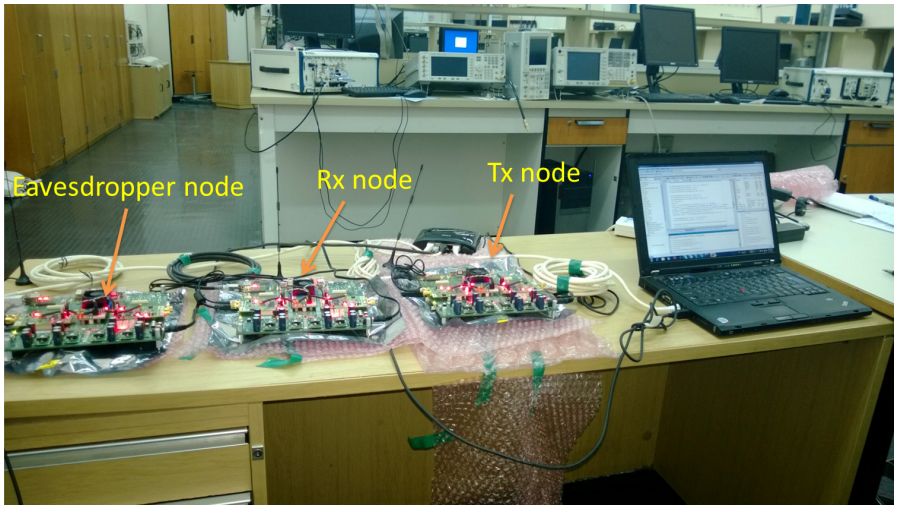

Fig. 4.15 Experimental Setup for the channel gain estimation

We implement channel gain estimation on an FPGA based WARP kits [62]. We use three WARP nodes in our scenario, one is set as the transmitter (Tx), Alice, the second as the intended receiver (Rx), Bob, and the third as the eavesdropper receiver, Eve. Each WARP node has two RF daughter cards that operate as a transceiver in the WiFi band. Figure 4.15 shows our experimental setup after programming the FPGA on the three nodes. Without loss of generality, we implement our algorithm in an indoor non-line of sight indoor environment. In other words, our algorithm can be implemented in any other environment whether its an indoor or outdoor, line of sight or non-line of sight. The Rx node and the eavesdropper node were placed on the corners of the lab while Tx node was at the back of the lab. The separation between the Rx and the eavesdropper was much larger than half the wavelength to avoid channel gain correlation. We estimated the channel gain for both the Alice-Eve channel as well as the Alice-Eve channel. Figure 4.16 shows the channel gain and phase for the two channels for 200 samples.

4.4.2 Distance estimation based On RSS measurements

Most of the currently deployed radios are equipped with RSS estimation circuitry. If the Tx-Rx radio propagation model is known, RSS can be used to estimate the distance between the two communicating node, Alice and Bob. Also distance estimation based on RSS readings does not require additional hardware for time

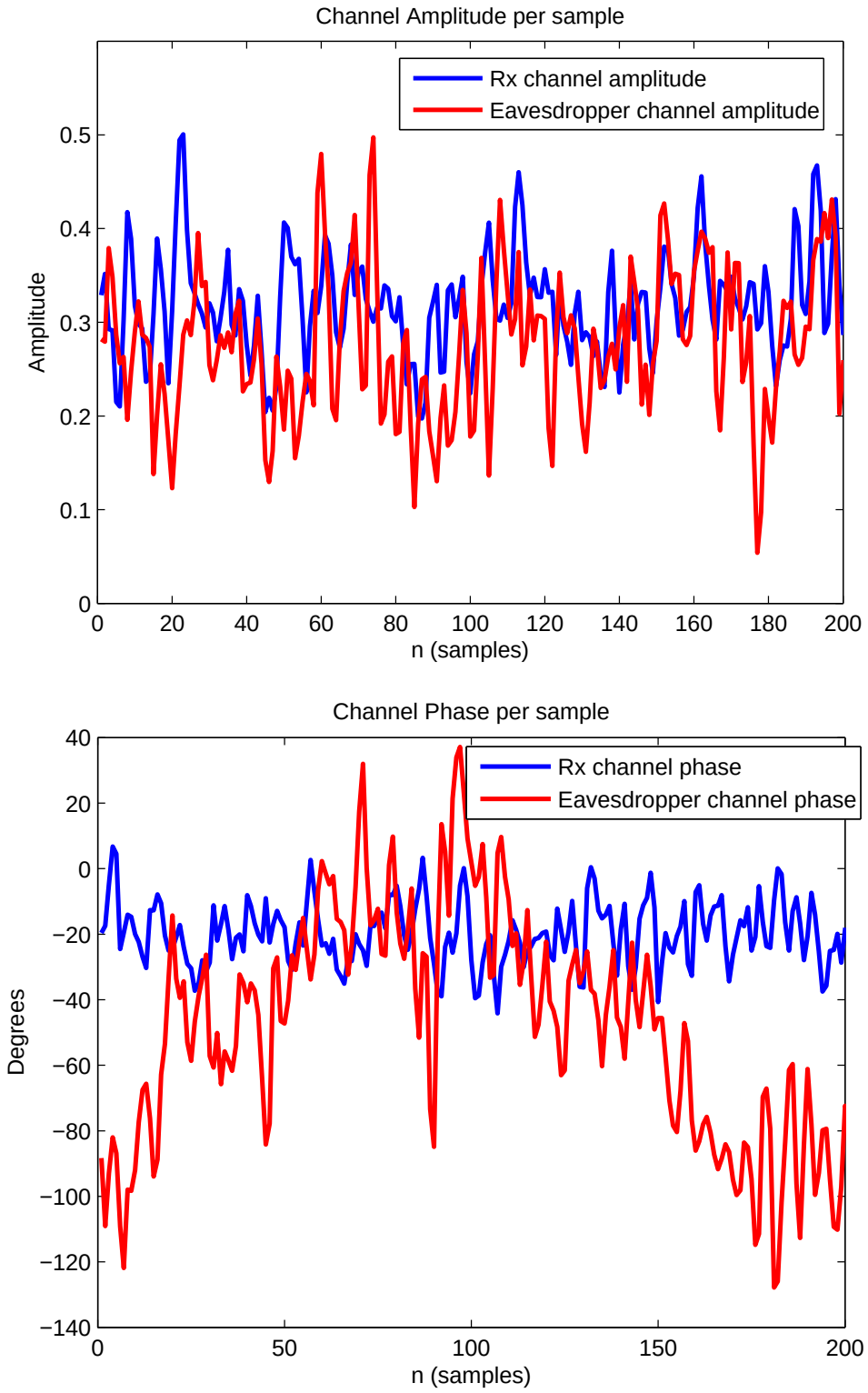

Fig. 4.16 Implementation of channel gain estimation

synchronization such as the TOA based algorithms. The RSS readings measured by Eve can determine the distance between itself and between either Alice or Bob. Eve can only estimate the distance between Alice and Bob if Eve's radio is equipped with AoA estimation system. In this case, given the two angles between Eve and Alice, and Eve and Bob and the two distances, Eve can estimate the distance between Alice and Bob.

Unlike the free space propagation model and the two ray ground model, the log distance path loss model is a more general model that can be used for both indoor and outdoor environments. The log distance path loss model is given by:

$$\overline{P_r(d)}(dBm) = P_r(d_0)(dBm) - 10n_p \log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \tag{4.29}$$

where $\overline{P_r(d)}$ is the average received power in dBm, $P_r(d_0)$ is the received power at a reference distance d_0, n_p is the path loss exponent and X_σ is a normally distributed random variable with zero mean and σ standard deviation. Using a reference distance of 1 meter the equation reduces to:

$$\overline{P_r(d)} = -10n_p \log_{10}(d) + C \tag{4.30}$$

where C is $P_r(1) + X_\sigma$. The distance can then be estimated as:

$$d = 10^{-\frac{RSS-C}{10n_p}} \tag{4.31}$$

For the non-line of sight indoor environment similar to our model, using linear regression estimation, [95] represents Eq. (4.30) as:

$$P_r(d) = -23.411 \log_{10}(d) - 48.676 \tag{4.32}$$

Based on the environment, (4.32) changes. One has to collect empirical data and adjust (4.32) accordingly to minimize the estimation error.

The RSSI readings obtained from our WARP nodes have a dynamic range of 0 to -92 dBm. The average RSSI reading for the received samples after conversion is -68.2 dBm for Bob and -72 dBm for Eve. The measured distance between Alice and Bob is 3.6 meters and between Alice and Eve is 7.5 meters. Based on our non-line

of sight indoor environment and WARP kits readings, we adjust Eq.(4.32) to be:

$$P_r(d) = -20.114\log_{10}(d) - 55.8 \tag{4.33}$$

The estimated distances between Alice and Bob and Alice and Eve are then 4.04 and 7.16 meters, respectively.

4.4.3 Fusing channel and distance measurements for SKG

Now that we have collected channel gain measurements and estimated the distances between the two communicating nodes based on RSS measurements, we will use these two parameters as common sources of randomness. For the fusion operation, we XOR the two bit streams generated from the channel gain and distance. Algorithm 3 presents the algorithm used for SKG exploiting channel gain and distance, which is similar to previous algorithms except line 9, which describes the fusion operation.

Algorithm 3 SKG algorithm exploiting channel gain and distance.

1: **Step 0: Initialization**
2: Alice and Bob exchange signals
3: Alice and Bob collect sequences of channel amplitude measurements
4: Alice and Bob collect sequences of RSS
5: Alice and Bob use average RSS to estimate distance
6: **Step 1: Uniform Quantization & Encoding**
7: Alice and Bob quantize channel amplitude measurements using $Y = Q(X) \quad X \in (d_i, d_{i+1})$
8: Alice and Bob quantize estimated distance using $Y = Q(X) \quad X \in (d_i, d_{i+1})$
9: **Step 2: Combining the Two Bit Streams**
10: Alice and Bob apply bit operation on the two bit streams (e.g., XOR)
11: **Step 3: Information Reconciliation**
12: Alice and Bob permute the bit stream and divide them into small blocks
13: Alice sends the permutation and parities to Bob
14: Bob compares the received parity information with his
15: In case of mismatch, Bob corrects his bits accordingly
16: **Step 4: Privacy Amplification**
17: Alice sends the number of the hash function to Bob
18: Alice and Bob apply the hash function to the bit stream

4.4.4 Performance evaluation

Now that we have presented an implementation test-bed for our algorithm, we evaluate its performance through extensive Monte Carlo simulations. We simulate our algorithm in a Rician fading channel with high K-factor. The Rician K-factor is the ratio between the collected power from the line of sight path to the collected power from all non-line of sight paths. The higher the K-factor, the stronger the line of sight path as compared to all non of light paths. We generate the secret key for our algorithm and compare it to the secret key generated by the channel-only and distance-only algorithms. We compare the bit mismatch rate (BMR) of the generated secret key between A-B and between A-E after quantization and encoding. We also compare the entropy of the secret key generated at either Alice or Bob to the entropy of the secret key generated at Eve for the three algorithms; namely: channel only, distance only and channel and distance. The bit operation applied on the two bit streams at either Alice or Bob is not known to Eve. In Table. 4.3 we summarize the simulation parameters for the subsequent figures.

In Fig.4.17, we present the simulation results for the three algorithms when the A-B channel's K-factor remains constant at 15 and the K-factor for the A-E channel changes between $0:30$. The standard deviation of the estimated distance at Eve is higher than that for either Alice and Bob due to AoA error as well as the errors in estimating the distances based on the received RSS's. The mean in the two cases is 10 meters. At the same time, the A-E BMR is the highest for our algorithm ($\simeq 0.4$). The entropy of the secret key generated at either Alice or Bob for our algorithm is higher than the achieved entropy of the key generated by the two other algorithms. While the entropy of the secret key generated by Eve through our algorithm is the lowest. In other words, our algorithms is achieving a higher secrecy rate than the other two algorithms. The A-E BMR for the channel-only algorithm increases at lower values of K-factor,i.e., weaker line of sight environment and saturates as the K-factor increases. Correspondingly, the BMR of our algorithm is slightly lower at lower values of the K-factor.

In Fig.4.18, we present the simulation results for the three algorithms when the SNR of the received signal by either Alice and Bob remains constant at $10dB$ and the received SNR by Eve changes between $0:30$. Again, the A-B BMR for our algorithm is low, close to the minimum achieved by the distance-only algorithm and the highest between A-E. At the same time, the entropy of the secret key generated

Table 4.3 Simulation Parameter for all the Subsequent Figures

–	Fig.4.17	Fig.4.18	Fig.4.19
SNR A&B	10	15	10
SNR E	10	0:1:30	10
K-factor A-B	15	16	16
K-factor A-E	0:1:30	4	4
Channel Iter.	200	200	200
No. Iter.	10000	10000	10000
A &B Dist. STD	0.92	0.92	2.25
E Dist. STD	1.73	1.73	0:12

at either Alice or Bob for our algorithm is higher than the achieved entropy for key generated by the two other algorithms. At lower values of Eve's received SNR, the performance of the channel-only algorithm was highly degraded since the A-B BMR and the A-E BMR are very comparable. The performance of our algorithm was slightly affected by changing Eve's SNR.

It's worth noting that changing either SNR or the Rician K-factor can be viewed as simulating the mobility of Eve. In other words, Eve is moving to improve its BMR with Alice or Bob.

In Fig.4.19, we present the simulation results for the three algorithms when the standard deviation of the estimated distance between Alice and Bob remains constant at 2.25 and standard deviation of the estimated distance by Eve changes between $0:12$. The mean in the two cases is 20 meters. One can see that performance of the distance only-algorithm was highly affected by changing the standard deviation of the estimated distance by Eve. Changing the standard deviation of the Eve's estimated distances simulates the errors of estimating the two RSS's and the two AoA's. The performance of our algorithm was again slightly affected.

4.5 Conclusion

Existing channel based SKG techniques fail to operate at very low SNR levels. For applications that require to operate at low and very low SNR levels, it is essential to

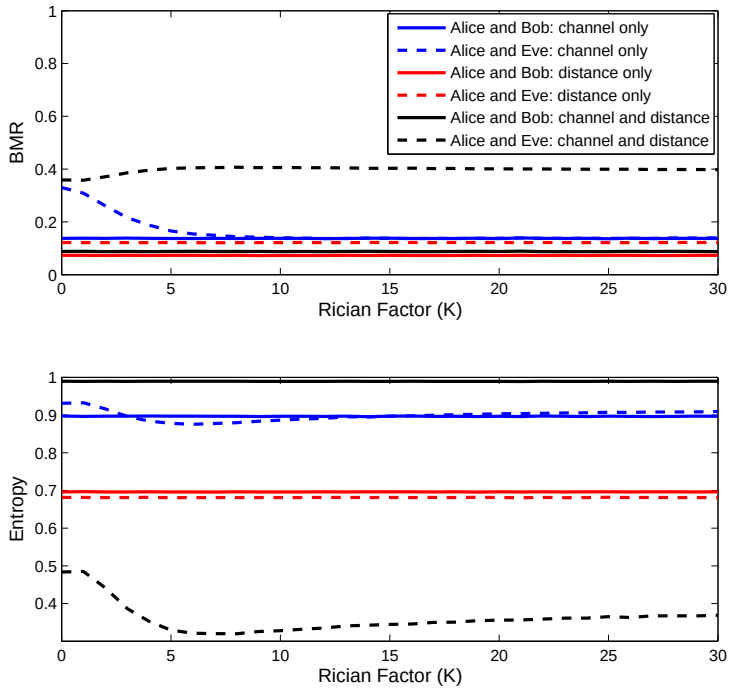

Fig. 4.17 Estimated BMR and entropy between Alice and Bob and Alice and Eve for channel only, distance only and both channel and distance algorithm with the Rician K factor changes at Eve's channel.

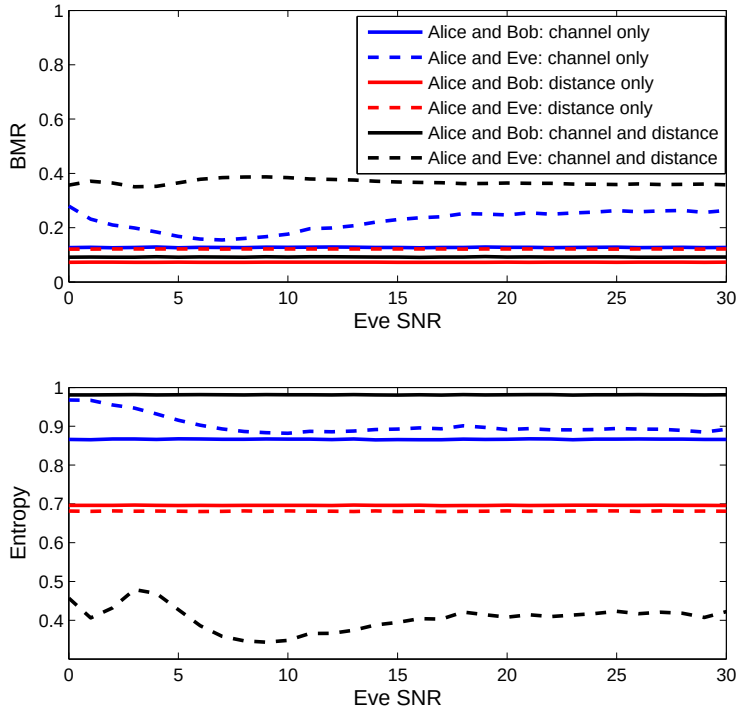

Fig. 4.18 Estimated BMR and entropy between Alice and Bob and Alice and Eve for channel only, distance only and both channel and distance algorithm with Eve's received SNR changes.

