PHYSICAL LAYER SECURITY IN CO-OPERATIVE MIMO NETWORKS - KEY GENERATION AND RELIABILITY EVALUATION

by

KAN CHEN

B.E., Wuhan University, 2006

M.E., Stevens Institute of Technology, 2010

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Electrical and Computer Engineering
College of Engineering

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2016

Abstract

Widely recognized security vulnerabilities in current wireless radio access technologies undermine the benefits of ubiquitous mobile connectivity. Security strategies typically rely on bit-level cryptographic techniques and associated protocols at various levels of the data processing stack. These solutions have drawbacks that have slowed down the progress of new wireless services. Physical layer security approaches derived from an information theoretic framework have been recently proposed with secret key generation being the primary focus of this dissertation. Previous studies of physical layer secret key generation (PHY-SKG) indicate that a low secret key generation rate (SKGR) is the primary limitation of this approach. To overcome this drawback, we propose novel SKG schemes to increase the SKGR as well as improve the security strength of generated secret keys by exploiting multiple input and multiple output (MIMO), cooperative MIMO (co-op MIMO) networks. Both theoretical and numerical results indicate that relay-based co-op MIMO schemes, traditionally used to enhance LTE-A network throughput and coverage, can also increase SKGR. Based on the proposed SKG schemes, we introduce innovative power allocation strategies to further enhance SKGR. Results indicate that the proposed power allocation scheme can offer 15% to 30% increase in SKGR relative to MIMO/co-op MIMO networks with equal power allocation at low-power region, thereby improving network security. Although co-op MIMO architecture can offer significant improvements in both performance and security, the concept of joint transmission and reception with relay nodes introduce new vulnerabilities. For example, even if the transmitted information is secured, it is difficult but essential to monitor the behavior of relay nodes. Selfish or malicious intentions of relay nodes may manifest as non-cooperation. Therefore, we propose relay node reliability evaluation schemes to

measure and monitor the misbehavior of relay nodes. Using a power-sensing based reliability evaluation scheme, we attempt to detect selfish nodes thereby measuring the level of non-cooperation. An overall node reliability evaluation, which can be used as a guide for mobile users interested in collaboration with relay nodes, is performed at the basestation. For malicious behavior, we propose a network tomography technique to arrive at node reliability metrics. We estimate the delay distribution of each internal link within a co-op MIMO framework and use this estimate as an indicator of reliability. The effectiveness of the proposed node reliability evaluations are demonstrated via both theoretical analysis and simulations results. The proposed PHY-SKG strategies used in conjunction with node reliability evaluation schemes represent a novel cross-layer approach to enhance security of cooperative networks.

PHYSICAL LAYER SECURITY IN CO-OPERATIVE MIMO NETWORKS - KEY GENERATION AND RELIABILITY EVALUATION

by

KAN CHEN

B.E., Wuhan University, 2006

M.E., Stevens Institute of Technology, 2010

A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Electrical and Computer Engineering
College of Engineering

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2016

Approved by:

Major Professor
Dr. Balasubramaniam Natarajan

Abstract

Widely recognized security vulnerabilities in current wireless radio access technologies undermine the benefits of ubiquitous mobile connectivity. Security strategies typically rely on bit-level cryptographic techniques and associated protocols at various levels of the data processing stack. These solutions have drawbacks that have slowed down the progress of new wireless services. Physical layer security approaches derived from an information theoretic framework have been recently proposed with secret key generation being the primary focus of this dissertation. Previous studies of physical layer secret key generation (PHY-SKG) indicate that a low secret key generation rate (SKGR) is the primary limitation of this approach. To overcome this drawback, we propose novel SKG schemes to increase the SKGR as well as improve the security strength of generated secret keys by exploiting multiple input and multiple output (MIMO), cooperative MIMO (co-op MIMO) networks. Both theoretical and numerical results indicate that relay-based co-op MIMO schemes, traditionally used to enhance LTE-A network throughput and coverage, can also increase SKGR. Based on the proposed SKG schemes, we introduce innovative power allocation strategies to further enhance SKGR. Results indicate that the proposed power allocation scheme can offer 15% to 30% increase in SKGR relative to MIMO/co-op MIMO networks with equal power allocation at low-power region, thereby improving network security. Although co-op MIMO architecture can offer significant improvements in both performance and security, the concept of joint transmission and reception with relay nodes introduce new vulnerabilities. For example, even if the transmitted information is secured, it is difficult but essential to monitor the behavior of relay nodes. Selfish or malicious intentions of relay nodes may manifest as non-cooperation. Therefore, we propose relay node reliability evaluation schemes to

measure and monitor the misbehavior of relay nodes. Using a power-sensing based reliability evaluation scheme, we attempt to detect selfish nodes thereby measuring the level of non-cooperation. An overall node reliability evaluation, which can be used as a guide for mobile users interested in collaboration with relay nodes, is performed at the basestation. For malicious behavior, we propose a network tomography technique to arrive at node reliability metrics. We estimate the delay distribution of each internal link within a co-op MIMO framework and use this estimate as an indicator of reliability. The effectiveness of the proposed node reliability evaluations are demonstrated via both theoretical analysis and simulations results. The proposed PHY-SKG strategies used in conjunction with node reliability evaluation schemes represent a novel cross-layer approach to enhance security of cooperative networks.