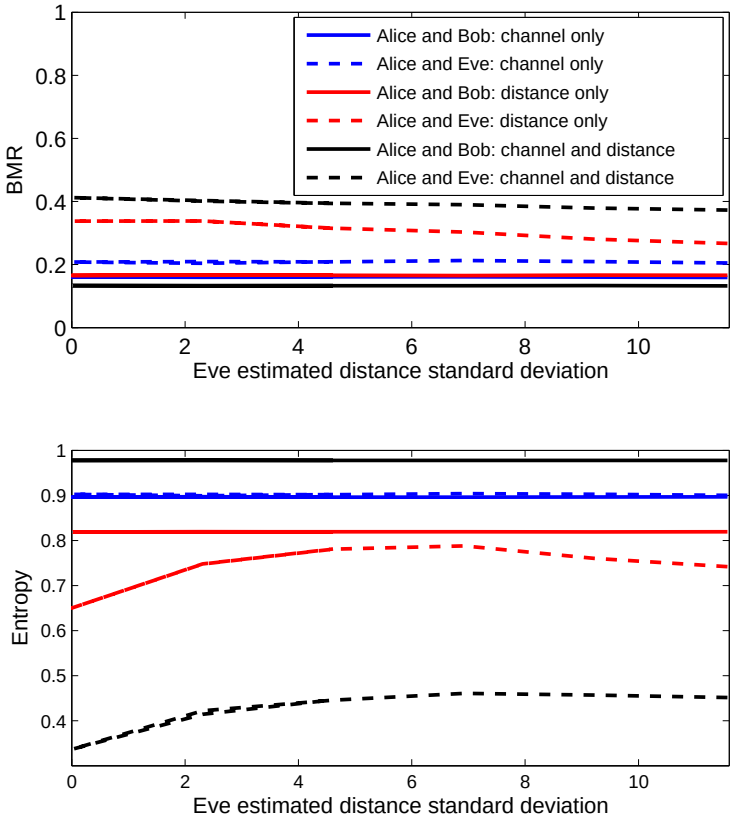

Fig. 4.19 Estimated BMR and entropy between Alice and Bob and Alice and Eve for channel only, distance only and both channel and distance algorithm when Eve's estimated distance standard deviation changes.

exploit a common source of randomness that is less effected by noise. We designed a SKG algorithm that exploits AoA between the two communication nodes for SKG. AoA estimation techniques can operate with high accuracy at low SNR level, hence it is appropriate for this objective.

On the other hand, existing AoA estimation techniques either have high hardware and computational complexity or low performance. For SKG, sequences of AoA has to be collected. Therefore, this motivated the need to design an AoA estimation technique that has low hardware and computational complexity, yet does not sacrifice the performance. We designed XSBS that has comparable performance to MUSIC, yet has much less hardware complexity since it uses only a single receiver chain. Moreover, we showed that XSBS's computational complexity is negligible when compared to MUSIC's.

Furthermore, we investigated fusing multiple common sources of randomness for SKG. In particular, we used channel gain and distance for SKG. We implemented channel estimation on WARP hardware platform as well as distance estimation based on RSS. For strong line of sight environment, exploiting channel gain may be inappropriate due to less fluctuation in the channel. Hence, it becomes necessary in such scenario to fuse another common source of randomness to overcome this shortcoming.

Chapter 5

Security in Cognitive Radio Networks

Rapid deployment of wireless communication systems in diverse applications resulting in an increasing urge for designated exclusive bandwidth allocations [96] is challenged by the scarcity of dedicated spectrum resources. The classic way of assigning the spectrum is that service providers acquire exclusive licenses for designated frequency bands and bandwidth. Recent statistical studies of dedicated spectrum usage revealed spectrum under utilization, which triggered the interest in cognitive radio networks based on deploying dynamic spectrum allocation to achieve higher spectrum utilization [8]. In cognitive radio networks (CRNs), a secondary user (SU) accesses the spectrum whenever the spectrum owner, named primary user (PU), is not transmitting, i.e., interweaving approach, or both PU and SU share the spectrum under the PU's defined terms of usage, i.e., underlay or overlay approach (limited interference). Consequently, reliable spectrum sensing is paramount to realization of efficient and successful cognitive radio networks.

To efficiently benefit from the available assigned spectrum, cognitive radios or secondary users must have the ability of sensing the spectrum to allocate the channels where the primary users are not using them. Several methods have been proposed to sense the spectrum and different detectors have been implemented. The quality of the detector mainly depends on how much information SUs know about the PU's signal. The performance of the detector is evaluated using the receiver operating characteristic (ROC) curves. Higher probability of miss detection, i.e.,

lower probability of detection, implies more interference with the PU signal, while higher probability of false alarm implies less utilization efficiency of empty spectrum slots. The SU's goal is then to achieve the highest possible probability of detection while maintaining the lowest probability of false alarm. In other words, achieving the ROC constraints even at low signal to noise ratio (SNR) levels.

On the other hand, securing the communication link between legitimate SUs is a challenging issue due to the fact that numerous attacks can be launched against cognitive radio networks. These attacks include spectrum sensing data falsification, eavesdropping, PU emulation and objective function attack.

Although CRN can benefit from our low SNR SKG techniques presented earlier, which suit the underlay way of operation of CRNs, and due to the peculiarity of CRNs where SUs exploit only empty spectrum slots for communication, it is of great interest to develop CRNs oriented physical layer security schemes that enable SUs to securely tap into the empty spectrum slots as soon as they are available. Since SUs periodically collect spectrum sensing data, we developed an algorithm to exploit this data for security without interrupting or affecting the sensing process. In other words, the collected data will be used for spectrum sensing as well as SKG. By doing so, SUs can securely exploit empty spectrum slots as soon as they are available rather than employing other physical layer security techniques, which require additional time to generate the secret key.

In this chapter, we first present literature reviews on different spectrum sensing techniques as well as security in CRNs in sections 5.1 and 5.2, respectively. We conduct performance analysis on likelihood ratio based spectrum sensing, which is presented in Section 5.3. In addition, we develop a general likelihood ratio test algorithm that can be used for both detection of PU signal as well as empty spectrum slots. We extend our study on likelihood ratio based spectrum sensing to multiple antenna case as well as full-duplex (FD) CRNs. In addition, we present FPGA implementation of general likelihood ratio based spectrum sensing. Although, we have some work on other spectrum sensing techniques including our work in [97] and [98], we only focus on likelihood ratio spectrum sensing since the data collected through this techniques is then exploited for SKG. In Section 5.4, we exploit general likelihood ratio spectrum sensing data to extract secret key to counteract two popular physical layer attacks on CRNs. The chapter is then concluded in Section 5.5. Some of our work in this chapter is presented in [99] and [100].

5.1 Literature Review on Spectrum Sensing Techniques

The literature in spectrum sensing is rich with numerous sensing methods and varieties of detector implementations. See for example [101, 102]. Typically, the quality of the detector depends on SU's knowledge of the PU's signal characteristics. Spectrum Sensing techniques include matched filtering, energy detection, cyclo-stationary detection (CSD), likelihood ratio based and eigenvalue based [103, 104]. Matched filtering provides the highest SNR in case of noise only. However, matched filter detection requires a prior full knowledge of the PU's transmitted signal [105]. This eventually leads to the need for a designated receiver for each PU's signal format. A simpler approach to spectrum sensing is to perform a non-coherent detection through energy detection (ED). Energy detectors are easy to implement and best suited for a quick decision. The measured energy is compared to a certain threshold to decide whether or not the PU signal is present. The main drawback of ED methods is that the performance of detectors is highly susceptible to varying background noise and interference levels. The fundamentals of ED were first presented in the classic paper by Urkowitz in 1967 [106]. A more sophisticated technique that exploits the structure of the PU's signal and can be used to detect random signals is cyclo-stationary detection. Cyclo-stationary detectors take advantage of the spectral redundancy or distinguished pattern of structured signals to determine whether or not they are present. The fundamentals of cyclo-stationary detection were presented in [107–109].

A different approach to signal detection is based on exploiting the signal's probabilistic models [110, 104]. Maximum likelihood ratio test (MLRT) is the most commonly used probabilistic signal detection technique. MLRT is a measure of how likely the data follows one probability model than the other. If all the probability distribution parameters are known, the test is named MLRT. Otherwise, the test is considered a general likelihood ratio test (GLRT) [105] and [110–112]. GLRT compares the best probabilistic model out of a set of possible models under the first hypothesis to the best probability model out of a set of possible models under the second.

In order to enhance the performance of spectrum sensing and further mitigate the effect of fading and shadowing, SU's can utilize multiple antenna transceiver systems and/or use collaborative decision making to decide on the existence of the PU's signal. The authors in [113] exploited the use of multiple antenna diversity

schemes to mitigate the effect of different fading channels on the performance of energy detectors. They compared three different schemes namely: equal gain combining (EGC), selection combining (SC) and switch and stay combining (SSC). They then studied other relevant schemes in [114] which are square law combining (SLC) and square law selection (SLS) instead of EGC and SC. The main difference between the two streams of schemes is that EGC and SC are pre-detection schemes meaning that the signals are added before sampling while SLC and SLS are post detection schemes meaning that the signals are added after sampling. Relevant work on multiple antennas , but for the energy detection technique, was presented in [115–117]. It was shown that multiple antenna schemes enhance the performance of the system in combating fading and shadowing as the number of antennas increase. It was also shown that EGC and SLC are superior to other schemes yet they are more expensive to implement.

Applying the GLRT approach on multiple antenna systems was introduced in [118–122], where all approaches are based on evaluating the sample covariance matrix as well as the eigenvalue decomposition of the covariance matrix, which has high implementation complexity. In [118], the authors reported that the optimal detector is a maximum ratio combining when all the distribution parameters are known. Their simulated results for the GLRT approach show that with number of antennas of 2 and 8 collected samples, to achieve a probability of detection (P_d) of 90% and a probability of false alarm (P_f) of 10%, an SNR of almost 5 dB is required. As the number of antennas as well as the number of the samples increase, the required SNR to achieve reasonable P_f and P_d decreases. The authors in [120] studied their approach under different MIMO schemes. For example, for P_d of higher than 90%, P_f of 10%, number of SU antennas of 4, number of PU antennas of 2 and number of samples of 512, the required SNR is -8 dB under the Alamouti scheme. The results in [121] are for an unreasonable number of collected samples of 10^4. A comparison between GLRT, ED, arithmetic to geometric mean (AGM) and maximum to minimum eigenvalue (MME) methods is presented in [122]. The GLRT approach showed superior results over the aforementioned approaches.

5.2 Literature Review on Cognitive Radio Security

Several attacks can be launched against CRNs. Comprehensive studies on this aspect [9–11] show that two of the major physical layer attacks against cognitive radio networks are spectrum sensing data falsification (SSDF) and eavesdropping. SSDF is performed on a collaborative sensing setup [12]: an attacker sends false spectrum sensing data to other SUs, in case of distributed sensing decision, or to the fusion center [13], resulting in a wrong spectrum access decision. Eavesdropping attackers instead are adversaries or unauthorized users that listen to the communication between legitimate users.

Conventional techniques to combat SSDF leverage a two-level defense mechanism [14]. The first level authenticates all the collected spectrum sensing results, while the second decides which spectrum sensing result is legitimate. Depending on whether a fusion center is available or the system is fully distributed, schemes such as the sequential probability ratio test (SPRT) [14], or reputation-based schemes can be exploited [14]. Techniques designed to counteract SSDF, however, require a long processing time for the two stages to occur. Moreover, either a large number of SUs or many successful iterations are needed to achieve a good reputation. Clearly, long processing time might lead to higher probability of missing the opportunity of exploiting empty spectrum slots for SUs. In addition, authentication techniques such as the approach in [15], where cyclo-stationary detection is used to classify and authenticate signals, adds to the complexity and limitations of the system, while failing to prevent a scenario where a malicious node mimics the SU's signal properties.

Alternatively, physical layer security techniques exploit the randomness inherent to communication channels, which are common to the two trusted parties and unknown to a potential eavesdropper, so as to generate secret keys [19, 123, 124]. Although these algorithms were not developed for cognitive radio network applications, they can be utilized by the SUs. However, physical-layer solutions, such as channel estimation based on one or two level defence mechanisms, involve exchange of multiple beacon signals as well as synchronization between legitimate SUs thus requiring a long time to generate the link key and, hence an inefficient usage of the spectrum.

To counteract eavesdropping, a power allocation approach is proposed in [125] to increase the secrecy level between authenticated SUs. Alternatively, conventional

wireless security, which relies on cryptographic techniques and application-layer protocols, can be adopted [126]. Fundamentals of key management protocols are presented in [127–129]. One drawback of these techniques however is that a complex key management scheme is required in the case of symmetric ciphers, while high computational complexity is needed in the case of asymmetric ciphers. In particular, in the case of symmetric ciphers, the continuous exchange of encryption keys poses a serious threat to the secrecy of the whole communication session. Minimizing the security risk that stems from key exchange mechanisms is the main reason for key reuse (i.e., using the same key for multiple packet encryptions), which introduces another secrecy weakness allowing an eavesdropper to have more chances to guess the encryption key.

5.3 Likelihood Ratio Based Spectrum Sensing

Likelihood ratio test (LRT) implies that all parameters about the two distributions of the two hypotheses are known. Cumulative sum (CUMSUM) [130–132] minimizes the worst case detection delay. We will present the case of detecting the entrance of the PU signal first followed by the case of detection of empty spectrum slots. We present a review on CUMSUM algorithm then provide our performance analysis for it as well as its extension to multiple antenna systems.

In our system model, a SU, listening to a specific frequency band, collects samples $y[i]$. If the spectrum slot is empty (hypothesis H_0), $y[i] = w[i]$, where $w[i]$ is the additive white gaussian noise (AWGN) with variance σ_w^2. σ_w^2 is receiver dependant and can be estimated ahead of time. If instead the PU is transmitting (hypothesis H_1), $y[i] = x[i] + w[i]$, where $x[i] = hs[i]$ is the product of the channel gain h and the PU's signal $s[i]$. $x[i]$ is assumed to be Gaussian distributed with zero mean and variance σ_x^2. The value of σ_x^2 depends on the channel gain and the power of the PU signal. Thus, in the presence of the PU's signal, $y[i]$ follows a Gaussian distribution $\mathcal{N}(0, \sigma_w^2 + \sigma_x^2)$ [133–135], which we denote by F_1. Instead, in the case of an empty frequency band, $y[i]$ follows $\mathcal{N}(0, \sigma_w^2)$, which we denote by F_0.

The authors in [133] presented a GLRT-based algorithm for the detection of the entrance of the PU's signal. In the presence of an empty spectrum slot, the samples

collected by the SUs follow distribution F_0 with density function f_0, and

$$y[i] = w[i], \qquad \text{for} \qquad i = 1, \cdots, k-1. \tag{5.1}$$

where k is the time instant at which the change of the frequency slot status is detected. As the PU enters the frequency band, the distribution changes to F_1 with density f_1, and

$$y[i] = x[i] + w[i], \qquad \text{for} \qquad i = k, \cdots, N \tag{5.2}$$

where N is the number of samples corresponding to the periodicity with which SUs make their spectrum sensing decisions.

5.3.1 Review of CUMSUM algorithm

Using the LRT based spectrum sensing [110], the problem is treated as a sequential change detection, where the received samples are processed sequentially and the decision is made after each sample. For an idle band, the collected samples by the SU follow distribution F_0 with density function f_0. As the PU starts using the frequency band, the distribution changes to F_1 with density f_1. The log-likelihood ratio is estimated for each sample sequentially:

$$l(y[i]) = \ln\left\{\frac{f_1(y[i])}{f_0(y[i])}\right\}, \tag{5.3}$$

$$= \frac{\sigma_x^2 y^2[i]}{2(\sigma_x^2+\sigma_w^2)\sigma_w^2} + \frac{1}{2}\ln\left\{\frac{\sigma_w^2}{\sigma_x^2+\sigma_w^2}\right\}. \tag{5.4}$$

The Kullback-Leibler divergence of f_0 from f_1 exhibits a negative drift before the entrance of PU signal and positive drift otherwise. The CUMSUM is formalized through:

$$g_N = \max_{k\le N}\left\{\sum_{i=1}^{N} l(y[i] - \sum_{i=1}^{k} l(y[i]))\right\},$$

$$= \max_{k\le N}\sum_{i=k+1}^{N} l(y[i]). \tag{5.5}$$

Therefore, the decision statistic for the CUMSUM test is applied recursively through [111]:

$$\begin{aligned} g_{i+1} &= \max\left\{\max_{k\leq N}\left\{\sum_{i=k+1}^{N} l(y[i])\right\} + l(y[i+1]), 0\right\} \\ &= \max\left\{g_i + l(y[i+1]), 0\right\}, \end{aligned} \tag{5.6}$$

with $g_0 = 0$.

5.3.2 Performance analysis of CUMSUM algorithm

Although the objective of CUMSUM test is to minimize the detection delay, it is of high interest when exploiting CUMSUM in the context of spectrum sensing to know the probability of false alarm as well as the probability of detection when the decision statistic exceeds the threshold.

We derive a closed form expression for the performance parameters, which are the probability of detection as well as the probability of false alarm, of the decision statistic of the CUMSUM test, g_{i+1}.