Table of Contents

Bibliography 113

List of Figures

List of Tables

Acknowledgments

First and foremost, I would like to thank all professors and friends who have helped and supported me in my Ph.D. career. This dissertation would not have been possible without the help of you.

I would like to give special and sincere thanks to my supervisor Dr. Bala Natarajan for his guidance, motivation, encouragement and uninterrupted help. It is a memorable experience for me to pursue my Ph.D. degree with the guidance of Dr. Bala. His encouragement and patience have been constantly helping me overcome challenge problems in my research. I consider him as one of my role model in both research (thorough insight and untiring perseverance) and life (time management).

I would like to express my gratitude to Dr. William Hsu for leading me to the fantastic world of Machine Learning and Big Data which inspire me to bring those techniques into my research of anomaly detection in cooperative networks. The hands on experience in technical side help me to open another door in my research.

My sincere appreciation to the Doctoral Committee Members Dr. Xinming Ou, Dr. Nathan Albin, Dr. Sanjoy Das and Dr. Yurii Maravin for their constructive feedback and advice in making this dissertation to the final shape.

I am also grateful for the chance to be a part of wireless communication (WiCom) group at Electrical and Computer Engineering department of Kansas State University. I would like to thanks to our former member Dr. Mohammed Taj-Eldin, Dr. Alam Shafiul, Dr. Chang Liu for their valuable experience, guidance and mentoring. Additionally, I am thankful to current lab members Kumar Jhala, Dale Scutti, Wenji Zhang, Solmaz Niknam, Reza Barazideh and Alaleh Alivar for their support and feedback on my research.

Last but not least, to my respectful parents and my dear wife, thank you so much.

Dedication

This dissertation is dedicated to my parents Qian Guan, Yihong Chen and my wife Xijue Wang, whose unconditional love and support me in my Ph.D. journey.

To Qian Guan and Yihong Chen, my respectful parents. I should not forget your countless sacrifices in order to raise me up. Without the inspiration, drive, and support that you have given me, I might not be the person I am today. I hope I can always make you proud.

To Xijue Wang, my dear wife. I am fortunate to have you as my life partner. You endless support and encouragement remind me of my capability and potential. Thanks for everything, you give me wings.

To Fiona, my lovely cat. You make my research full of joy and happiness.

Finally, I am grateful to all of my well-wishers.

Chapter 1

Introduction

As wireless communication-dependent industries such as smart grid, healthcare services, and transportation systems rapidly develop, advanced wireless communication networks must provide higher data rates, lower latency, enhanced security, reduced operating cost, multi-antenna support, flexible bandwidth operation, and seamless integration with existing systems. The cooperative multiple input multiple output (co-op MIMO) network [1] [2], currently incorporated into 4G LTE , is a potential solution for meeting the challenges of evolving wireless communications [3]. A co-op MIMO network typically utilizes distributed antennas on multiple radio devices in order to boost network throughput, conserve energy, and improve network coverage. Co-op MIMO fundamentally groups multiple devices into virtual antenna arrays (VAAs) in order to emulate MIMO communications. A co-op MIMO transmission involves multiple point-to-point radio links, including links within a VAA and links between various VAAs. In practice, many wireless devices may not be able to support multiple antennas due to dimension, budget, and hardware limitations. A co-op MIMO network is especially useful for allowing those devices to reap the benefits provided by MIMO networks. Although co-op MIMO architecture significantly improves the performance of wireless communication, it is vulnerable from a security perspective. Due to the open architecture, relay nodes with selfish or malicious intentions may join a cooperative network.

Selfish nodes may suddenly choose not to cooperate in order to preserve their battery resources or prioritize other services. Malicious nodes, on the other hand, attempt to prevent communication between source and destination nodes at any cost. Note that an adversary may control malicious nodes to attack cooperative networks (i.e., denial of service attack at the physical layer).