For two random variables X and Y, the probability distribution function of the random variable $Z = \max[X,Y]$, $F_Z(z)$, can be given by

$$F_Z(z) = Pr\{X \leq z, X > Y\} + Pr\{Y \leq z, X \leq Y\}. \tag{5.7}$$

In our case, g_{i+1} is a random variable defined as the maximum of another random variable and zero. Let $X_{i+1} = g_i + l(y[i+1])$, hence

$$F_{g_{i+1}}(h) = Pr\{X_{i+1} \leq h, X_{i+1} > 0\} + Pr\{0 \leq h, X_{i+1} \leq 0\} \tag{5.8}$$

Since the threshold, h, is always positive, (5.8) becomes

$$F_{g_{i+1}}(h) = Pr\{0 < X_{i+1} \leq h\} + Pr\{X_{i+1} \leq 0\}, \tag{5.9}$$

$$= F_{X_{i+1}}(h), \tag{5.10}$$

where $F_{X_{i+1}}$ is the cumulative distribution of X_{i+1}. The random variable X_{i+1} is the summation of likelihood ratios up to the sample $i+1$ with the chance that each

g_i will be reset to zero at any sample inside the $i+1$ ($g_i = \max[g_{i-1} + l(y[i]), 0]$). Regardless of the number, combination or the locations of each zero incident, what matters is the location of the last occurring zero. Hence, X_{i+1} has $i+1$ possibilities. For example, if the output of the maximization with zero process resulted in no zero, $X_{i+1} = \sum_{j=1}^{i+1} l(y[j])$. If a zero occurred at the first sample, $X_{i+1} = \sum_{j=2}^{i+1} l(y[j])$. Hence

$$F_{X_{i+1}} = Pr\{X_{i+1} \leq h\} \tag{5.11}$$

$$= Pr\left\{\sum_{j=1}^{i+1} l(y[j]) \leq h\right\} + Pr\left\{\sum_{j=2}^{i+1} l(y[j]) \leq h\right\}$$

$$+ \cdots + Pr\{l(y[i+1]) \leq h\} \tag{5.12}$$

$$= \sum_{r=1}^{i+1} Pr\left\{\sum_{j=r}^{i+1} l(y[j]) \leq h\right\}. \tag{5.13}$$

Note that

$$\sum_{j=r}^{i+1} l(y[j]) \leq h = k_1 \left(\sum_{j=r}^{i+1} y^2[j]\right) + (i+2-r)k_2 \leq h \tag{5.14}$$

$$= \sum_{j=r}^{i+1} y^2[j] \leq h_n. \tag{5.15}$$

where $h_n = \frac{h-(i+2-r)k_2}{k_1}$, $k_1 = \frac{\sigma_x^2}{2(\sigma_x^2+\sigma_w^2)\sigma_w^2}$ and $k_2 = \frac{1}{2}\ln\frac{\sigma_x^2}{\sigma_x^2+\sigma_w^2}$. Remember that the received samples, $y[i]$, follow a Gaussian distribution. Therefore, $y^2[i]$ follow a Chi-square distribution. Thus, $\sum_{j=r}^{i+1} y^2[j]$ is a summation of chi-square random variables, hence it is a Chi-square random variable with $i+2-r$ degrees of freedom. Let $G = \sum_{j=1}^{i+1} y^2[j]$.

$$Pr\left\{\sum_{j=r}^{i+1} l(y[j]) \leq h\right\} = Pr\left\{\sum_{j=r}^{i+1} y^2[j] \leq h_n\right\} \tag{5.16}$$

$$= \frac{\gamma\left(\frac{i+2-r}{2}, \frac{h_n}{2\sigma^2}\right)}{\Gamma\left(\frac{i+2-r}{2}\right)}, \tag{5.17}$$

where $\gamma(\cdot,\cdot)$ is the lower incomplete gamma function and $\Gamma(\cdot)$ is the gamma function.

$$F_{X_{i+1}} = \sum_{r=1}^{i+1} \frac{\gamma\left(\frac{i+2-r}{2}, \frac{h_n}{2\sigma^2}\right)}{\Gamma\left(\frac{i+2-r}{2}\right)}. \tag{5.18}$$

The probability of false alarm for the $(i+1)^{th}$ sample where $i \in [1:N]$, is given by:

$$\begin{aligned} P_{f_{i+1}} &= Pr\left\{X_{i+1} > h, \max\left[X_1, \cdots, X_i\right] < h \mid H_0\right\} \\ &= \left(1 - F_{X_{i+1}}\right)\left(\prod_{j=1}^{i} F_{X_j}(h)\right) \\ &= \left(1 - \sum_{r=1}^{i+1} \frac{\gamma\left(\frac{i+2-r}{2}, \frac{h_n}{2\sigma_w^2}\right)}{\Gamma\left(\frac{i+2-r}{2}\right)}\right)\left(\prod_{j=1}^{i}\sum_{r=1}^{j} \frac{\gamma\left(\frac{j+1-r}{2}, \frac{h_n}{2\sigma_w^2}\right)}{\Gamma\left(\frac{j+1-r}{2}\right)}\right). \end{aligned} \tag{5.19}$$

The total probability of false alarm is then

$$P_f = \sum_{i=1}^{N} P_{f_i}. \tag{5.20}$$

Likewise, the probability of detection can be given by

$$P_{d_{i+1}} = Pr\left\{X_{i+1} > h, \max\left[X_1, \cdots, X_i\right] < h \mid H_1\right\} \tag{5.21}$$

$$= \left(1 - F_{X_{i+1}}\right)\left\{\prod_{j=1}^{i} F_{X_j}(h)\right\} \tag{5.22}$$

$$= \left(1 - \sum_{r=1}^{i+1} \frac{\gamma\left(\frac{i+2-r}{2}, \frac{h_n}{2(\sigma_x^2+\sigma_w^2)}\right)}{\Gamma\left(\frac{i+2-r}{2}\right)}\right)\left(\prod_{j=1}^{i}\sum_{r=1}^{j} \frac{\gamma\left(\frac{j+1-r}{2}, \frac{h_n}{2(\sigma_x^2+\sigma_w^2)}\right)}{\Gamma\left(\frac{j+1-r}{2}\right)}\right). \tag{5.23}$$

The total probability of detection is then

$$P_d = \sum_{i=0}^{N} P_{d_{i+1}}. \tag{5.24}$$

5.3.3 Extension to multiple antenna system

Here, we investigate the use of multiple antennas with CUMSUM. Let $Y_{SLC}[i] = \sum_{m=1}^{M} y_m^2[i]$, where M is the number of antennas. Y_{SLC} is a summation of M Chi-square random variables each with 1 degree of freedom. Hence, Y_{SLC} follows a chi-square distribution with M degrees of freedom. Therefore, the probability of false alarm and the probability of detection can be given by:

$$P_{f_{i+1}} = \left(1 - \sum_{r=0}^{i+1} \frac{\gamma\left(\frac{M(i+1-r)}{2}, \frac{h_n}{2\sigma_w^2}\right)}{\Gamma\left(\frac{M(i+1-r)}{2}\right)}\right)\left(\prod_{j=1}^{i}\sum_{r=0}^{j} \frac{\gamma\left(\frac{M(j-r)}{2}, \frac{h_n}{2\sigma_w^2}\right)}{\Gamma\left(\frac{M(j-r)}{2}\right)}\right). \tag{5.25}$$

The probability of detection can be given by

$$P_{d_{i+1}} = \left(1 - \sum_{r=0}^{i+1} \frac{\gamma\left(\frac{M(i+1-r)}{2}, \frac{h_n}{2(\sigma_x^2+\sigma_w^2)}\right)}{\Gamma\left(\frac{M(i+1-r)}{2}\right)}\right)\left(\prod_{j=1}^{i}\sum_{r=0}^{j} \frac{\gamma\left(\frac{M(j-r)}{2}, \frac{h_n}{2(\sigma_x^2+\sigma_w^2)}\right)}{\Gamma\left(\frac{M(j-r)}{2}\right)}\right). \tag{5.26}$$

5.3.4 GLR algorithm

When one of the parameters in the likelihood ratio test in (5.4) is unknown, the test transforms into the generalized form. The scenario we are interested in is when σ_w^2 is known and σ_x^2 is in the range $[\sigma_S^2, \sigma_M^2]$. The generalized log-likelihood ratio is given by [111]:

$$\begin{aligned} B_N &= \max_{k\le N} \sup_{\sigma_x^2} \ln\left\{\prod_{i=k+1}^{N} \frac{f_{1,\sigma_x^2}(y[i])}{f_0(y[i])}\right\} \\ &= \max_{k\le N} \sup_{\sigma_x^2} \sum_{i=k+1}^{N} \left\{\frac{\sigma_x^2 y^2[i]}{2(\sigma_x^2+\sigma_w^2)\sigma_w^2} + \frac{1}{2}\ln\left\{\frac{\sigma_w^2}{\sigma_x^2+\sigma_w^2}\right\}\right\} \end{aligned} \tag{5.27}$$

Let

$$f(\sigma_x^2) = \frac{\sigma_x^{2^*} y^2[i]}{2(\sigma_x^{2^*}+\sigma_w^2)\sigma_w^2} + (N-k)\frac{1}{2}\ln\left\{\frac{\sigma_w^2}{\sigma_x^{2^*}+\sigma_w^2}\right\} \tag{5.28}$$

To estimate the sup in (5.27), one has to solve for the $\sigma_x^{2^*}$ value that maximizes $f(\sigma_x^2)$ over the given σ_x^2 region. The authors in [111] defined k as the sample where $l(y)$ shows a consistent positive drift after. We have

$$\sigma_x^{2^*} = \begin{cases} \sigma_{\mathrm{M}x}^2, & (N-\hat{k}) \leq \frac{\widehat{y}}{\sigma_{\mathrm{M}x}^2+\sigma_w^2}, \\ \frac{\widehat{y}}{N-\hat{k}} - \sigma_w^2, & \frac{\widehat{y}}{\sigma_{\mathrm{M}x}^2+\sigma_w^2} \leq (N-\hat{k}) \leq \frac{\widehat{y}}{\sigma_{\mathrm{S}x}^2+\sigma_w^2}, \\ \sigma_{\mathrm{S}x}^2, & (N-\hat{k}) \geq \frac{\widehat{y}}{\sigma_{\mathrm{S}x}^2+\sigma_w^2}, \end{cases} \tag{5.29}$$

where $\widehat{y} = \sum_{i=\hat{k}+1}^{N} y^2[i]$.

For GLR test, $\sigma_x^{2^*}$ is estimated for each sample inside the N samples. Hence

$$B_N = \max_{k \leq N} \sum_{i=k+1}^{N} \left\{ \frac{\sigma_x^{2^*}[i] y^2[i]}{2(\sigma_x^{2^*}[i]+\sigma_w^2)\sigma_w^2} + \frac{1}{2} \ln \left\{ \frac{\sigma_w^2}{\sigma_x^{2^*}[i]+\sigma_w^2} \right\} \right\}$$

The probability distribution of B_N is given by

$$F_{B_N} = Pr\{g_N \leq h\} \tag{5.30}$$

$$= Pr\left\{ \max_{k \leq N} \sum_{i=k+1}^{N} \left\{ \frac{\sigma_x^{2^*}[i] y^2[i]}{2(\sigma_x^{2^*}[i]+\sigma_w^2)\sigma_w^2} + \frac{1}{2} \ln \left\{ \frac{\sigma_w^2}{\sigma_x^{2^*}[i]+\sigma_w^2} \right\} \right\} \leq h \right\} \tag{5.31}$$

$$= Pr\left\{ \max_{k \leq N} \sum_{i=k+1}^{N} \left(C_1[i] y^2[i] + C_2[i] \right) \leq h \right\} \tag{5.32}$$

$$= Pr\left\{ \max_{k \leq N} \sum_{i=k+1}^{N} C_1[i] y^2[i] \leq \alpha_k \right\}, \tag{5.33}$$

where $C_1[i] = \frac{\sigma_x^{2^*}[i]}{2(\sigma_x^{2^*}[i]+\sigma_w^2)\sigma_w^2}$, $C_2[i] = \frac{1}{2} \ln \left\{ \frac{\sigma_w^2}{\sigma_x^{2^*}[i]+\sigma_w^2} \right\}$ and $\alpha_k = h - \sum_{i=k+1}^{N} C_2[i]$.

$$F_{B_N} = Pr\left\{ \sum_{i=1}^{N} C_1[i] y^2[i] \leq \alpha_0 \right\} \times Pr\left\{ \sum_{i=2}^{N} C_1[i] y^2[i] \leq \alpha_1 \right\} \times \cdots \times Pr\left\{ C_1[N] y^2[N] \leq \alpha_{N-1} \right\}. \tag{5.34}$$

Note that each term in (5.34) is a linear combination of chi-square random variables

5.3.5 Performance of spectrum sensing based on GLR in full-duplex CRN

The residual self interference, $z[i]$, is modelled as Gaussian with zero mean and variance $\sigma_z^2 = \gamma_{zw}\sigma_w^2$ [136–138], where γ_{zw} is the residual self interference signal to noise ratio. When the PU signal is present, $y_{FD}[i]$ follows $\mathcal{N}(0, \gamma_{zw}(\sigma_w^2+1)+\sigma_x^2)$, which we denote by F_1^{FD}. When there exists an empty spectrum slot, $y_{FD}[i]$ follows $\mathcal{N}(0, \sigma_w^2(\gamma_{zw}+1))$, which we denote by F_0^{FD}. The FD signal to noise ratio is given by $\gamma_{FD} = \gamma_{HD}/(1+\gamma_{zw})$. Due to residual self interference in FD systems, the log-likelihood ratio for the detection of the entrance of the PU signal is estimated for each sample sequentially as:

$$l_2(y_{FD}[i]) = \ln\left\{\frac{f_1^{FD}(y[i])}{f_0^{FD}(y[i])}\right\}. \tag{5.35}$$

By substituting the probability density functions f_1^{FD} and f_0^{FD} and taking the natural log, (5.35) reduces to:

$$\begin{aligned} l_2(y_{FD}[i]) = \frac{1}{2}\ln\left\{\frac{\sigma_w^2(\gamma_{zw}+1)}{\sigma_x^2+\sigma_w^2(\gamma_{zw}+1)}\right\} \\ + \frac{\sigma_x^2 y_{FD}^2[i]}{2(\sigma_x^2+\sigma_w^2(\gamma_{zw}+1))\sigma_w^2(\gamma_{zw}+1)}. \end{aligned} \tag{5.36}$$

While the spectrum is empty, i.e., H_0

$$\begin{aligned} \mathbb{E}_{f_0^{FD}}\left\{l_2\left(y_{FD}[i]\right)\right\} &= \int f_0^{FD}(y_{FD})\ln\left\{\frac{f_1^{FD}(y_{FD})}{f_0^{FD}(y_{FD})}\right\}dy \\ &= -D\left(f_0^{FD}||f_1^{FD}\right) \le 0, \end{aligned} \tag{5.37}$$

where the Kullback-Leibler divergence of f_0^{FD} from f_1^{FD}, $D\left(f_0^{FD}||f_1^{FD}\right)$, estimated as

$$\begin{aligned} D\left(f_0^{FD}||f_1^{FD}\right) = -\frac{1}{2}\ln\left\{\frac{\sigma_w^2(\gamma_{zw}+1)}{\sigma_x^2+\sigma_w^2(\gamma_{zw}+1)}\right\} \\ - \frac{\sigma_x^2}{2\left(\sigma_x^2+\sigma_w^2(\gamma_{zw}+1)\right)}. \end{aligned} \tag{5.38}$$

After the entrance of the PU in the case H_1,

$$\begin{aligned}\mathbb{E}_{f_1^{FD}}\left\{l_2\left(y_{FD}[i]\right)\right\} &= \int f_1^{FD}(y_{FD}) \ln\left\{\frac{f_1^{FD}(y_{FD})}{f_0^{FD}(y_{FD})}\right\} dy \\ &= D\left(f_1^{FD}||f_0^{FD}\right) \geq 0, \end{aligned} \tag{5.39}$$

where $D\left(f_1^{FD}||f_0^{FD}\right)$ estimated as:

$$\begin{aligned} D\left(f_1^{FD}||f_0^{FD}\right) &= \frac{1}{2}\ln\left\{\frac{\sigma_w^2(\gamma_{zw}+1)}{\sigma_x^2+\sigma_w^2(\gamma_{zw}+1)}\right\} \\ &\quad + \frac{\sigma_x^2}{2\sigma_w^2(\gamma_{zw}+1)}. \end{aligned} \tag{5.40}$$

$l_1(y_{FD})$ shows a negative drift during H_0 and a positive drift during H_1. The decision statistic based on GLR for the FD system, E_N, can be written as:

$$\begin{aligned} E_N &= \max_{k\leq N}\sup_{\sigma_x^2}\left\{\sum_{i=k+1}^{N} l_{2,\sigma_x^2}(y_{FD}[i])\right\}, \\ &= \max_{k\leq N}\sup_{\sigma_x^2}\ln\left\{\prod_{i=k+1}^{N}\frac{f_{1,\sigma_x^2}^{FD}(y_{FD}[i])}{f_0^{FD}(y_{FD}[i])}\right\}, \\ &= \max_{k\leq N}\sup_{\sigma_x^2}\sum_{i=k+1}^{N}\left(\frac{1}{2}\ln\left\{\frac{\sigma_w^2(\gamma_{zw}+1)}{\sigma_x^2+\sigma_w^2(\gamma_{zw}+1)}\right\}\right. \\ &+ \left.\frac{\sigma_x^2 y_{FD}^2[i]}{2(\sigma_x^2+\sigma_w^2(\gamma_{zw}+1))\sigma_w^2(\gamma_{zw}+1)}\right). \end{aligned} \tag{5.41}$$

Let:

$$\begin{aligned} f_1^{FD}(\sigma_x^2) &= \frac{N-k}{2}\ln\left\{\frac{\sigma_w^2(\gamma_{zw}+1)}{\sigma_x^2+\sigma_w^2(\gamma_{zw}+1)}\right\} \\ &\quad + \frac{\sigma_x^2\widehat{y}_{FD}}{2(\sigma_x^2+\sigma_w^2(\gamma_{zw}+1))\sigma_w^2(\gamma_{zw}+1)}. \end{aligned} \tag{5.42}$$

$$\sigma_x^{2^*} = \begin{cases} \sigma_{\mathrm{M}x}^2, & (N-k) \leq \frac{\widehat{y}_{FD}}{\sigma_{\mathrm{M}x}^2+\sigma_w^2(\gamma_{zw}+1)}, \\ \frac{\widehat{y}_{FD}}{N-k} - \sigma_w^2(\gamma_{zw}+1), & \frac{\widehat{y}_{FD}}{\sigma_{\mathrm{M}x}^2+\sigma_w^2(\gamma_{zw}+1)} \leq (N-k) \leq \frac{\widehat{y}_{FD}}{\sigma_{\mathrm{S}x}^2+\sigma_w^2(\gamma_{zw}+1)}, \\ \sigma_{\mathrm{S}x}^2, & (N-k) \geq \frac{\widehat{y}_{FD}}{\sigma_{\mathrm{S}x}^2+\sigma_w^2(\gamma_{zw}+1)}. \end{cases} \tag{5.43}$$

where $\widehat{y}_{FD} = \sum_{i=1}^{N} y_{FD}^2[i]$. σ_x^2 is not known, we find its estimate $\sigma_x^{2^*}$ by solving (5.42) for the value that maximizes it within the given range $\sigma_{Sx}^2 \leq \sigma_x^2 \leq \sigma_{Mx}^2$, which results in (5.43). So, in order to estimate the decision statistic E_N, we first find $\sigma_x^{2^*}$ through (5.43) and then substitute it in (5.41) for a preset N and iterative k.