1.1 Physical Layer Security

Although a number of distinguished studies have focused on ways to improve wireless network performance by exploiting advanced network architecture, such as MIMO, co-op MIMO, and cognitive radio networks, security issues have often been overlooked [4] [2] [1].Two fundamental characteristics of the wireless medium, namely broadcast and superposition, present unique challenges for ensuring reliable and/or secure communications in the presence of adversarial users. The broadcast nature of wireless communications creates difficulty for shielding transmitted signals from unintended recipients, and superposition can lead to overlapping of multiple signals at the receiver [5]. Issues of privacy and security in wireless communication networks have become increasingly crucial as these networks continue to flourish worldwide [6]. Therefore, investigation of security issues related to wireless networks has become an increasingly popular research field in recent years. Security has traditionally been viewed as an independent feature addressed above the physical layer, and all commonly used cryptographic protocols, such as RSA and AES are designed and implemented with the assumption that the physical layer has been established and provides an error-free link. However, in dynamic wireless networks, this raises issues such as key distribution for symmetric cryptosystems and high computational complexity of asymmetric cryptosystems [7]. More importantly, all cryptographic measures are based on the premise that their deciphering is computationally infeasible without knowledge of the secret key; but, this premise remains mathematically unproven. Ciphers that were previously considered vir-

tually unbreakable are continually surmounted due to relentless growth of computational power [5]. Existing theoretical and practical contributions support the potential of physical layer security techniques to significantly strengthen the security of wireless communication networks [8]. Consequently, secrecy at the physical layer has recently attracted significant interest among researchers.

The basic principle of information-theoretic security, widely accepted as the strictest notion of security, requires the combination of cryptographic schemes with channel coding techniques that exploit the randomness of communication channels to guarantee that sent messages cannot be decoded by a third party maliciously eavesdropping on the wireless medium [9]. Following Shannon's fundamental work on information-theoretic security, Wyner introduced a new wiretap channel model [10]. Based on the assumption that the wiretap channel is a probabilistically degraded version of the main channel, the objective of Wyner's keyless security scheme at the physical layer is to maximize transmission rate of the main channel while minimizing the amount of information leaked to the wiretap channel (wiretapper). Maurer later presented a strategy that allows joint development of secret keys between transmitter and receiver with the help of a public error-free feedback channel [11], thereby permitting secret keys to be extracted between communication parties by exploiting common randomness in the wireless channel (reciprocity). Recently, the Radio Frequency (RF) fingerprinting technique is proposed by the physical layer security community as an additional protection layer for wireless devices. Transmitters are identified by their unique transient characteristics. A receiver can challenge a user to prove its unique identity to further enhance the security level of wireless communication. Therefore, the three main thrust areas in PHY-layer security research are (1) keyless security based on work by Wyner [10] [12] [13]; (2) physical layer secret key generation (PHY-SKG) following the work of Shannon and Maurer [11] [14] [15]; and (3) RF fingerprinting [16] [17].

This dissertation primarily focuses on the PHY-SKG. Secret keys are typically generated by common randomness that sources extract from channels between parties in a wireless

communication system. Eavesdroppers experience independent physical channels from legitimate users as long as they are a few wavelengths away from legitimate nodes [18], as is common in wireless networks. Therefore, keys are secure with an information-theoretic guarantee [19]. Compared to a traditional SKG algorithm, such as Diffie-Hellman protocol, the PHY-SKG technique has the following advantages: (1) a computationally bounded adversary does not need to be assumed [20]; (2) does not require key management, a challenging issue in traditional key generation schemes [21]; and (3) ability to dynamically replenish secret keys because wireless channels vary over time [19]. In addition, PHY-SKG can be used to enhance existing security schemes because it can be implemented independently from higher layer security schemes [5].

1.2 Challenges in Physical Layer Security

Successful and reliable implementation of a physical layer security protocol in co-op MIMO networks presents at least two major challenges: security and reliability. These challenges are briefly discussed in the following paragraphs.

Security : Low secret key generation rate (SKGR), a critical performance metric, is the primary limitation of PHY-SKG. This is straightforward to understand because the security strength of a secret key is theoretically proportional to key length [22]. As mentioned in 1.1, secret keys are generated using common randomness that sources extract from channels between parties in a wireless communication system. Traditional invariant point-to-point communication does not increase randomness between wireless channels as well as SKGR. Thus, the next stage of PHY-SKG evolution involves exploitation of common randomness in reciprocal channels using advanced network technology. In addition, power is another factor that significantly impacts SKGR. Maximization of SKGR under power constraints is an open research area.

Reliability: In co-op MIMO architectures, mobile users are allowed to recruit relay

nodes (e.g., idle users, femtocells, and picocells). While PHY-SKG provides protection against eavesdropping, detecting misbehavior of relay nodes that have already joined the cooperative communication is very difficult. Selfish or malicious intentions of relay nodes may manifest as non-cooperation. Selfish nodes may suddenly choose not to cooperate in order to preserve their battery resources or prioritize other services. Malicious nodes, on the other hand, attempt to prevent communication between source and destination nodes at any cost. Note that an adversary may control malicious nodes to attack cooperative networks, i.e., a denial of service attack at the physical layer. Therefore, understanding how to measure and monitor reliability of relay nodes is a critical challenge in co-op MIMO based physical layer security schemes.

This dissertation seeks to address a few fundamental research questions related to these challenge. These questions and prior efforts to address them are discussed in the following subsections.

1.3 Research Questions

Question 1: *How can one increase the SKGR in order to improve the security strength of generated secret keys using advanced network technology (e.g., co-op MIMO, etc)?*

Question 2: *What is the effect of optimizing power on SKGR in MIMO and co-op MIMO systems?*

Question 3: *How to measure and monitor the reliability of relay nodes under co-op MIMO architecture, especially, how to detect selfish relay nodes who suddenly choose not to cooperate in order to preserve their battery resources or prioritize other services?*

Question 4: *How to measure and monitor the reliability of relay nodes under co-op MIMO*

architecture in a more general manner, i.e., how to detect non-cooperative relay nodes with malicious behavior?

1.4 Related Work

This dissertation attempts to address the above research questions in the context of co-op MIMO networks. However, the methods, algorithms, and theoretical results/insights developed in this work can be applied to any dynamic wireless network with minor application-specific modifications. From a security perspective, the following subsections summarize prior work related to the research questions of interest.

1.4.1 Question 1: Increasing SKGR by exploiting common randomness

[23] proposes three types of relay-based co-op MIMO models and provides an overview of co-op MIMO channel modeling and associated challenges in a cellular system. [19] introduces several prevalent methods to enhance security at the PHY-layer in wireless networks, and [24] discusses challenges regarding implementation of wireless PHY-layer security. [25] and [21] present the basics of SKG technique and introduce two popular methods: SKG based on channel phase and SKG based on received signal strength (RSS). Wang et al. analyze SKG technique based on channel phase randomness [20]. In [26], the authors present a practical SKG technique based on RSS; however, both [20] and [26] require complex algorithms to realize an acceptable SKGR. In [27], SKG technique is applied to a MIMO wireless channel, and an information-theoretic measure of SKGR is proposed. Lai et al. present SKG protocols for a wireless communication system with relays [18], however, their analysis is limited to single antenna-based point-to-point communication. In the context of prior efforts in SKG, it is evident that understanding how to effectively exploit relay-based

co-op MIMO architecture for SKG is still an open problem.

1.4.2 Question 2: Increasing SKGR by optimizing power allocations

A comprehensive review of physical layer security in wireless networks is presented in [5]. [19] introduces several prevalent methods to enhance security at physical layer in wireless networks. Challenges related to implementation of physical layer security schemes in wireless communication are discussed in [24]. [21] and [25] present the basics of SKG and introduce two popular methods: SKG based on channel phase and SKG based on received signal strength (RSS). Detailed analysis of SKG based on channel phase randomness is provided in [20]. The authors of [26] present a practical SKG technique based on RSS. However, both [20] and [26] require complex algorithms to realize an acceptable SKGR. Wallace et al. implement SKG in MIMO networks and propose an information theoretic measure of SKGR. Lai et al. present SKG protocols for wireless communication systems with relays in [18]. However, analysis in [18] is limited to a single antenna-based point-to-point communication. [28] proposes three types of relay-based coop MIMO models and provides an overview of coop MIMO channel modeling and associated challenges in a cellular system. Zhou et al. propose a key generation scheme in a two-way relay channel and discuses optimal power allocation of SKGR with a passive attacker in [29]. However, the analysis in [29] is restricted to a single antenna relay network in which all nodes, including transmitter, receiver, and relay nodes, employ only one antenna. This is not a realistic assumption for contemporary large-scale wireless networks. (i.e., LTE-A) Furthermore, thanks to the single antenna assumption, the optimal power allocation problem simplifies to a water-filling solution. In the context of prior efforts related to PHY-SKG schemes, it is evident that quantifying the effect of power allocation strategies on SKGR in co-op MIMO architectures remains an open problem.