The decision statistic E_N is computed for the entire N samples and then compared to a threshold λ_E to decide on the presence or absence of the PU's signal according to:

$$E_N \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_E. \tag{5.44}$$

The relationship between the average delay to false alarm, $\overline{T_0}$, and the threshold, h, is obtained through [139, 140]:

$$\lambda_E = -\ln\{a/b\}, \tag{5.45}$$

where a is a design parameter, which is set based on $\overline{T}_0$ according to:

$$\overline{T}_0 \geq 1/a, \tag{5.46}$$

and b is given by:

$$b = 3\ln\left\{a^{-1}\left(1 + \frac{1}{D_E(f_{1,\sigma_{Sx}^2}^{FD} || f_0^{FD})}\right)^2\right\}, \tag{5.47}$$

where $D_E(f_{1,\sigma_{Sx}^2}^{FD} || f_0^{FD})$ is estimated as in (5.40) at σ_{Sx}^2. When detecting an empty spectrum slot, the probability of false alarm is defined as:

$$P_f = Pr\left(E_N > \lambda_E | H_1\right), \tag{5.48}$$

and the probability of detection as:

$$P_d = Pr\left(E_N > \lambda_E | H_1\right). \tag{5.49}$$

5.3.6 Uncertainty in estimating the variance of residual self interference and noise

So far perfect knowledge of the noise variance as well as the variance of the residual self interference was assumed. However, in practical systems, due to several reasons including lack of noise calibration and interference, noise uncertainty is inevitable. In addition, error in estimating the variance of the residual self interference is likely due to calibration and/or the self interference channel not being a flat fading channel. This affects the sensitivity of the GLR algorithm presented above.

We study the sensitivity of the GLR algorithm in the FD case, when there is uncertainty in the noise variance and/or the residual self interference. It is worth noting that this is different from the case where the variance is completely unknown, which leads to nonparametric detection as in [141]. Uncertainty in the noise variance and/or the residual self interference leads to what is known as signal to noise ratio (SNR) wall, which is the SNR level below which reliable sensing is impossible [142]. Below the SNR wall, increasing the number of collected samples does not improve the performance of the sensing algorithm. In order to estimate the SNR wall for the FD GLR algorithm presented above, we model both uncertainty by the parameter $\rho > 1$, which quantifies the size of uncertainty. The variance of $(z[i] + w[i])$ lies in the range $\left(\sigma_z^2 + \sigma_w^2\right) \in \left[(1/\rho)\left(\sigma_z^2 + \sigma_w^2\right) : \rho\left(\sigma_z^2 + \sigma_w^2\right)\right]$. $\rho = 1$ indicates that there exists no uncertainty in the variance of $(z[i] + w[i])$.

5.3.7 FPGA implementation of GLR based spectrum sensing

We introduce an implementation of our GLR algorithm on an FPGA. The design is implemented on the WARP kits. Our design presented in Fig.5.1 is carried out in ISE System Generator for DSP. The design is then incorporated with the WARP core files using Xilinx Platform Studio (XPS) and Xilinx Software Development Kit (SDK). After successful generation of the bit stream file, it's downloaded to the FPGA using iMPACT. Our design is represented in the Fix 16_15 format. It has a series combination of two bit-division procedures. The minimum achievable sample delay for each bit-division calculation is the number of the bits divided, which is 16 bits in our case. This means that an excess delay of 32 samples is added to the algorithm detection time. Our design is for the unknown σ_x^2. Before the design

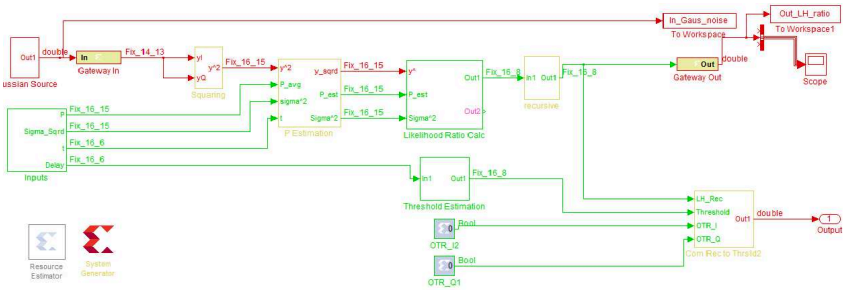

Fig. 5.1 FPGA design for GLR detection algorithm..

Table 5.1 Resources Table

Resources	ED	GLR	CSD
Slices	985	6848	3093
Flip flops	1471	10184	4794
Block RAM's	–	–	9
LUT's	1327	9532	4418
IOB's	–	–	150
Multipliers	1	6	39

is incorporated with the WARP core files, it was simulated using SIMULINK's Gaussian source as the input and the output was plotted on a scope.

Our design consists of several blocks. We first compute the square of the received signal. The output of this block can be used to estimate the decision statistic for the ED approach as well. We then estimate the value of $\sigma_x^{2^*}$ in the *P Estimation block* by implementing equation (5.29). The decision statistic for our GLR algorithm is then computed recursively in the *Likelihood Ratio Calc* block by implementing equation (5.27).

We compare the resources used to implement GLR to the resources uses by cyclostationary detection as well as energy detection (ED) [97]. Table 5.1 shows the resources used in the implementation of the three techniques. It is shown that the cylostationary detection consumes more resources than the conventional energy detection technique and less than GLR based algorithm.

5.3.8 Detection of empty spectrum slots

We develop the GLR algorithm to detect the transmission opportunities, i.e. empty spectrum slots, rather than detecting the entrance of the PU's signal. Again, at first the samples collected by the SU follow distribution F_1 with density function f_1 (hypothesis H_1), and

$$y[i] = x[i] + w[i], \qquad \text{for} \qquad i = 1, \cdots, k-1, \tag{5.50}$$

As the PU leaves the frequency band, the distribution changes to F_0 with density f_0 (hypothesis H_0) and $\exists k \in [1, N]$

$$y[i] = w[i], \qquad \text{for} \qquad i = k, \cdots, N. \tag{5.51}$$

With $l_2(y)$ being the log-likelihood ratio in this case, note that:

$$\begin{aligned} \sum_{i=\hat{k}+1}^{N} l_2(y[i]) &= \ln \left\{ \prod_{i=\hat{k}+1}^{N} \frac{f_0(y[i])}{f_{1,\sigma_x^2}(y[i])} \right\} \\ &= \sum_{i=\hat{k}+1}^{N} \left\{ \frac{1}{2} \ln \left\{ \frac{\sigma_w^2 + \sigma_x^2}{\sigma_w^2} \right\} - \frac{\sigma_x^2 y^2[i]}{2(\sigma_x^2 + \sigma_w^2)\sigma_w^2} \right\}. \end{aligned} \tag{5.52}$$

Let:

$$f(\sigma_x^2) = (N - \hat{k}) \frac{1}{2} \ln \left\{ \frac{\sigma_x^2 + \sigma_w^2}{\sigma_w^2} \right\} - \frac{\sigma_x^2 \widehat{y}}{2(\sigma_x^2 + \sigma_w^2)\sigma_w^2}. \tag{5.53}$$

Since σ_x^2 is unknown, we find its estimate $\sigma_x^{2^*}$ by solving (5.53) for the value that maximizes it, which results in:

$$\sigma_x^{2^*} = \begin{cases} \sigma_{\mathrm{M}x}^2, & (N - \hat{k}) \leq \frac{\widehat{y}}{\sigma_{\mathrm{M}x}^2 + \sigma_w^2}, \\ \frac{\widehat{y}}{N - \hat{k}} - \sigma_w^2, & \frac{\widehat{y}}{\sigma_{\mathrm{M}x}^2 + \sigma_w^2} \leq (N - \hat{k}) \leq \frac{\widehat{y}}{\sigma_{\mathrm{S}x}^2 + \sigma_w^2}, \\ \sigma_{\mathrm{S}x}^2, & (N - \hat{k}) \geq \frac{\widehat{y}}{\sigma_{\mathrm{S}x}^2 + \sigma_w^2}, \end{cases} \tag{5.54}$$

where $\widehat{y} = \sum_{i=\hat{k}+1}^{N} y^2[i]$. Consequently, for a preset N, an iterative $\hat{k}$ and $\sigma_x^{2^*}$ estimated through (5.54), the decision statistic, denote by g_N, is given by:

$$\begin{aligned} g_N &= \max_{\hat{k}\leq N} \sup_{\sigma_x^2} \ln \left\{ \prod_{i=\hat{k}+1}^{N} \frac{f_0(y[i])}{f_{1,\sigma_x^2}(y[i])} \right\} \\ &= \max_{\hat{k}\leq N} \sum_{i=\hat{k}+1}^{N} \left\{ \frac{1}{2} \ln \left\{ \frac{\sigma_w^2 + \sigma_x^{2^*}}{\sigma_w^2} \right\} - \frac{\sigma_x^{2^*} y^2[i]}{2(\sigma_x^{2^*} + \sigma_w^2)\sigma_w^2} \right\}. \end{aligned} \tag{5.55}$$

The decision statistic g_N is again compared to a threshold λ_g to decide on the presence or absence of the PU's signal according to: $E_N \underset{H_1}{\overset{H_0}{\gtrless}} \lambda_g$. The threshold, $\lambda_B = -\ln\{a/b\}$, is set based on the average delay for false alarm $\overline{T_0} \geq 1/a$ where a is a design parameter and b is given by

$$b = 3 \ln \left\{ a^{-1} \left(1 + \frac{1}{D(f_0 || f_{1,\sigma_{Sx}^2})} \right)^2 \right\}, \tag{5.56}$$

with $D(f_0||f_{1,\sigma_{Sx}^2})$ being the Kullback-Leibler divergence of f_0 from f_1 estimated at σ_{Sx}^2. The Kullback-Leibler divergence of f_0 from f_1 is given by:

$$\begin{aligned} D(f_0||f_1) &= \mathbb{E}_{f_0} \{ l_2(y[i]) \} \\ &= \int f_0(y) \ln \left\{ \frac{f_0(y)}{f_1(y)} \right\} dy, \end{aligned} \tag{5.57}$$

where $\mathbb{E}$ denotes the expectation operator. Substituting f_0 and f_1 at σ_{Sx}^2 yields

$$D\left(f_0||f_{1,\sigma_{Sx}^2}\right) = \frac{1}{2} \ln \left\{ \frac{\sigma_w^2 + \sigma_{Sx}^2}{\sigma_w^2} \right\} - \frac{\sigma_{Sx}^2}{2(\sigma_{Sx}^2 + \sigma_w^2)}. \tag{5.58}$$

5.3.9 Proposed algorithm for dual detection

As presented in Section 5.3.7, the computational complexity of GLR based spectrum sensing is much higher than other techniques. It is even higher than cyclo-stationary based spectrum sensing as can be seen from Table 5.1. As a matter of fact, the implementation presented in Section 5.3.7 was for the detection of the entrance of the PU's signal only, i.e., implementation of (5.27). However, as stated in [133], one should implement (5.27) for the detection of the entrance of the PU's signal and

(5.55) for the detection of empty spectrum slots. One can see that this will increase the computational complexity significantly. In order to address this issue, we design a dual detection algorithm for which we continue to use the same decision statistic for the detection of the entrance of PU's signal, but for the entrance of an empty spectrum slots. In other words, we use either (5.27) or (5.55) for both the detection of the PU's signal as well as detection of empty spectrum slot. For the detection of the PU's signal, (5.27) is used as is. And for the detection of empty spectrum slot, we estimate the slope of the decision statistic according to

$$S_{B_i} = \frac{B_{i+t_s} - B_i}{t_s}, \tag{5.59}$$

where t_s is the number of samples at which the slope is estimated. Hence, for the detection of empty of spectrum slots, we use

$$S_{B_i} < \varepsilon, \tag{5.60}$$

where $\varepsilon \approx 0$. We will show below how S_{B_i} is used for the detection of empty spectrum slot. One can see that by using this simple approach, we save significantly on computational complexity.

5.3.10 Results for likelihood ratio based spectrum sensing

We simulate the performance of the GLR FD algorithm presented above. We use the half duplex (HD) case presented in Section 5.3.4 as a baseline against which we compare the performance of the FD case. We start by plotting the decision statistic for the GLR algorithm and proceed to present the probability of detection versus the required number of samples at a fixed probability of false alarm. We then study the effect of uncertainty in the noise and residual self interference variance on the performance of the GLR FD algorithm. Typically, the requirement for an efficient spectrum sensing is to achieve $P_d \geq 90\%$, while $P_f \leq 10\%$. The results below are for a fixed $P_f = 10\%$, $\sigma^2_{\mathrm{S}x} = 0.5\sigma^2_x$ and $\sigma^2_{\mathrm{M}x} = 2\sigma^2_x$.

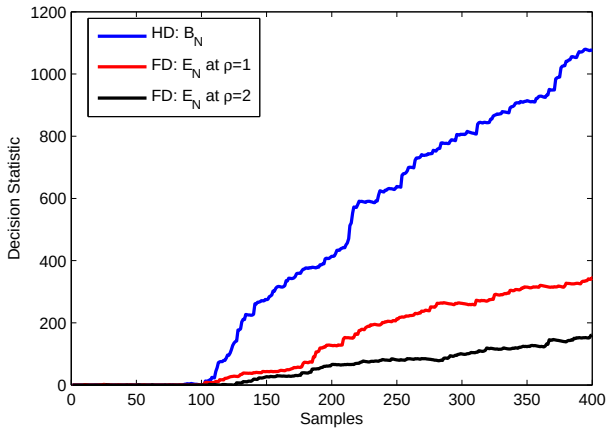

Fig. 5.2 Decision statistic for the HD case, FD at $\rho = 1$ and FD at $\rho = 2$. The PU enter the spectrum at the 100^{th} sample.

GLR decision statistic

We start by plotting the decision statistic for both HD and FD GLR algorithms in Fig. 5.2. The simulation is for 400 samples with the PU entering the spectrum at the 100^{th} sample. $\gamma_{HD} = 10$ dB and $\gamma_{zw} = 3$ dB. The FD GLR algorithm is simulated at $\rho = 1$, i.e., perfect knowledge of the variance of the noise and the residual self interference, and at $\rho = 2$. As a PU enters the spectrum, the decision statistic in the three cases starts to increase rapidly. However, the amplitude of the HD case is higher than the two FD cases, which indicates that once a threshold is set, detection of the PU signal will have a higher probability of detection at lower number of collected samples.

Probability of detection vs. number of samples

We numerically compute the probability of detection for HD GLR and FD GLR ($\rho = 1$ and $\rho = 2$) algorithms at a fixed probability of false alarm for different number of samples collected after the entrance of the PU signal. Fig. 5.3 shows the simulation results for P_d vs. number of samples, where γ_{zw} was fixed at 6 dB, while γ_{HD} changed from (a) 3 dB, to (b) 6 dB to (c) 10 dB. The same simulation parameters are used in Fig. 5.4, but for $\gamma_{HD} = 9$ dB and (a) $\gamma_{zw} = 9$ dB, (b) $\gamma_{zw} = 12$ dB and (c) $\gamma_{zw} = 15$ dB. It can be inferred from both figures that HD GLR algorithm performs better than FD GLR algorithm. This degradation in the performance of the FD GLR algorithm is due to the residual self interference. As γ_{HD} increases,

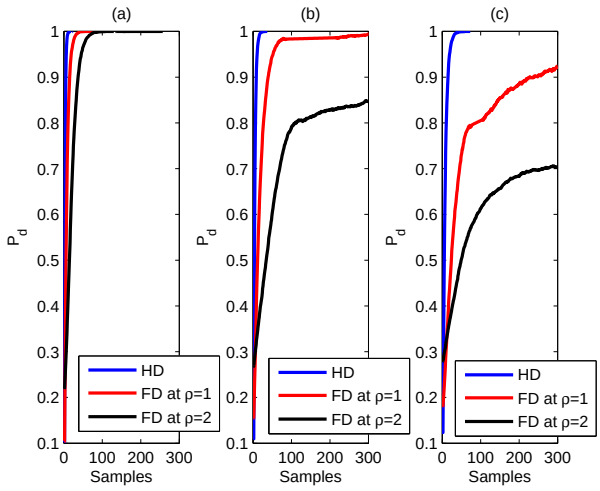

Fig. 5.3 Probability of detection vs. number of samples for $\gamma_{zw} = 6$ dB and (a) $\gamma_{HD} = 10$ dB, (b) $\gamma_{HD} = 6$ dB and (c) $\gamma_{HD} = 3$ dB.

lower number of samples are required to achieve the target $P_d \geq 90\%$. For example, for $\gamma_{zw} = 6$ dB and $\gamma_{HD} = 3$ dB, HD GLR requires approximately 10 samples, FD GLR at $\rho = 1$ requires approximately 275 samples, while FD GLR at $\rho = 2$ fails to achieve $P_d > 70\%$ for a preset number of collected samples of 300. Same notion is inferred as γ_{zw} decreases.

Uncertainty in the variance of the noise and residual self interference

We first introduce different levels of uncertainty and study its performance on the FD GLR algorithm. In Fig. 5.5, we plot P_d vs. ρ at (a) fixed γ_{zw} and different γ_{HD} and (b) fixed γ_{HD} and different γ_{zw}. Regardless of the level of γ_{zw} and γ_{HD}, the degradation in the performance of the FD GLR saturates at $\rho \geq 2$. We then use $\rho = 2$ in Fig. 5.6 to evaluate the boundaries, i.e., the SNR wall of the FD GLR algorithm. We plot P_d vs a large number of samples (1000) for (a) different levels of $(\gamma_{zw} - \gamma_{HD})$ and for (b) low γ_{HD} levels. If γ_{zw} is approximately 9 dB higher than γ_{HD}, or more, P_d saturates at 70%, no matter how many samples are collected. In addition, for $\gamma_{HD} \leq -9$ dB, P_d also saturates to 70%, no matter how low γ_{zw} gets.