1.4.3 Question 3&4: Relay node reliability evaluation

An overview of co-op MIMO networks is introduced in [30]. The authors of [30] propose three types of relay-based coop MIMO models, and the implementation and performance of co-op MIMO networks are discussed in [31] and [32]. [33] proposes an energy-efficient, reliable topological clustering algorithm (ERCTNA) to increase reliability of network topology using an auxiliary cluster head node and optimizing information transfer mode. The authors of [34,35] propose a selection criterion for cooperating nodes in a wireless multi-hop networks. However, they focus on increasing network level reliability by selecting the best route from source to destination. [36] introduces a MAC layer scheme for wireless sensor networks, thereby improving overall network reliability via cooperative communication. [37] investigates the relationship between node reliability and system performance, where node reliability is defined as reliability of cooperation, which is modeled via a probability distribution of non-cooperation. Authentication is a common tool for ensuring reliability. Therefore, [38] and [39] improve node reliability in cooperative networks by exploiting authentication techniques. However, none of these prior efforts provide any insights into how to evaluate the reliability of individual nodes [40]. evaluates the reliability of relay nodes based on a power sensing algorithm; however, the reliability evaluation scheme is restricted to a specific non-cooperative scenario. Therefore, evaluating and appropriately exploiting relay node reliability metrics in a co-op MIMO architecture is an open problem that requires further investigation.

1.5 Contributions of This Dissertation

This dissertation proposes a cross-layer high-level security protocol for co-op MIMO networks that can be easily applied to any dynamic wireless network with minor application-specific modifications. The security protocol contains two main components: PHY-SKG schemes and relay nodes reliability evaluation schemes. Novel PHY-SKG schemes are pro-

posed to increase the SKGR, considered to be the main limitation of PHY-SKG schemes. In order to further improve the security strength, innovative power allocation algorithms are proposed to optimize the SKGR under MIMO and co-op MIMO architectures. Both of these efforts demonstrate the feasibility of implementing PHY-SKG schemes to protect transmitted information in wireless communication. However, even if the transmitted information is secured, it is difficult but essential to monitor the behavior of relay nodes since mobile users are allowed to recruit relay nodes (i.e., idle users, femtocells, and picocells) during communication. Therefore, in order to measure and monitor the misbehavior of these nodes, two relay node reliability evaluation schemes that exploit power sensing and network tomography, respectively, are proposed in this dissertation. First, a power-sensing based scheme focuses on detecting selfish nodes, i.e., whether relay nodes are cooperating or not (transmission or not is the primary concern). Secondly, the network-tomography based scheme generally focuses on identifying malicious nodes i.e., whether relay nodes are properly cooperate with system or not. In addition, the proposed node reliability evaluation scheme used in conjunction with proposed cooperative PHY-SKG strategies offer a novel cross-layer security protocol to significantly enhance security of cooperative networks. In this regard, the major contributions of this dissertation are presented below, which forms the foundation of this dissertation:

- Question 1: How can one increase SKGR by exploiting common randomness in co-op MIMO networks
  - This dissertation proposes innovative SKG schemes in two practical scenarios of LTE-A network with relay-based co-op MIMO architecture.
  - This dissertation demonstrates that relay schemes and co-op MIMO techniques used to enhance throughput and coverage of network, can also improve SKGR.
  - This dissertation studies the relationship between SKGR and the number of relay nodes or number of antennas in both scenarios. Results indicate that the number

of source antennas play a more significant role compared to the number of relay nodes in the first scenario and both the number of source antennas and number of relay nodes have an equivalent impact on SKGR in the second scenario.

Details regarding the findings related to this question can be found in 3 of this dissertation and following publication:

- K. Chen, B. Natarajan, and S. Shatti, "Relay-based secret key generation in LTE-A," in *Communications and Network Security: Physical Layer security workshop. IEEE Conference on*, Oct 2014
- K. Chen and B. Natarajan, "Mimo-based secret key generation strategies: Rate analysis," *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, vol. 6, no. 3, pp. 22–55, Jan 2015

- Question 2: What is the impact of optimizing power on SKGR?
  - This dissertation extends the basic SKG scheme to the MIMO case and derives a power allocation strategy.
  - This dissertation derives the optimal power allocation for the two novel SKG schemes proposed for the co-op MIMO architectures.
  - Results demonstrate that the proposed power allocation schemes can offer 15% to 30% increase in SKGR relative to equal power allocation in MIMO/co-op MIMO networks, thereby improving network security.

Results related to this question can be found in 4 of this dissertation and the following publication:

- K. Chen, B. Natarajan, and S. Shattil, "Secret key generation rate with power allocation in relay-based lte-a networks," *Information Forensics and Security, IEEE Transactions on*, vol. 10, no. 11, pp. 2424–2434, Nov 2015

- Question 3: How to evaluate relay node reliability by identifying non-cooperation due to selfish behavior?
  - This dissertation proposes novel power-sensing based node reliability evaluation schemes to enhance security of co-op MIMO networks.
  - This dissertation introduces two distributed node level reliability detection methods: (1) a one-shot instantaneous reliability detection and (2) Bayesian framework based dynamic reliability detection that incorporates history of node behavior.
  - A centralized reliability evaluation strategies to fuse the node level reliability information is proposed. The central server (e.g., base station) can share these metrics with other mobile users who are interested in recruiting trustworthy nodes for cooperative operations.

  Results related to this question can be found in 5 of this dissertation and the following publication:

  - K. Chen and B. Natarajan, "Evaluating node reliability in cooperative mimo networks (under review)," *Information Forensics and Security, IEEE Transactions on*, 2015

- Question 4: How to evaluate relay node reliability by detecting non-cooperative relay nodes with malicious behavior?
  - This dissertation proposes a novel node reliability evaluation scheme based on internal link delay distribution.
  - This dissertation implements an active probing network tomography to estimate internal link delay distribution by utilizing an EM algorithm.
  - Simulation results demonstrate the effectiveness of the delay distribution based reliability detection.

Results related to this question can be found in 6 of this dissertation and the following publication:

– K. Chen and B. Natarajan, "Network tomography based node reliability evaluation in cooperative mimo networks (under review)," *Special Issue on Physical Layer Security for Emerging Wireless Networks: From Theory to Practice*, 2015

1.6 Organization of This Dissertation

Chapter 2 provides the background on basics of physical layer security, performance metrics, information-theoretic models of SKG, toy example of SKG scheme for wireless point-to-point network and co-op MIMO networks. Chapter 3 describes the proposed novel SKG schemes, which significantly increase SKGR as well as security strength of generated secret keys, by exploiting advanced co-op MIMO networks. In order to further improve the security level of generated secret keys, Chapter 4 proposes innovative power allocation algorithms to enhance SKGR by utilizing advantages of MIMO and co-op MIMO architectures. In Chapter 5, power-sensing based reliability evaluation schemes are proposed to monitor and measure whether or not relay nodes are cooperating/transmitting in co-op MIMO networks. Network-tomography based reliability evaluation scheme is presented in Chapter 6 and can be used to evaluate general scenarios of relay node misbehavior by estimating internal link delay distribution. Concluding remarks and future research directions are discussed in Chapter 7.

Chapter 2

Physical Layer Security – Basics

2.1 Basic Information-Theoretic Models for SKG

This section reviews basic information-theoretic models for SKG assuming availability of a public channel. All prior efforts in this area can be categorized as investigations based on source-type model (STM) and studies based on channel-type model (CTM). Following Rudolph Ahlswede and Imre Csiszir's distinguished works in [45], definitions of STM and CTM are included in the following paragraphs.

Source-type model: An STM is a discrete memoryless multiple source (DMMS) with two component sources and generic variables (X, Y). Terminal Alice can observe source outputs $X^n = (X_1, \ldots, X_n)$ and terminal Bob can observe source outputs $Y^n = (Y_1, \ldots, Y_n)$. In addition, a noiseless public channel of unlimited capacity is available for communication between the two terminals.

Channel-type model: A CTM is a discrete memoryless channel (DMC) $\{W : X \to Y\}$. Terminal Alice governs the input of this DMC while Terminal Bob observes output. In addition to transmissions of length n over this DMC, referred to as a secure channel, a noiseless public channel of unlimited capacity may be used for communication

between the two terminals.

This dissertation primarily focus on STM, providing background knowledge for further investigations. A detailed discussion of SKG strategy with unlimited public channel is initially presented.

2.1.1 SKG strategy with unlimited public channel

For a basic STM, both Alice and Bob can observe source output X^n and Y^n, which are correlated discrete i.i.d source sequences, respectively. In addition, a noiseless public channel with unlimited capacity is available for communication between Alice and Bob. Since the eavesdropper Eve can also access the public channel, an SKG strategy should be deployed between Alice and Bob to prevent Eve from eavesdropping. Alice generates forward transmission message Φ_i and Bob generates backward transmission message Ψ_i at consecutive instances $i = 1, \ldots, k$ by considering communication over public channels to be an exchange of messages or codewords between two terminals. Φ_i and Ψ_i depend on all available information for corresponding terminal at instance i. The assumption is made that, at the initially time, Alice and Bob generate independent random variables M_A and M_B, respectively. Therefore, the formal definition of an SKG strategy for STM is as follows:

- Step 0) The terminals generate random variables M_A and M_B such that X^n, Y^n, and (X^n, Y^n) are mutually independent.
- Step 1) The two terminals exchange messages Φ_i and Ψ_i over the public channel, where $\Phi_1 = \Phi_1(M_A, X^n)$, $\Psi_1 = \Psi_1(M_B, Y^n)$.
- Step i) The two terminals exchange messages Φ_i and Ψ_i where $\Phi_1 = \Phi_1(M_A, X^n, \Psi^{i-1})$, $\Psi_1 = \Psi_1(M_B, Y^n, \Psi^{i-1})$.
- Final step) Both terminals compute what they deem to be the key established

by the secret sharing process, as a function of available information:

$$K = K(M_A, X^n, \Psi^k)) \tag{2.1}$$

$$K = L(M_B, Y^n, \Phi^k)). \tag{2.2}$$

For successful SKG strategies, K and L must satisfy certain conditions. For example, two terminals should generate a common key with a small probability of error.