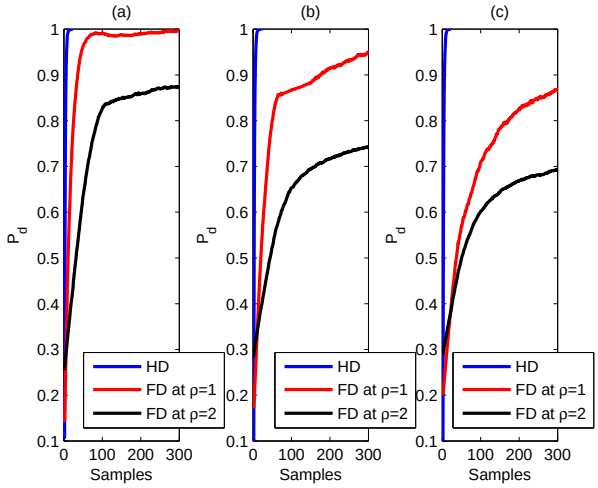

Fig. 5.4 Probability of detection vs. number of samples for $\gamma_{HD} = 9$ dB and (a) $\gamma_{zw} = 9$ dB, (b) $\gamma_{zw} = 12$ dB and (c) $\gamma_{zw} = 15$ dB.

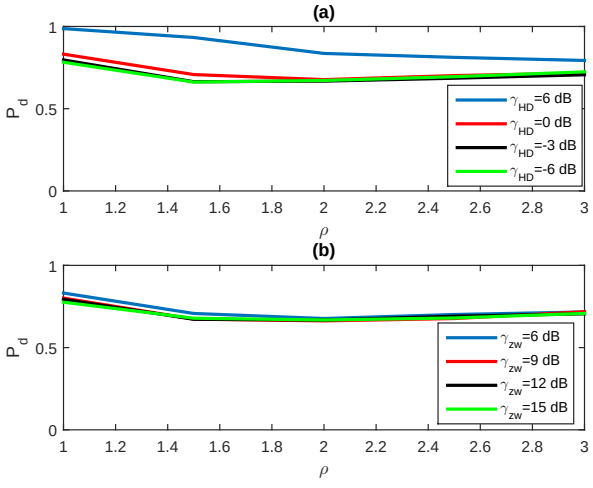

Fig. 5.5 Probability of detection vs. ρ using 250 samples (a) $\gamma_{zw} = 6$ dB and different γ_{HD}, (b) $\gamma_{HD} = 0$ dB and different γ_{zw}.

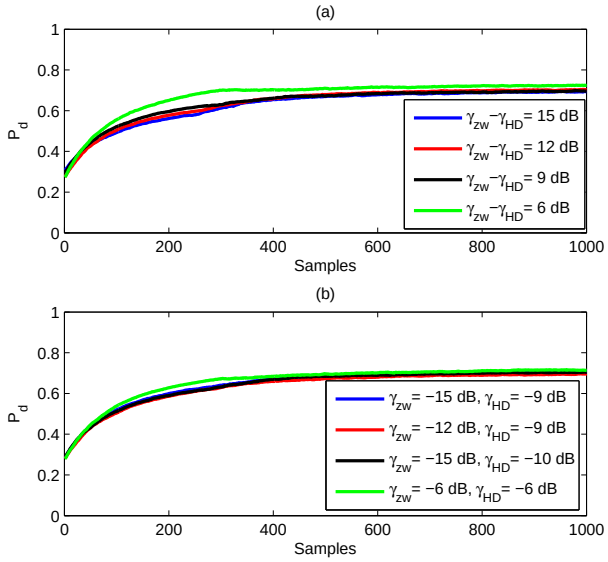

Fig. 5.6 Probability of detection vs. number of samples (a) different levels of $(\gamma_{zw} - \gamma_{HD})$ values (b) low γ_{HD} levels.

Dual detection algorithm

We first present how our slope based proposed decision statistic B_N behaves when used in the detection of empty spectrum slots in Fig. 5.7. The PU leaves the spectrum at the 300^{th} sample. As soon the PU leaves the spectrum, B_N starts to decline. Hence its slope takes a negative drift. In Fig. 5.8, we simulate S_B for (a) $t_s = 10$, (b) $t_s = 20$ and (c)$t_s = 30$ samples. As t_s increases, it becomes easier to detect the entrance of empty spectrum slots, however, it becomes harder to accurately detect the exact time at which this occurred. In Fig. 5.9, we plot P_d at SNR = 0 dB and $P_f = 1\%$ for (a) $t_s = 10$, (b) $t_s = 20$ and (c)$t_s = 30$ samples. As expected, as t_s increases, P_d improves.

5.4 Exploiting Spectrum Sensing Data for Security

Consider a radio cognitive network where the SUs sense the spectrum so as to detect empty spectrum slots that they can exploit for communication, i.e., the spectrum is already occupied by the PU's signal and the objective is to determine the gaps in the PUs communications. While communicating, SUs periodically sense the spectrum

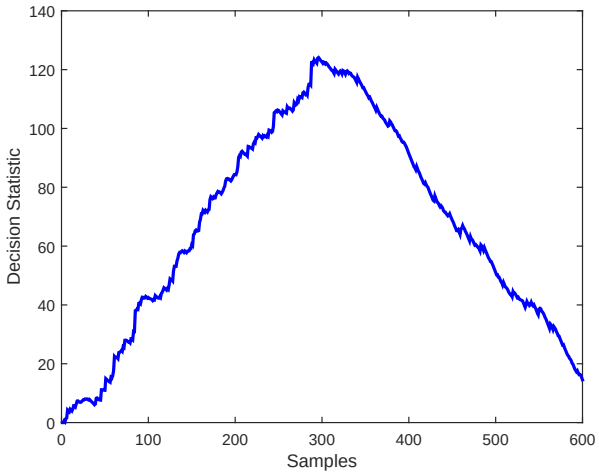

Fig. 5.7 B_N when used to detect empty spectrum slots at SNR = 3 dB. The PU leaves the spectrum at the 300^{th} sample.

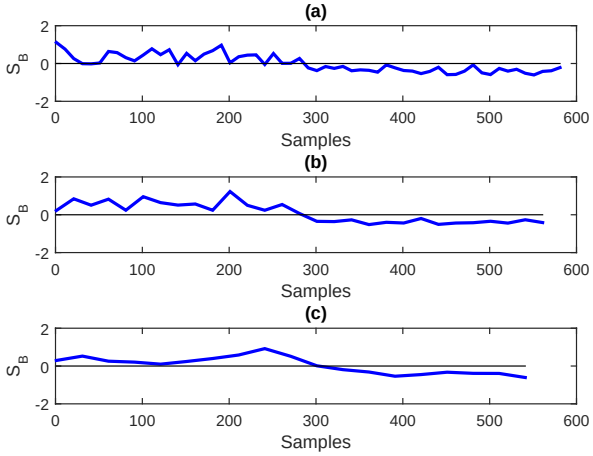

Fig. 5.8 S_B at SNR = 3 dB for (a) $t_s = 10$, (b) $t_s = 20$ and (c) $t_s = 30$ samples.)

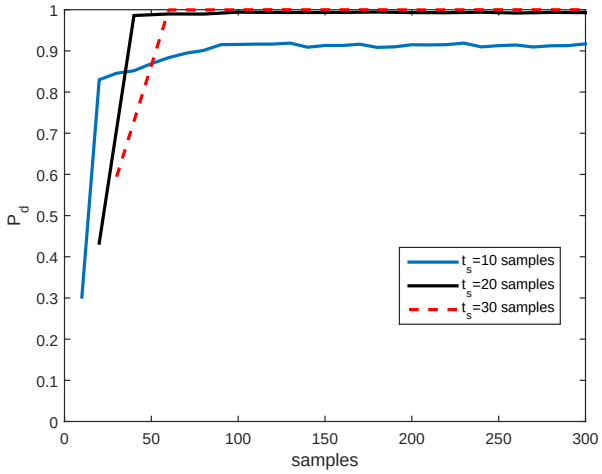

Fig. 5.9 P_d at $P_f = 1\%$ and SNR = 0 dB for (a) $t_s = 10$, (b) $t_s = 20$ and (c) $t_s = 30$ samples.)

in order to be able to detect the entrance of a PU and, in case, retreat from using the spectrum slot. The time intervals corresponding to the two operations are referred to as Phase I and Phase II, respectively, and they are depicted in Figure 5.10. A detection cycle is defined as the time period comprising the two phases. Note that the length of the detection cycle and of the two phases therein is not constant. Indeed, PUs exploit their assigned spectrum as desired and, therefore, the length of each phase may differ from one detection cycle to the next.

We assume that every N samples, each SU makes its own decision about the frequency slot status (empty/occupied) and sends it to the other SUs, in case of distributed collaborative sensing, or to the SU acting as fusion center. The first objective is to ensure that the decisions collected from all SUs, which will be used to produce the overall decision on the presence or absence of PUs, are validated and false samples generated by malicious nodes are discarded. To this end, decisions from legitimate SUs are encrypted with a *link* key only known to them. A decision maker can then easily decrypt the data and filter out information injected by malicious nodes. Similarly, in the presence of an empty spectrum slot, legitimate SUs encrypt their communication through a *link* key, so as to avoid eavesdropping by a malicious user.

A link key is generated by SUs at every detection cycle. In order to do that, we assume that an authorized network entity distributes a secret primary key to legitimate SUs prior to the spectrum sensing operation, using any of the conventional

cryptographic schemes presented in [143]. The primary key includes information that is essential to the algorithm we devise to generate the link key. Note that the primary key is also delivered to any legitimate SU that joins the network later on. A new primary key is instead distributed whenever its effect on the link key generation diffuses with time (e.g., every number of detection cycles), and whenever a legitimate SU leaves the network. The latter is necessary to secure the network against the scenario when a legitimate SU later becomes a malicious node.

Finally, our adversary model assumes that a malicious node can listen to the spectrum used by the PU and can use the same SS technique used by the legitimate SUs. In other words, the malicious node has access to the spectrum sensing data. The malicious node's intention is to launch an SSDF attack by transmitting false spectrum sensing data to the other SUs, or to the SU operating as fusion center. It can move freely within the field and can visit any of the locations where either the PU or the SUs were or will be. In the case of eavesdropping, the malicious node is assumed to be a passive adversary.

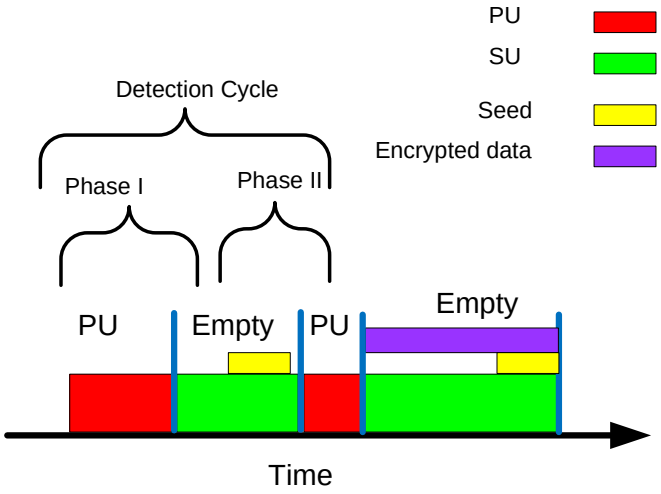

Fig. 5.10 Spectrum sensing and link key generation during each detection cycle.

5.4.1 Secret key generation algorithm

In our proposed link key management algorithm, we will use the estimated GLR decision statistic introduced before as a common seed for secret *link* key generation. We assume that all the legitimate SUs employ the same spectrum sensing algorithm, hence the decision statistic is already calculated at all the SUs. Below we first

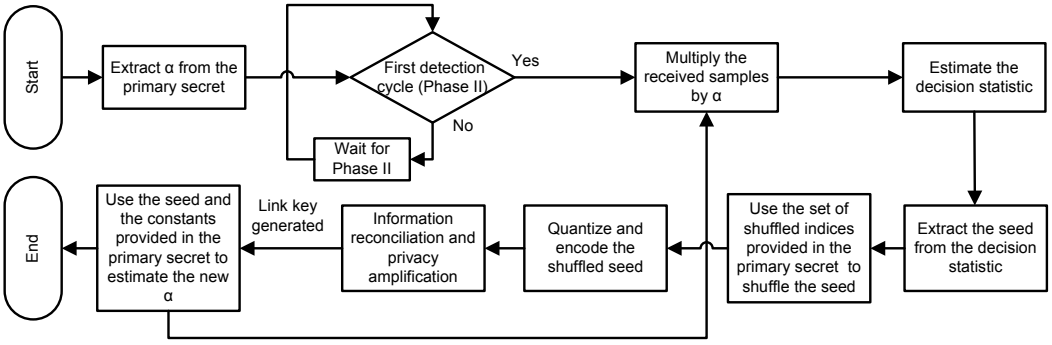

Fig. 5.11 Flow chart of the proposed algorithm.

provide an outline of our algorithm and then we detail the steps on how to generate the secret link key from the decision statistic.

Algorithm outline

The flow chart of our algorithm is presented in Figure 5.11. The algorithm is initialized at the first detection cycle, during Phase II. It is then repeated in Phase II of every cycle.

As mentioned, our technique consists of a primary key distribution and a link key generation algorithm. We assume that a primary secret key is pre-distributed to the legitimate nodes. Using the information provided in the primary pre-distributed key, our algorithm manipulates the samples collected by each legitimate SU during Phase II, i.e., when SUs are sampling white noise. Doing so, the estimated decision statistic at any two legitimate SUs will be very similar[1], providing a common seed. This manipulation process is performed by applying at the legitimate SUs a mathematical operation on the collected samples, which can be as simple as a multiplication, or more complex such as a nonlinear function. For simplicity, here we assume a multiplication by a constant α, which, in the first cycle, coincides with one of the pieces of information included in the primary secret key and is then updated in the following cycles. Based on such samples, the decision statistic in (5.27) is computed.

Next, N_s samples are sequentially picked from the estimated decision statistic and used as seed, $S = [s_1, \ldots, s_{N_s}]$. S is shuffled, quantized using N_q bits and encoded to

[1]The seed used for link key generation (explained later) is not exactly the same, but it is similar enough to act for link key generation. We will show that by plotting the bit mismatch rate between the generated links keys in Section 5.4.2.

generate a serial bit stream. An information reconciliation and privacy amplification is applied to the generated serial bit stream in order to generate the final *link* key. S is then used to generate the new α for the following detection cycle through a pseudo-random number generator [144].

Counteracting SSDF and eavesdropping

The *link* key generated in one detection cycle is used in the two phases of the following detection cycle. The aims are twofold.

1. To counteract SSDF: during Phase I of the following detection cycle, the SS decision statistic estimated through (5.55) is encrypted with the generated *link* key and transmitted to the fusion center. The fusion center being one of the legitimate SU or another node having access to the spectrum has also generated the *link* key. Hence, it decrypts the transmitted SS decision statistic sent from legitimate nodes and easily filters out data sent from malicious nodes.

2. To counteract eavesdropping: once availability of an empty spectrum slot is declared, legitimate SU start communicating. Data is encrypted using the generated *link* key available at the legitimate SUs. An eavesdropper, which does not have the key, will not be able to decrypt the transmitted data.

Primary key

As mentioned, the pre-distributed primary key is needed *only once* at the system set up, or after a number of detection cycles. This primary key is not the secret *link* key that will be used to encrypt the transmitted data. Rather, it contains some pieces of information that will be used in the process of generating the secret link key at two legitimate SUs. Specifically,

- the initial value of α;
- the set of the shuffled indices of the seed samples;
- the number of the compression function and universal hash function applied in the information reconciliation and privacy amplification step;

- the constants (β, γ and ρ) used in the process of generating the new value of α_n.

The number of quantization bits, N_q and the number of seed sample, N_S are fixed and given beforehand.

Seed generation

In Phase II, each legitimate SU listens to the spectrum and collects AWGN samples before the entrance of the PU's signal. The SU first multiplies the samples by the initial value of α that is provided in the primary secret key, thus obtaining $y_\alpha[i] = \alpha y[i]$. Accordingly, distributions F_0 and F_1 change into $\mathcal{N}(0, \alpha^2(\sigma_w^2 + \sigma_x^2))$ and $\mathcal{N}(0, \alpha^2\sigma_w^2)$, respectively. We denote by B_α the decision statistic in (5.27) when y_α is used as input instead of y. Also, in Phase II, legitimate SUs may use either B or B_α for signal detection; clearly, in the latter case, the threshold used for SS should be adjusted accordingly.

Once B_α is available, the seed (S) is given by the N_s samples of B_α estimated before the entrance of the PU's signal. We will show that this seed does not depend on the signal-to-noise ratio (SNR) at the legitimate SUs but it mainly depends on α. This implies that, regardless of the received SNR, the generated seed can be considered common to all legitimate SUs making it suitable for secret *link* key generation.

Link key generation

The generation of the secret link key at legitimate users consists of the following four steps.

1) Once estimated the common seed, its indices are shuffled according to a sequence that is provided in the primary key. The main purpose of shuffling is to increase the level of randomness of the seed.

2) Next, the shuffled seed has to be converted into a bit stream that is suitable as link key. To quantize the seed samples, we use uniform quantization [145]. The number of quantization bits, N_q, determines the number of quantization levels, $L = 2^{N_q}$. The quantized decimal value is then converted into bits.

3) Although uniform quantization is easy to implement, increasing the quantization bit number dramatically degrades the performance of the algorithm since the Bit Mismatch Rate (BMR) between two communicating SUs increases. To solve this problem, we adopt the technique presented in [45]. There the authors proposed an encoding algorithm and applied it on a uniformly quantized reciprocal link signatures. On link signatures exhibiting a BMR up to 84.48%, their encoding scheme could reduce the BMR to almost 4% thus leading to an excellent improvement.

4) The final step towards the link key generation is information reconciliation, where the two legitimate SUs use a protocol, such as the one in [46], to minimize the BMR between bit streams generated at two different SUs. In this protocol, public communication over the channel must occur to correct the mismatched bits. Consequently, some of the information will be leaked to the eavesdropper. Therefore, information reconciliation is usually followed by data compression and universal amplification where a universal compression function and a universal hash function is selected randomly from a saved set and applied to the bit streams at both the SUs [146]. The generated link key will then become shorter in length but higher in entropy. In our algorithm, the number of the compression function as well as the hash function is provided in the *primary* secret. It is worth noting that for the information reconciliation step to be applied efficiently, the BMR after the encoding step should not exceed a certain value, namely, 15% [146]. After this step, the link key is generated and ready to be used to encrypt the transmitted data in the next cycle.