Definition 2.1.1. SKGR For STM, an SKGR is achievable if for every $\epsilon > 0$ and sufficiently large n an SKG strategy exists such that K and L satisfy

$$PrK \neq L \leq \epsilon \tag{2.3}$$

$$\frac{1}{n} I(\Phi^k), \Psi^k; K) \leq \epsilon \tag{2.4}$$

$$\frac{1}{n} H(K) \geq R_s - \epsilon \tag{2.5}$$

$$\frac{1}{n} \log K \leq \frac{1}{n} H(K) + \epsilon. \tag{2.6}$$

Eq. 2.3 means that K should be equal to L with high probability, and Eq. 2.4 means that K and L are secret keys since exchange over the public channel provided no information concerning the keys. A measurement of SKGR is given in Eq. 2.6, indicating that distribution of the key is almost uniformly distributed in entropy sense. This is certainly important when one generated secret key is used for encryption. Uniform distribution is the maximum entropy distribution among all distributions with finite support. Because entropy is a measure of uncertainty in a random variable, higher entropy of encryption keys leads to increased challenges for eavesdroppers to crack them.

Evaluation of SKG techniques performance requires a standard performance metric, as defined below. Maximum secret key generation rate (MSKGR) is

$$R_{s_{max}} = I(X;Y). \tag{2.7}$$

In the following sections, MSKGR $R_{s_{max}}$ is the standard performance metric for theoretical analysis. For simplicity, the term SKGR is used to represent MSKGR in the following sections.

2.2 SKG Strategies for Wireless Networks

In this section, the basics of the PHY-SKG technique based on the channel reciprocity property are introduced in order to provide background knowledge for this research as well as a standard for performance comparison. The following paragraphs outlines the basic concept behind SKG.

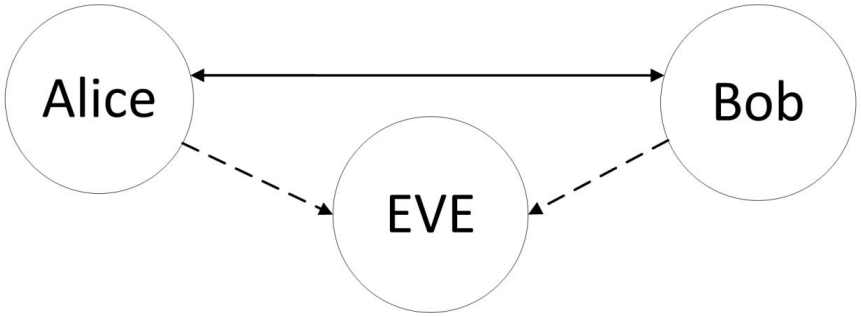

Figure 2.1: *A Simple Wiretap Channel Model*

Consider a simple wiretap channel model [10] depicting the simplest case of a multiuser environment as shown in Fig. 2.1. Here, the model consists of three nodes: transmitter (Alice), receiver (Bob), and eavesdropper (Eve). A general method for generating secret key between Alice and Bob in the presence of Eve is as follows. Alice/Bob sends probe signals to corresponding receivers, and the receivers have the ability to

estimate common random channel state information (CSI) of their communication channel. Therefore, because channel fading is random, Alice and Bob can convert their estimated CSI into random bit strings. Theoretically, the random bit strings generated by Alice and Bob should be identical because of the reciprocal property of wireless channel. However, in practice, errors and/or disagreements are possible between the random bit strings. An agreed and corrected secret key is generated with the help of key reconciliation and privacy amplification techniques [46] [6]. Although the eavesdropper (Eve) is present during this entire process, the secret key between Alice and Bob cannot be "stolen" as Eve experiences an independent channel (as long as the distance between Eve and Alice/Bob is at least one-half wavelength) [47]. In an other word, the channel between legitimate users and the channel between legitimate users and eavesdroppers are independent. In order to analyze theoretical performance, the wiretap channel is transferred to a point-to-point communication system, as shown in Fig. 2.2. Alice and Bob are two users who want to generate a secret key via a wireless fading channel. Both of them can transmit over the wireless channel and public channel [48].The point-to-point system is assumed to be half duplex and the channel to be reciprocal in a channel coherence time T_C. A detailed SKG scheme for general wireless communication based on previously discussed information-theoretic models that exploit channel reciprocity via public channels with unlimited capacity [49] are introduced in the following paragraphs.