At last, SUs have to compute a new value of α to be used in the next detection cycle. To this end, the following operation is applied to the estimated seed:

$$S_{LGN} = \ln \mathbb{E}[S]. \tag{5.61}$$

S_{LGN} is the input to the Linear Congruential Generator (LGN) – a pseudo random number generator [144] requiring constants β, γ and ρ to compute the new value of α as:

$$\alpha = (\beta S_{LGN} + \gamma) \, mod(\rho). \tag{5.62}$$

where *mod* is the modulo operator. The constants β, γ and ρ are included in the primary secret.

We will use the root mean square error (RMSE) as the metric to evaluate the drift in computing α between two legitimate SUs, i.e., $RMSE = \sqrt{\mathbb{E}\left[(\alpha|_{SU_1} - \alpha|_{SU_2})^2\right]}$.

5.4.2 Results

We present the simulation results for our proposed key management algorithm. We show the effect of multiplying the received samples by α on the estimated decision statistic in Phase II. An example of shuffled seed is then illustrated. The effect of change in SNR and α on the BMR of the generated *link* key is then presented. We compare the bit mismatch and entropy rates of the key generated through our algorithm to conventional channel based algorithm. In addition, we depict how the value of α changes with different detection cycles.

Impact of α on seed generation

We start by presenting the impact of α on seed generation. Figure 5.12 shows the simulation results obtained for B_α at the legitimate SUs, when $\alpha = 2.5$ (top) and 5 (bottom), respectively. In both subfigures, the SNR is set to 15 dB at the first legitimate SU, to 10 dB at the second, and 10 dB at the malicious node. Since the malicious node does not know the value of α, it is assumed that it uses $\alpha = 1$. Although, the malicious node uses the same spectrum sensing technique, its decision statistic before the entrance of the PU's signal is almost zero making it unsuitable for secret key generation. The change in SNR between the two legitimate SUs leads to different values of B_α after the entrance of the PU's signal, exhibiting higher values as the SNR increases. Nevertheless, the seed S, which is zoomed-in in both subfigures, is not affected by the different values of SNR, since it is generated from the samples collected before the entrance of the PU's signal. Rather, it is affected only by the value of α. As α grows, the drift in the first 200 samples of B increases. Moreover, S at both legitimate SUs is very similar. The samples used as seed at the malicious node are close to zero, making them unsuitable for link key generation. Furthermore, one can see that B_α can be used also to detect the entrance of the PU's signal instead of B, by properly adjusting the value of the threshold to account for the effect of α.

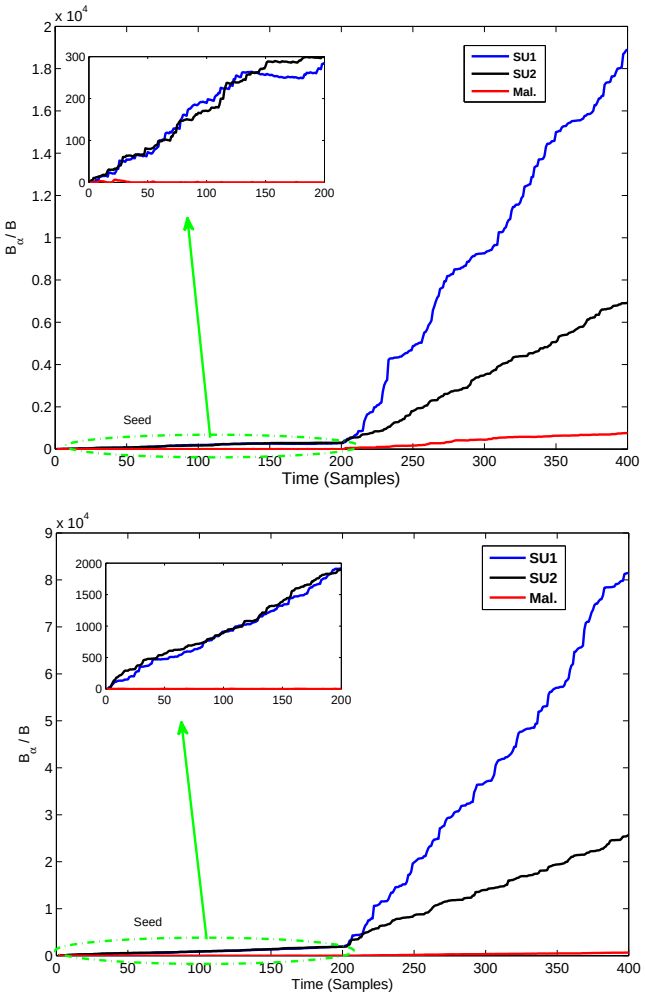

Fig. 5.12 B_α for $\alpha = 2.5$ (top) and $\alpha = 5$ (bottom) at two legitimate SUs, and B at the malicious user. B_α and B are plotted as functions of time (400 samples, the seed is zoomed in).

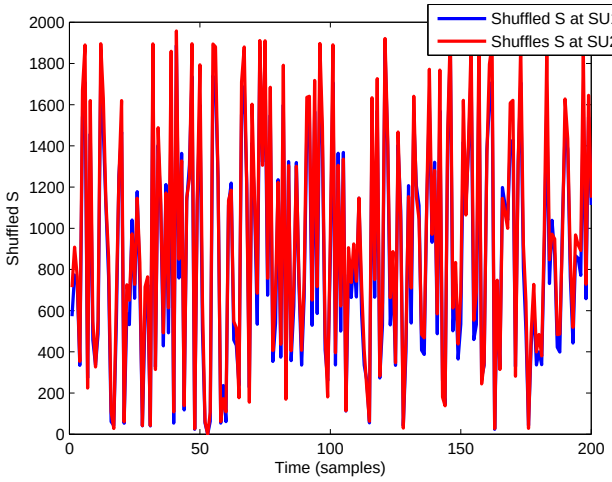

Fig. 5.13 Shuffled S at the two legitimate SUs.

Seed shuffling

In Figure 5.13, we present a shuffled version of the samples of S. The shuffled indices set is provided in the *primary* secret to the legitimate SUs. One can see that S does not follow the continuously increasing pattern anymore. Rather, it is completely randomized.

BMR

Next, Figure 5.14 shows the simulation results for the BMR of the link key extracted at two legitimate SUs vs. the difference in SNR between the SUs. The SNR at SU1 varies between 0 and 20 dB, while the SNR at SU2 is fixed at 10 dB. We set $\alpha = 10$ and use different numbers of quantization bits, namely, $N_q = 4, 6$ and 8. We compare the results of our proposed algorithm to conventional channel based secret key generation algorithm [147]. Each BMR value is estimated through extensive Monte Carlo simulation using 10,000 iterations. The results clearly show that the change in SNR between the two SUs does not affect the performance of our link key generation algorithm. As expected, as N_q increases, the BMR increases, however, the achieved BMR after encoding is less than 10%. The achieved BMR before information reconciliation and privacy amplification is well below the value provided in [146] of 15%, thus leading to very good performance. The BMR achieved through our algorithm shows comparable results to channel based physical layer security

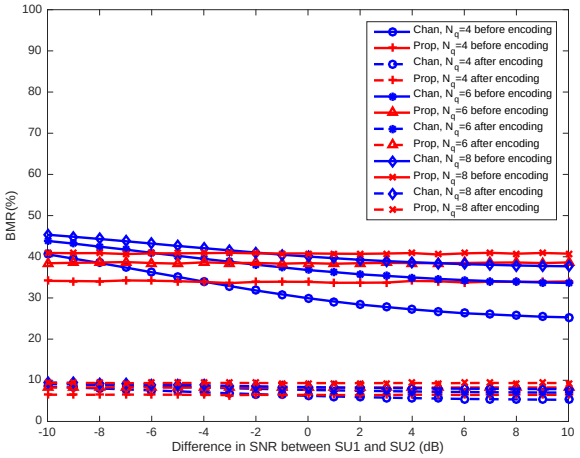

Fig. 5.14 BMR vs. the difference in SNR between the two legitimate SUs, for different numbers of quantization bits.

scheme. However, unlike our proposed algorithm, the effect of change in SNR is clear in channel based key generation algorithm. Furthermore, it is important to stress that changing the value of α does not have much effect on the achieved BMR. BMR results presented in Figure 5.15 highlight that the achieved BMR for α varying between 5 and 30 is almost constant and equal to 44% before encoding, and to 11% after encoding.

Entropy

Entropy is a measure of the level of randomness of the generated key. We compare the entropy of the link key generated through our algorithm to channel based algorithm [147] in Fig. 5.16 for $N_q = 6$ bits. The entropy rate achieved through our proposed algorithm is comparable to that achieved by conventional channel based technique.

α vs. number of detection cycles

The way α evolves over time is depicted in Figure 5.17 (top), for $\alpha = 2$, $\beta = 18$, $\gamma = 5$, $\rho = 200$ and the SNRs at the two legitimate equal to 15 dB and 10 dB, respectively. One can see that using the LGN makes the estimated α to fluctuate randomly, which is exactly what we want in order to generate efficient link keys.

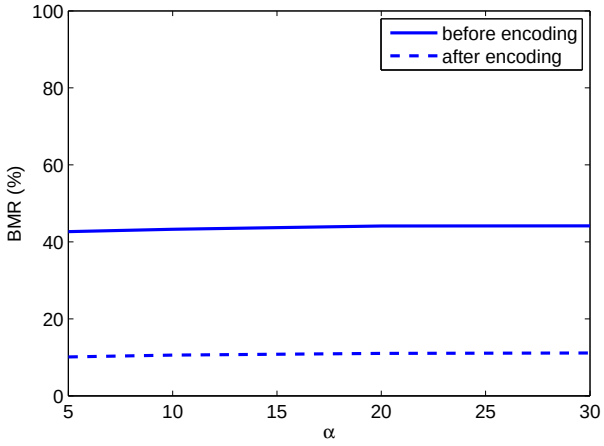

Fig. 5.15 The BMR vs. α before and after encoding for our proposed algorithm and channel based algorithm.

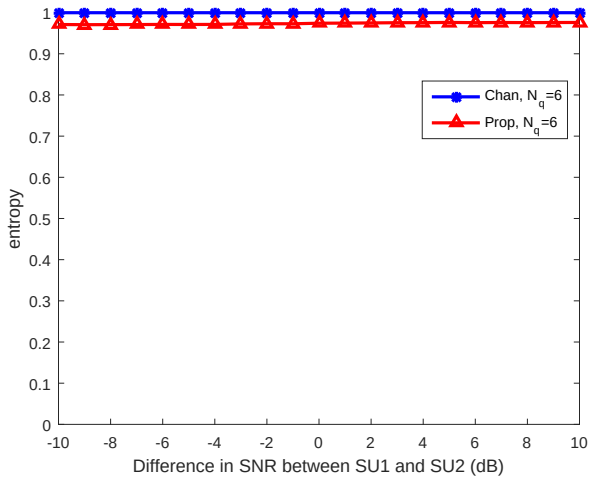

Fig. 5.16 Entropy rate of the generated key for our proposed algorithm and channel based algorithm.

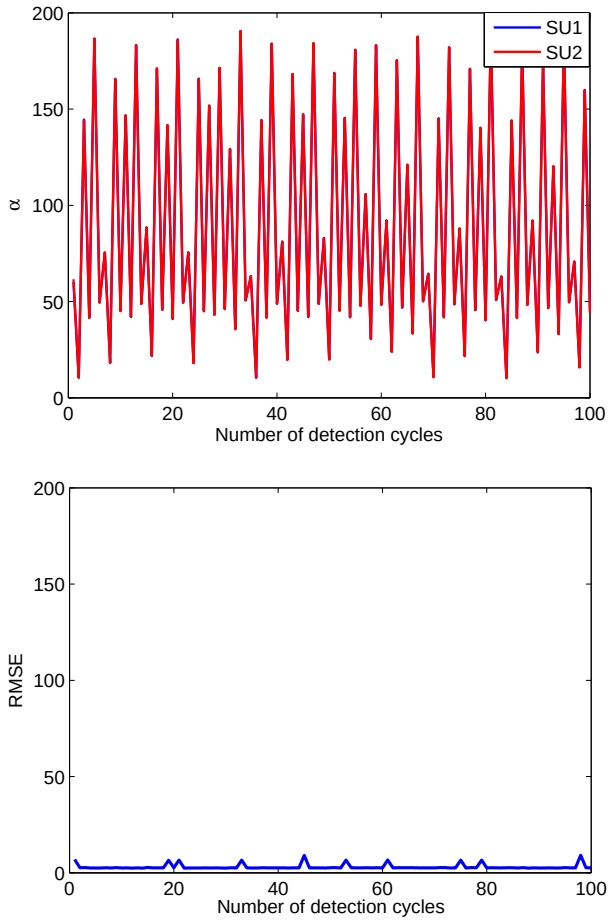

Fig. 5.17 α_n at the two legitimate SUs as a function of the number of detection cycles (top). RMSE of the estimated α_n at the two legitimate SUs (bottom).

Also, the results in Figure 5.17 (bottom) (obtained under the same settings) confirm that the RMSE of α is very low.

How often should the primary key be distributed?

As stated earlier, a new primary key may need to be distributed when its effect on the link key generation, through the parameter α, tends to dissolve. Then a reasonable concern is about when a new primary key should be generated. Figure 5.18 depicts the estimated α versus the number of detection cycles, for initial $\alpha = 2$, $\beta = 8$, $\gamma = 5$ and $\rho = 200$ (top) and $\alpha = 2$, $\beta = 30$, $\gamma = 10$ and $\rho = 200$ (bottom). From Figure 5.17 (top) and Figure 5.18, it can be inferred that the periodicity and randomness of

the newly generated α depends on the selection of the parameters[2] β, γ, ρ and initial α. Therefore, a new primary key is distributed whenever the value of α follows a periodic pattern or does not fluctuate randomly from one detection cycle to the next as desired.

A qualitative comparison

To counteract SSDF, reputation based techniques such as the ones presented in [14, 148] require long time, i.e., many detection cycles, to build up a good reputation. In addition, reputation is built based on the overall decision, which may be incorrect in case of SSDF attacks launched by many malicious nodes. Non-reputation based techniques such as [149–151], are also based on the assumption that the overall decision is correct. On the other hand, our algorithm neither requires many detection cycles to efficiently operate, nor it assumes the correctness of the overall decision.

Typical physical layer security techniques, such as [19], used to counteract eavesdropping require extensive channel probing to generate a suitable link key. The frequent channel probing requires multiple beacon exchange, synchronization and employment of a channel estimation technique. In addition, they may need an initial agreement on some parameters [19] as in our proposed technique. On the contrary, our solution exploits the spectrum sensing data, which is already available at the two legitimate nodes to extract the link key to make key exchange less frequent. Thus, our algorithm requires a shorter time to generate the link key as well as much lower computational complexity stemming from not deploying channel estimation techniques.

5.5 Conclusion

In this chapter, we first presented literature reviews on spectrum sensing techniques as well as security in cognitive radio networks. We conducted performance analysis of likelihood ratio based spectrum sensing. Furthermore, we studied its performance under residual self interference in full duplex CRN. We implemented general likelihood ratio based spectrum sensing on WARP platform and compared its resource utilization to both cyclo-stationary based as well energy detection spectrum sensing

[2]Refer to [144] for more details on the selection and limitations of the LGN parameters.

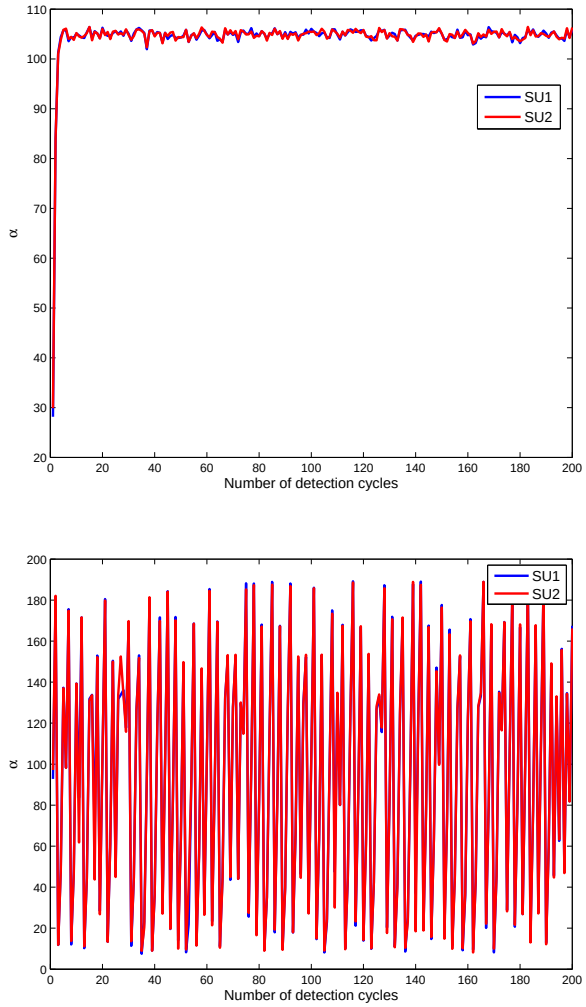

Fig. 5.18 α_n at the two legitimate SUs as a function of the number of detection cycles: for initial $\alpha = 2$, $\beta = 8$, $\gamma = 5$ and $\rho = 200$ (top) and $\beta = 30$, $\gamma = 10$ and $\rho = 200$ (bottom).

techniques. We then proposed a general likelihood ratio based techniques that can operate for both detection of the entrance of primary users and empty spectrum slots. Hence, reducing the computational complexity.

We then explored a novel idea of exploiting general likelihood ratio based spectrum sensing collected data for secret key generation. Our presented algorithm is designed to counteract two popular attacks on cognitive radio networks, which are spectrum sensing data falsification and eavesdropping. We presented all steps needed to extract the secret key from the collected data. Our algorithm is designed such that it does not interrupt the spectrum sensing operation. Furthermore, no beacon exchange is needed in our algorithm. Hence, increasing spectrum usage efficiency.

Chapter 6

Conclusion and Future Work

Conventional cryptographic techniques depend on distribution of shared secret key, which requires a complex key management scheme in the case of symmetric ciphers and high computational complexity in the case of asymmetric ciphers, particularly in large networks due to scalability issues. In addition, due to the broadcast nature of the wireless network, key exchange becomes a security threat. Hence, key reuse was introduced.

In the recent years, exploiting characteristics of the physical layer between the two communicating nodes was proposed for secret key generation. Such characteristics are common between the two legitimate nodes and unknown to unintended nodes, i.e., eavesdroppers. By exploiting common physical layer characteristics, key exchange is no longer required and a new secret key can be possibly generated for every packet transmission rendering the secrecy potential higher than upper layers cryptographic methods while maintaining lower computational complexity. In addition, key management center is no longer required.

The most widely used physical layer characteristic for secret key generation is the wireless channel. One well known characteristic of the communication channel is reciprocity. When two antennas communicate by radiating the same signal through a linear and isotropic channel, the received signals by each antenna will be identical.

In chapter two, we first presented a survey on common physical layer characteristics used for secret key generation. In addition, we presented the common steps used to extract the secret key from the common physical layer characteristic. We investigated both statistical and information theoretic metrics used to evaluate the

generated secret key. As a conclusion to the literature survey, we found out that high key generation rate is one main advantage of exploiting channel randomness for secret key generation. On the other hand, a major drawback is that additive white Gaussian noise, interference and channel estimation errors at the receivers of both legitimate nodes cause a high bit mismatch rate between the keys generated at the two nodes, which limits the use of secret key generation based on channel estimates to medium and high level of signal to noise ratios. This motivated the need for developing novel techniques that overcome such shortcoming.

In chapter three, we proposed a novel algorithm that exploits both channel gain and phase to create secondary random processes, which are then used to extract the secret key. We investigated the distribution of the secondary random process. Furthermore, we computed the probabilities used for secret key capacity estimation. Our proposed algorithm reduced the bit mismatch rate by up to 25%. On the other hand, our proposed algorithm slightly reduced the entropy of the generated secret key. This issue was overcome by fusing both channel gain and phase secret key bits. Not only the fusion process increased the entropy of the generated secret key, but also increased the generated key length as well as reduced the overall bit mismatch rate since we dropped the least significant bits before the fusion process. The least significant bits are known to highly contribute to the bit mismatch. In addition, our proposed secondary random process based secret key generation algorithm is easy to implement.

Although our channel secondary random process presented in chapter three improved the bit mismatch rate, i.e., increased the dynamic range of the system, channel based secret key generation algorithms are still limited to signal to noise ratio levels higher than 0 dB. For certain applications, the operational range will be lower than 0 dB. Hence, it was essential to introduce a new physical layer characteristic that can be estimated with high accuracy at low signal to noise ratio levels. Therefore, in chapter four we investigated exploiting the angle of arrival as a common source of randomness for secret key generation. One obstacle that we met was that angle of arrival estimation systems have high implementation and computation complexities. This motivated our work on developing a novel angle of arrival estimation system that has low hardware and computation complexities yet can operate with acceptable accuracy at low signal to noise ratio levels. We designed our cross correlation switched beam system that has comparable performance to one of the best literature

angle of arrival estimation algorithm, yet uses a single receiver and has negligible computation complexity.

On the other hand, cognitive radio networks are designed to increase the efficiency of spectrum usage by exploiting unused spectrum slots. Secondary users sense the spectrum to detect transmission opportunities, i.e., spectrum slots that are not used by primary users. Similar to other networks, cognitive radio networks are susceptible to security attacks such as spectrum sensing data falsification and eavesdropping. However, due to the peculiarity of cognitive radio networks, conventional physical layer security schemes are not typically applied. This is due to the beacon exchange process, which requires time that is not acceptable from the perspective of a secondary user who wants to tap into the spectrum slot as soon as it is available. Therefore, we first conducted a performance analysis on general likelihood ratio based as well as developed a new technique that can be used in detection of empty spectrum slots as well as PU entrance. We then developed an algorithm that exploits spectrum sensing data already collected by secondary user to generate a link key. The link key is then used to encrypt the transmitted data. Our developed algorithm neither interrupts the spectrum sensing process nor requires additional time for beacon exchange, hence suitable for cognitive radio networks.

6.1 Roadmap to the Future

Hybridization for key generation

As mentioned earlier, nodes can always benefit from estimating multiple common sources of randomness simultaneously. As shown earlier in the case of using both channel gain and phase to generate the secret key. The problem of combining multiple common sources of randomness whether as raw data or bit streams remains an open research direction. Different hybridization (i.e., combining) functions can be applied on the multiple common sources of randomness with the objective of minimizing the bit mismatch rate and maximizing the key entropy. In addition to that, exploiting multiple common sources of randomness adds an extra degree of freedom to the legitimate nodes since the function, which they will apply on the common sources of randomness will be hidden from the eavesdropper.

Towards convergence of physical layer and cryptographic secrecy

Till date, the two worlds of physical layer secrecy and cryptographic secrecy speaks two different languages. While the former can only measure a non–vanishing secrecy capacity under the assumptions of infinitely long keys without any key reuse and assuming an infinite computation capabilities for the eavesdropper, the latter measures secrecy under finite computational capabilities of the eavesdropper, finite key lengths and mandatory key reuse. It would be highly desirable to find a way to converge the two worlds in order to allow for practical comparisons between conventional cryptographic methods and relatively recent physical layer secrecy based methods. There is a potential to move the information theoretic measures of the physical layer based methods towards more practical measures using some approximate representations of secrecy capacity under certain allowable probabilities of key breaking by the eavesdropper providing promising results towards arriving at common secrecy measures that can be used by the two worlds.

Secret key generation in static environment

For channel based secret key generation techniques, static environments cause key generation rate to drop significantly. This issue remains a challenging issue within the context of secret key generation. Random beamforming was proposed as a solution to this issue. However, this requires the employment of smart antenna system, which increases the hardware complexity of significantly. Therefore, it is of great interest to develop new techniques for channel based secret key generation and/or exploit new physical layer characteristics to overcome the issue of static environments.

Exploiting full duplex communication for key generation

The vast majority of existing secret key generation algorithm assume half duplex communication. Recently, research in full duplex communication has attracted a significant interest from the research community. One main advantage of generating a secret key using full duplex radios is that beacon exchange between the two communication nodes during the coherence time of the channel can occur simultaneously. Hence, increasing the secret key rate. In addition, the collected signal at the eavesdropper side is a superposition of the two exchanged signals, which may enhance security. More work is needed in this area to model and analyze effect of full duplex communication for secret key generation.

Secret key generation in 5G

Millimeter wave communication, massive multiple input multiple outputs (MIMO) communication and high mobility are integral parts of 5G standard. From the perspective of secret key generation, these can be thought of as both challenges and opportunities. One main advantage of millimeter wave communication is that signal fades a lot faster with distance than low frequency signals. Hence, an eavesdropper may receive deteriorated version of the signal, which shall enhance security. Higher key generation rate is expected with massive MIMO systems.

Security in cognitive radio networks

Due to the peculiarity of cognitive radio networks, conventional cryptographic and physical layer security schemes may not be suitable for it. We presented a novel algorithm that exploits the already collected general likelihood ratio based spectrum sensing data for secret key generation. It is essential develop more techniques to exploit spectrum sensing data collected through different spectrum sensing techniques and/or exploit other common sources of randomness that are shared between legitimate secondary users.

References

[1] A. Mukherjee, S.A.A. Fakoorian, Jing Huang, and A.L. Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. *Communications Surveys Tutorials, IEEE*, 16(3):1550–1573, Third 2014.

[2] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[3] R. Wilson, D. Tse, and R.A. Scholtz. Channel identification: Secret sharing using reciprocity in ultrawideband channels. *Information Forensics and Security, IEEE Transactions on*, 2(3):364–375, 2007.

[4] Akito Kitaura, H. Iwai, and H. Sasaoka. A scheme of secret key agreement based on received signal strength variation by antenna switching in land mobile radio. In *Advanced Communication Technology, The 9th International Conference on*, volume 3, pages 1763–1767, Feb 2007.

[5] O. Gungor, F. Chen, and C.E. Koksal. Secret key generation via localization and mobility. *Vehicular Technology, IEEE Transactions on*, PP(99):1–1, 2014.

[6] N. Patwari, J. Croft, S. Jana, and S.K. Kasera. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *Mobile Computing, IEEE Transactions on*, 9(1):17–30, 2010.

[7] Kai Zeng. Physical layer key generation in wireless networks: challenges and opportunities. *Communications Magazine, IEEE*, 53(6):33–39, June 2015.

[8] Simon Haykin. Cognitive radio: brain-empowered wireless communications. *Selected Areas in Communications, IEEE Journal on*, 23(2):201–220, 2005.

[9] G. Baldini, T. Sturman, A.R. Biswas, R. Leschhorn, G. Godor, and M. Street. Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead. *Communications Surveys Tutorials, IEEE*, 14(2):355–379, 2012.

[10] Zhihui Shu, Yi Qian, and Song Ci. On physical layer security for cognitive radio networks. *Network, IEEE*, 27(3):28–33, 2013.

[11] A.G. Fragkiadakis, E.Z. Tragos, and I.G. Askoxylakis. A survey on security threats and detection techniques in cognitive radio networks. *Communications Surveys Tutorials, IEEE*, 15(1):428–445, 2013.

[12] A. Ghasemi and E.S. Sousa. Collaborative spectrum sensing for opportunistic access in fading environments. In *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, pages 131 –136, nov. 2005.

[13] Zhi Quan, Shuguang Cui, H. Poor, and A. Sayed. Collaborative wideband sensing for cognitive radios. *Signal Processing Magazine, IEEE*, 25(6):60 –73, november 2008.

[14] Ruiliang Chen, Jung-Min Park, Y.T. Hou, and J.H. Reed. Toward secure distributed spectrum sensing in cognitive radio networks. *Communications Magazine, IEEE*, 46(4):50–55, 2008.

[15] C.R.C. da Silva, B. Choi, and Kyouwoong Kim. Distributed spectrum sensing for cognitive radio systems. In *Information Theory and Applications Workshop, 2007*, pages 120–123, 2007.

[16] Ahmed Badawy, Tarek Elfouly, Tamer Khattab, Amr Mohamed, and Mohsen Guizani. Unleashing the secure potential of the wireless physical layer: Secret key generation methods. *Physical Communication*, 19:1 – 10, 2016.

[17] Constantine A Balanis. *Antenna theory: analysis and design*. John Wiley & Sons, 2012.

[18] G.S. Smith. A direct derivation of a single-antenna reciprocity relation for the time domain. *Antennas and Propagation, IEEE Transactions on*, 52(6):1568–1577, 2004.

[19] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, MobiCom '08, pages 128–139, 2008.

[20] Zang Li, Wenyuan Xu, Rob Miller, and Wade Trappe. Securing wireless systems via lower layer enforcements. In *Proceedings of the 5th ACM Workshop on Wireless Security*, WiSe '06, pages 33–42, 2006.

[21] J. Wallace. Secure physical layer key generation schemes: Performance and information theoretic limits. In *2009 IEEE International Conference on Communications*, pages 1–5, June 2009.

[22] X. Sun, W. Xu, M. Jiang, and C. Zhao. Improved generation efficiency for key extracting from wireless channels. In *2011 IEEE International Conference on Communications (ICC)*, pages 1–6, June 2011.

[23] D. Qin and Z. Ding. Exploiting multi-antenna non-reciprocal channels for shared secret key generation. *IEEE Transactions on Information Forensics and Security*, 11(12):2693–2705, Dec 2016.

[24] C. Y. Wu, P. C. Lan, P. C. Yeh, C. H. Lee, and C. M. Cheng. Practical physical layer security schemes for mimo-ofdm systems using precoding matrix indices. *IEEE Journal on Selected Areas in Communications*, 31(9):1687–1700, September 2013.

[25] S. Im, H. Jeon, J. Choi, and J. Ha. Secret key agreement with large antenna arrays under the pilot contamination attack. *IEEE Transactions on Wireless Communications*, 14(12):6579–6594, Dec 2015.

[26] H. Zhou, L. M. Huie, and L. Lai. Secret key generation in the two-way relay channel with active attackers. *IEEE Transactions on Information Forensics and Security*, 9(3):476–488, March 2014.

[27] K. Chen, B. B. Natarajan, and S. Shattil. Secret key generation rate with power allocation in relay-based lte-a networks. *IEEE Transactions on Information Forensics and Security*, 10(11):2424–2434, Nov 2015.

[28] C. D. T. Thai, J. Lee, and T. Q. S. Quek. Physical-layer secret key generation with colluding untrusted relays. *IEEE Transactions on Wireless Communications*, 15(2):1517–1530, Feb 2016.

[29] Amer A. Hassan, Wayne E. Stark, John E. Hershey, and Sandeep Chennakeshu. Cryptographic key agreement for mobile radio. *Digital Signal Processing*, 6(4):207 – 212, 1996.

[30] H. Koorapaty, A. Hassan, and S. Chennakeshu. Secure information transmission for mobile radio. In *Information Theory, 1998. Proceedings. 1998 IEEE International Symposium on*, pages 381–, Aug 1998.

[31] Qian Wang, Kaihe Xu, and Kui Ren. Cooperative secret key generation from phase estimation in narrowband fading channels. *Selected Areas in Communications, IEEE Journal on*, 30(9):1666–1674, October 2012.

[32] Q. Wang, H. Su, K. Ren, and K. Kim. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In *INFOCOM, 2011 Proceedings IEEE*, pages 1422–1430, April 2011.

[33] Y. El Hajj Shehadeh, O. Alfandi, and D. Hogrefe. Towards robust key extraction from multipath wireless channels. *Journal of Communications and Networks*, 14(4):385–395, Aug 2012.

[34] Sriram Nandha Premnath, Suman Jana, Jessica Croft, Prarthana Lakshmane Gowda, Mike Clark, Sneha Kumar Kasera, Neal Patwari, and Srikanth V. Krishnamurthy. Secret key extraction from wireless signal strength in real environments. *Mobile Computing, IEEE Transactions on*, 12(5):917–930, 2013.

[35] Kai Zeng, Daniel Wu, An Chan, and Prasant Mohapatra. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In *Proceedings of the 29th Conference on Information Communications*, INFOCOM'10, pages 1837–1845, Piscataway, NJ, USA, 2010. IEEE Press.

[36] R. Guillaume, F. Winzer, A. Czylwik, C. T. Zenger, and C. Paar. Bringing phy-based key generation into the field: An evaluation for practical scenarios. In *Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd*, pages 1–5, Sept 2015.

[37] S. T. Ali, V. Sivaraman, and D. Ostry. Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices. *IEEE Transactions on Mobile Computing*, 13(12):2763–2776, Dec 2014.

[38] H. Liu, J. Yang, Y. Wang, Y. J. Chen, and C. E. Koksal. Group secret key generation via received signal strength: Protocols, achievable rates, and implementation. *IEEE Transactions on Mobile Computing*, 13(12):2820–2835, Dec 2014.

[39] M. Wilhelm, I. Martinovic, and J. B. Schmitt. Secure key generation in sensor networks based on frequency-selective channels. *IEEE Journal on Selected Areas in Communications*, 31(9):1779–1790, September 2013.

[40] Kui Ren, Hai Su, and Qian Wang. Secret key generation exploiting channel characteristics in wireless communications. *Wireless Communications, IEEE*, 18(4):6–12, August 2011.

[41] Neal Patwari and Alfred O. Hero, III. Using proximity and quantized rss for sensor localization in wireless networks. In *Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications*, WSNA '03, pages 20–29, 2003.

[42] Suman Jana, Sriram Nandha Premnath, Mike Clark, Sneha K. Kasera, Neal Patwari, and Srikanth V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, MobiCom '09, pages 321–332, 2009.

[43] Hongbo Liu, Jie Yang, Yan Wang, and Yingying Chen. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In *INFOCOM, 2012 Proceedings IEEE*, pages 927–935, March 2012.

[44] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. *Antennas and Propagation, IEEE Transactions on*, 53(11):3776–3784, Nov 2005.

[45] J. Zhang, S.K. Kasera, and N. Patwari. Mobility assisted secret key generation using wireless link signatures. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–5, 2010.

[46] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. pages 410–423. Springer-Verlag, 1994.

[47] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin. Wireless information-theoretic security. *Information Theory, IEEE Transactions on*, 54(6):2515–2534, June 2008.

[48] Yanpei Liu, S.C. Draper, and A.M. Sayeed. Exploiting channel diversity in secret key generation from multipath fading randomness. *Information Forensics and Security, IEEE Transactions on*, 7(5):1484–1497, Oct 2012.

[49] Chan Dai Truyen Thai, Jemin Lee, Chi Cheng, and T.Q.S. Quek. Physical-layer secret key generation with untrusted relays. In *Globecom Workshops (GC Wkshps), 2014*, pages 1385–1390, Dec 2014.

[50] U.M. Maurer. Secret key agreement by public discussion from common information. *Information Theory, IEEE Transactions on*, 39(3):733–742, 1993.

[51] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 5th edition, 2001.

[52] Nist: Computer security resource center.

[53] Nist - csrs: Public key interoperability test suite certification path validation.

[54] Ahmed Badawy, Tamer Khattab, Tarek M. Elfouly, Carla-Fabiana Chiasserini, Amr Mohamed, and Daniele Trinchero. Channel secondary random process for robust secret key generation. In *IWCMC 2015 Security Symposium (IWCMC 2015 Security Symposium)*, Dubrovnik, Croatia, August 2015.

[55] Ahmed Badawy, Tarek Elfouly, Tamer Khattab, Carla-Fabiana Chiasserini, Amr Mohamed, and Daniele Trinchero. Robust secret key extraction from channel secondary random process. *Wireless Communications and Mobile Computing*, 16(11):1389–1400, 2016. wcm.2695.

[56] Steven M. Kay. *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1993.

[57] Endre Süli and David F. Mayers. *An Introduction to Numerical Analysis*. Cambridge University Press, 2003. Cambridge Books Online.

[58] Jessica Erin, Dudley Croft, Erin Dudley Croft, Sneha K. Kasera, Rong rong Chen, Cynthia Furse, and John Regehr. Shared secret key establishment using wireless channel measurements, 2011.

[59] Christian Cachin and Ueli M. Maurer. Linking information reconciliation and privacy amplification. *Journal of Cryptology*, 10(2):97–110.

[60] A. Badawy, T. Khattab, T. Elfouly, D. Mohamed, A. Trinchero, and C. Chiasserini. Secret key generation based on aoa estimation for low snr conditions. In *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st*, pages 1–7, May 2015.

[61] A. Badawy, T. Khattab, T. Elfouly, A. Mohamed, and D. Trinchero. Secret key generation based on channel and distance measurements. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2014 6th International Congress on*, pages 136–142, Oct 2014.

[62] Warp project.

[63] B. Liao, Z.G. Zhang, and S.C. Chan. A new robust kalman filter-based subspace tracking algorithm in an impulsive noise environment. *Circuits and Systems II: Express Briefs, IEEE Transactions on*, 57(9):740–744, Sept 2010.

[64] T. Engin Tuncer and Benjamin Friedlander. *Classical and Modern Direction-of-Arrival Estimation*. Academic Press, 2009.

[65] Constantine A Balanis and Panayiotis I Ioannides. Introduction to smart antennas. *Synthesis Lectures on Antennas*, 2(1):1–175, 2007.

[66] Zhizhang Chen, Gopal Gokeda, and Yiqiang Yu. *Introduction to Direction-of-Arrival Estimation*. Artech House, 2010.

[67] Sathish Chandran. *Advances in Direction-of-Arrival Estimation*. Artech House, 2006.

[68] Jeffrey Foutz, Andreas Spanias, and Mahesh K. Banavar. *Narrowband Direction of Arrival Estimation for Antenna Arrays*. Morgan & Claypool Publishers, 2006.

[69] M. S. BARTLETT. Periodogram analysis and continuous spectra. *Biometrika*, 37(1-2):1–16, 1950.

[70] J. Capon. High-resolution frequency-wavenumber spectrum analysis. *Proceedings of the IEEE*, 57(8):1408–1418, 1969.

[71] R. O. Schmidt. *A signal subspace approach to multiple emitter location and spectral estimation*. PhD thesis, Stanford University.

[72] Petre Stoica, P. Handel, and A. Nehoral. Improved sequential music. *Aerospace and Electronic Systems, IEEE Transactions on*, 31(4):1230–1239, Oct 1995.

[73] A.J. Weiss and Benjamin Friedlander. Doa and steering vector estimation using a partially calibrated array. *Aerospace and Electronic Systems, IEEE Transactions on*, 32(3):1047–1057, July 1996.

[74] R. Roy and T. Kailath. Esprit-estimation of signal parameters via rotational invariance techniques. *Acoustics, Speech and Signal Processing, IEEE Transactions on*, 37(7):984–995, Jul 1989.

[75] H.H. Chen, S.C. Chan, Z.G. Zhang, and K.L. Ho. Adaptive beamforming and recursive doa estimation using frequency-invariant uniform concentric spherical arrays. *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 55(10):3077–3089, Nov 2008.

[76] Zhao Tan, Y.C. Eldar, and A. Nehorai. Direction of arrival estimation using co-prime arrays: A super resolution viewpoint. *Signal Processing, IEEE Transactions on*, 62(21):5565–5576, Nov 2014.

[77] Qing Shen, Wei Liu, Wei Cui, Siliang Wu, Y.D. Zhang, and M.G. Amin. Low-complexity direction-of-arrival estimation based on wideband co-prime arrays. *Audio, Speech, and Language Processing, IEEE/ACM Transactions on*, 23(9):1445–1456, Sept 2015.

[78] Jian-Feng Gu, S.C. Chan, Wei-Ping Zhu, and M.N.S. Swamy. Joint doa estimation and source signal tracking with kalman filtering and regularized qrd rls algorithm. *Circuits and Systems II: Express Briefs, IEEE Transactions on*, 60(1):46–50, Jan 2013.

[79] K.A. Gotsis, K. Siakavara, and J.N. Sahalos. On the direction of arrival (doa) estimation for a switched-beam antenna system using neural networks. *Antennas and Propagation, IEEE Transactions on*, 57(5):1399–1411, May 2009.

[80] Y. Ozaki, J. Ozawa, E. Taillefer, Jun Cheng, and Y. Watanabe. Direction-of-arrival estimation using adjacent pattern power ratio with switched beam antenna. In *Communications, Computers and Signal Processing, 2009. PacRim 2009. IEEE Pacific Rim Conference on*, pages 453–458, Aug 2009.

[81] Jeongkeun Lee, Dongkyun Kim, C. K. Toh, Taekyoung Kwon, and Yanghee Choi. A table-driven aoa estimation algorithm for switched-beam antennas in wireless networks. In *Wireless Conference 2005 - Next Generation Wireless and Mobile Communications and Services (European Wireless), 11th European*, pages 1–6, April 2005.

[82] J. Werner, J. Wang, A. Hakkarainen, N. Gulati, D. Patron, D. Pfeil, K. Dandekar, D. Cabric, and M. Valkama. Sectorized antenna-based doa estimation and localization: Advanced algorithms and measurements. *IEEE Journal on Selected Areas in Communications*, 33(11):2272–2286, Nov 2015.

[83] J. Werner, J. Wang, A. Hakkarainen, D. Cabric, and M. Valkama. Performance and cramer-rao bounds for doa/rss estimation and transmitter localization using sectorized antennas. *IEEE Transactions on Vehicular Technology*, 65(5):3255–3270, May 2016.

[84] M.A. Ringer and Gordon J. Frazer. Waveform analysis of transmissions of opportunity for passive radar. In *Signal Processing and Its Applications, 1999. ISSPA '99. Proceedings of the Fifth International Symposium on*, volume 2, pages 511–514 vol.2, 1999.

[85] C.R. Berger, B. Demissie, J. Heckenbach, P. Willett, and Shengli Zhou. Signal processing for passive radar using ofdm waveforms. *Selected Topics in Signal Processing, IEEE Journal of*, 4(1):226–238, Feb 2010.

[86] Sophocles J. Orfanidis. *Electromagnetic Waves and Antennas*. 2010.

[87] H. Krim and M. Viberg. Two decades of array signal processing research: the parametric approach. *IEEE Signal Processing Magazine*, 13(4):67–94, Jul 1996.

[88] X. Zhang and D. Xu. Low-complexity esprit-based doa estimation for colocated mimo radar using reduced-dimension transformation. *Electronics Letters*, 47(4):283–284, February 2011.

[89] Ahmed Khallaayoun. *A High Resolution Direction of Arrival Estimation Analysis and Implementation in a Smart Antenna System*. PhD thesis, Montana State University.

[90] B. Razavi. Challenges in portable rf transceiver design. *IEEE Circuits and Devices Magazine*, 12(5):12–25, Sep 1996.

[91] B. Debaillie, P. Van Wesemael, G. Vandersteen, and J. Craninckx. Calibration of direct-conversion transceivers. *IEEE Journal of Selected Topics in Signal Processing*, 3(3):488–498, June 2009.

[92] Christoph Stoeckle, Jawad Munir, Amine Mezghani, and Josef A. Nossek. Doa estimation performance and computational complexity of subspace- and compressed sensing-based methods. In *WSA 2015; 19th International ITG Workshop on Smart Antennas; Proceedings of*, pages 1–6, March 2015.

[93] Ying Zhang and Boon Poh Ng. Music-like doa estimation without estimating the number of sources. *Signal Processing, IEEE Transactions on*, 58(3):1668–1676, March 2010.

[94] Guanghan Xu and T. Kailath. Fast subspace decomposition. *Signal Processing, IEEE Transactions on*, 42(3):539–551, Mar 1994.

[95] R. Al Alawi. Rssi based location estimation in wireless sensors networks. In *Networks (ICON), 2011 17th IEEE International Conference on*, pages 118–122, 2011.

[96] FCC. Spectrum policy task force. ET Docket No.(02-135), Nov, 2002.

[97] A. Badawy and T. Khattab. A novel peak search amp; save cyclostationary feature detection algorithm. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 253–258, April 2014.

[98] A. Badawy, T. Elfouly, T. Khattab, C. F. Chiasserini, and D. Trinchero. Performance of eigenvalue based spectrum sensing in full-duplex cognitive radio networks. In *2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–6, May 2016.

[99] A. Badawy, T. Khattab, T. Elfouly, C. F. Chiasserini, and D. Trinchero. On the performance of spectrum sensing based on glr for full-duplex cognitive radio networks. In *2016 IEEE Wireless Communications and Networking Conference*, pages 1–6, April 2016.

[100] Ahmed Badawy, Tarek Elfouly, Carla-Fabiana Chiasserini, Tamer Khattab, and Daniele Trinchero. Exploiting spectrum sensing data for key management. *Computer Communications*, 97:31 – 39, 2017.

[101] T. Yucek and H. Arslan. A survey of spectrum sensing algorithms for cognitive radio applications. *Communications Surveys Tutorials, IEEE*, 11(1):116–130, First 2009.

[102] D.D. Ariananda, M.K. Lakshmanan, and H. Nikookar. A survey on spectrum sensing techniques for cognitive radio. In *Cognitive Radio and Advanced Spectrum Management, 2009. CogART 2009. Second International Workshop on*, pages 74–79, May 2009.

[103] Ezio Biglieri, Andrea J. Goldsmith, Larry J. Greenstein, Narayan B. Mandayam, and H. Vincent. Poor. *Principles of Cognitive Radio*. Cambridge University Press, 2012.

[104] Robert Caiming Qiu, Zhen Hu, Husheng Li, and Michael. C. Wicks. *Cognitive Radio Communication and Networking: Principles and Practice*. Wiley, 2012.

[105] Steven M. Kay. *Fundamentals of Statistical Signal Processing: Detection Theory*. Prentice Hall, Englewood Clifs, NJ, 1998.

[106] H. Urkowitz. Energy detection of unknown deterministic signals. *Proceedings of the IEEE*, 55(4):523 – 531, april 1967.

[107] W.A. Gardner. Signal interception: a unifying theoretical framework for feature detection. *Communications, IEEE Transactions on*, 36(8):897 –906, aug 1988.

[108] W.A. Gardner. Exploitation of spectral redundancy in cyclostationary signals. *Signal Processing Magazine, IEEE*, 8(2):14 –36, april 1991.

[109] W.A. Gardner and C.M. Spooner. Signal interception: performance advantages of cyclic-feature detectors. *Communications, IEEE Transactions on*, 40(1):149 –159, jan 1992.

[110] H. Vincent Poor and Olympia Hadjiliadis. Cambridge University Press, 2008.

[111] Lifeng Lai, Yijia Fan, and H.V. Poor. Quickest detection in cognitive radio: A sequential change detection framework. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5, 2008.

[112] Lifeng Lai, H.V. Poor, Yan Xin, and G. Georgiadis. Quickest search over multiple sequences. *Information Theory, IEEE Transactions on*, 57(8):5375–5386, 2011.

[113] F.F. Digham, M.-S. Alouini, and M.K. Simon. On the energy detection of unknown signals over fading channels. In *Communications, 2003. ICC '03. IEEE International Conference on*, volume 5, pages 3575 – 3579 vol.5, may 2003.

[114] F. F. Digham, M.-S. Alouini, and M. K. Simon. On the energy detection of unknown signals over fading channels. *Communications, IEEE Transactions on*, 55(1):21 –24, jan. 2007.

[115] S.P. Herath, N. Rajatheva, and C. Tellambura. Energy detection of unknown signals in fading and diversity reception. *Communications, IEEE Transactions on*, 59(9):2443 –2453, september 2011.

[116] O. Olabiyi and A. Annamalai. Further results on the performance of energy detector over generalized fading channels. In *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium on*, pages 604 –608, sept. 2011.

[117] A. Pandharipande and J. P M G Linnartz. Performance analysis of primary user detection in a multiple antenna cognitive radio. In *Communications, 2007. ICC '07. IEEE International Conference on*, pages 6482–6486, 2007.

[118] A. Taherpour, M. Nasiri-Kenari, and S. Gazor. Multiple antenna spectrum sensing in cognitive radios. *Wireless Communications, IEEE Transactions on*, 9(2):814–823, 2010.

[119] E. Axell and E.G. Larsson. Comments on "multiple antenna spectrum sensing in cognitive radios". *Wireless Communications, IEEE Transactions on*, 10(5):1678–1680, 2011.

[120] E. Soltanmohammadi, M. Orooji, and M. Naraghi-Pour. Spectrum sensing over mimo channels using generalized likelihood ratio tests. *Signal Processing Letters, IEEE*, 20(5):439–442, 2013.

[121] Rui Zhang, Teng Joon Lim, Ying-Chang Liang, and Yonghong Zeng. Multi-antenna based spectrum sensing for cognitive radios: A glrt approach. *Communications, IEEE Transactions on*, 58(1):84–88, 2010.

[122] Pu Wang, Jun Fang, Ning Han, and Hongbin Li. Multiantenna-assisted spectrum sensing for cognitive radio. *Vehicular Technology, IEEE Transactions on*, 59(4):1791–1800, 2010.

[123] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong. Relay selection for security enhancement in cognitive relay networks. *IEEE Wireless Communications Letters*, 4(1):46–49, Feb 2015.

[124] Lisheng Fan, Shengli Zhang, T. Q. Duong, and G. K. Karagiannidis. Secure switch-and-stay combining (sssc) for cognitive relay networks. *IEEE Transactions on Communications*, 64(1):70–82, Jan 2016.

[125] Lan Zhang, Rui Zhang, Ying-Chang Liang, Yan Xin, and Shuguang Cui. On the relationship between the multi-antenna secrecy communications and cognitive radio communications. *Communications, IEEE Transactions on*, 58(6):1877–1886, June 2010.

[126] Serge Vaudenay. *A Classical Introduction to Cryptography: Applications for Communications Security*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2005.

[127] W. Fumy and P. Landrock. Principles of key management. *IEEE Journal on Selected Areas in Communications*, 11(5):785–793, Jun 1993.

[128] Mukesh M. Prabhu and S.V. Raghavan. Security in computer networks and distributed systems. *Computer Communications*, 19(5):379 – 388, 1996.

[129] Paul Halliden. Network security issues. *Computer Communications*, 13(10):626 – 629, 1990.

[130] E. S. PAGE. Continuous inspection schemes. *Biometrika*, 41(1-2):100–115, 1954.

[131] George V. Moustakides. Optimal stopping times for detecting changes in distributions. *Ann. Statist.*, 14(4):1379–1387, 12 1986.

[132] Gary Lorden. On excess over the boundary. *Ann. Math. Statist.*, 41(2):520–527, 04 1970.

[133] Lifeng Lai, Yijia Fan, and H.V. Poor. Quickest detection in cognitive radio: A sequential change detection framework. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5, 2008.

[134] Y. C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang. Sensing-throughput tradeoff for cognitive radio networks. *IEEE Transactions on Wireless Communications*, 7(4):1326–1337, April 2008.

[135] L. Lu, G. Y. Li, and S. Li. Optimum periodic spectrum sensing for cr networks. *IEEE Communications Letters*, 16(12):1–4, December 2012.

[136] T. Riihonen and R. Wichman. Energy detection in full-duplex cognitive radios under residual self-interference. In *Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), 2014 9th International Conference on*, pages 57–60, June 2014.

[137] W. Afifi and M. Krunz. Incorporating self-interference suppression for full-duplex operation in opportunistic spectrum access systems. *Wireless Communications, IEEE Transactions on*, 14(4):2180–2191, April 2015.

[138] Yun Liao, Tianyu Wang, Lingyang Song, and Bingli Jiao. Cooperative spectrum sensing for full-duplex cognitive radio networks. In *Communication Systems (ICCS), 2014 IEEE International Conference on*, pages 56–60, Nov 2014.

[139] Gary Lorden. Procedures for reacting to a change in distribution,. *Ann. Statist.*, (6):1897–1908, 07.

[140] Gary Lorden. Open-ended tests for koopman-darmois families. *Ann. Statist.*, (4):633–643, 07.

[141] Louis Gordon and Moshe Pollak. A robust surveillance scheme for stochastically ordered alternatives. *Ann. Statist.*, (4):1350–1375, 08.

[142] R. Tandra and A. Sahai. Snr walls for signal detection. *Selected Topics in Signal Processing, IEEE Journal of*, 2(1):4–17, 2008.

[143] Seyit A Camtepe and Bülent Yener. Key distribution mechanisms for wireless sensor networks: a survey. *Rensselaer Polytechnic Institute, Troy, New York, Technical Report*, pages 05–07, 2005.

[144] Shu Tezuka. *Uniform Random Numbers Theory and Practice, Vol. 315*. Springer Science+Business Media,LLC., 1 edition.

[145] Li Tan. *Digital Signal Processing Fundamentals and Applications*. Academic Press, 2007.

[146] O. Gungor, F. Chen, and C.E. Koksal. Secret key generation via localization and mobility. *Vehicular Technology, IEEE Transactions on*, PP(99):1–1, 2014.

[147] A. Sayeed and A. Perrig. Secure wireless communications: Secret keys through multipath. In *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, pages 3013–3016, March 2008.

[148] P. Kaligineedi, M. Khabbazian, and V.K. Bhargava. Malicious user detection in a cognitive radio cooperative sensing system. *Wireless Communications, IEEE Transactions on*, 9(8):2488–2497, August 2010.

[149] F. Adelantado and C. Verikoukis. A non-parametric statistical approach for malicious users detection in cognitive wireless ad-hoc networks. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–5, June 2011.

[150] E. Soltanmohammadi and M. Naraghi-Pour. Fast detection of malicious behavior in cooperative spectrum sensing. *Selected Areas in Communications, IEEE Journal on*, 32(3):377–386, March 2014.

[151] Wei Wang, Lin Chen, K.G. Shin, and Lingjie Duan. Thwarting intelligent malicious behaviors in cooperative spectrum sensing. *Mobile Computing, IEEE Transactions on*, 14(11):2392–2405, Nov 2015.