Figure 2.2: *A Simple Wireless Fading Channel*

Previous research [18] has indicated that two steps are necessary to generate the secret key via channel reciprocity. In the first step, channel estimation, Alice and Bob estimate the common channel gain, h_{AB} and h_{BA}, through training. In the second step, key agreement, Alice and Bob agree on a secret key based on common channel information using Slepian-Wolf source coding.

For channel estimation, the assumption is made that the amount of time for training between Alice and Bob is T. Let T_A be training time spent by Alice and T_B be training time spent by Bob ($T_A + T_B = T$). The SKG scheme for point-to-point network is shown in Table. 2.1.

Channel Estimation	
Timeslots	Action
Timeslot 1	Alice sends a known training sequence $\mathbf{s_A}$ of length L to Bob over wireless fading channel with transmit power P.
Timeslot 2	Bob transmits a known training signal $\mathbf{s_B}$ of length L to Alice over wireless fading channel with the same power P.
Key Agreement	
Steps	Action
	Alice and Bob agree on key K_{AB} extracted from reciprocal fading channel $(\tilde{h_{AB}}, \tilde{h_{AB}})$ using public channel.

Table 2.1: *SKG schemes for point-to-point wireless networks*

In the first timeslot (T_A), Alice sends a known training sequence $\mathbf{s_A}$of length L over a wireless channel. Bob receives

$$\mathbf{y_B} = h_{AB}\mathbf{s_A} + \mathbf{n_B} \tag{2.8}$$

where, h_{AB} and N_B denote channel fading gain from Alice to Bob and Gaussian noise

at Bob's receiver. Using similar notation, Bob transmits a known training signal $\mathbf{s_B}$ of length L in the second timeslot. Alice receives:

$$\mathbf{y_A} = h_{BA}\mathbf{s_B} + \mathbf{n_A}. \tag{2.9}$$

The system is assumed to be half duplex, and the channel is reciprocal.

In order to generate secret key based on common randomness between forward and backward channels, Alice and Bob must generate the estimation of h_{AB} and h_{BA}, respectively.

$$\tilde{h}_{AB} = \mathbf{Y_A}\frac{\mathbf{s_A^T}}{\|\mathbf{s_A}\|^2} = \mathbf{h_{AB}} + \mathbf{n_B}\frac{\mathbf{s_A^T}}{\|\mathbf{s_A}\|^2} \tag{2.10}$$

$$\tilde{h}_{BA} = \mathbf{Y_B}\frac{\mathbf{s_B^T}}{\|\mathbf{s_B}\|^2} = \mathbf{h_{BA}} + \mathbf{n_A}\frac{\mathbf{s_B^T}}{\|\mathbf{s_B}\|^2} \tag{2.11}$$

, where $\|.\|$ denotes the norm of its argument. In order to derive theoretical expression of SKGR, the assumption is made that h_{AB} and h_{BA} are Gaussian random variables with zero mean and variance σ_{AB}^2 and σ_{BA}^2 ($\sigma_{AB}^2 = \sigma_{BA}^2$), respectively, and n_A and n_B are zero mean additive Gaussian noise with variance σ_A^2 and σ_B^2 (all additive Gaussian noise are independent of each other). Therefore, $\tilde{h}_{AB}$ is a Gaussian random variable with zero mean and variance $\sigma_{AB}^2 + \sigma_B^2/\left\|S_A\right\|^2$. Similarly, $\tilde{h}_{BA}$ is a Gaussian random variable with zero mean and variance $\sigma_{BA}^2 + \sigma_A^2/\left\|S_B\right\|^2$.

The reasonable assumption can be made that the transmit power of Alice and Bob are equal, thereby denoted as P. Therefore, $\tilde{h}_{AB}$ and $\tilde{h}_{BA}$ can be rewritten as $\sigma_{AB}^2 + \sigma_B^2/(T_A P)$ and $\sigma_{BA}^2 + \sigma_A^2/(T_B P)$ since $\left\|S_A\right\|^2 = T_A P$ and $\left\|S_B\right\|^2 = T_B P$. According to the definition of SKGR, theoretical expression of R_{P2P} can be written as follows.

Assuming the estimated $\tilde{h}_{AB}$ and $\tilde{h}_{BA}$ are Gaussian random variables with zero mean and variance σ_1^2 and $T_A = T_B = T$, information-theoretic definition of SKGR, the

typical performance metric, corresponds to [18]

$$R_{P2P} = \frac{1}{T} I(\tilde{h}_{AB}; \tilde{h}_{BA}) = \frac{1}{2T} \log\left(1 + \frac{\sigma_1^4 P^2 T^2}{4(\sigma^4 + \sigma^2\sigma_1^2)PT}\right) \tag{2.12}$$

where σ^2 denotes variance of Gaussian noise, and P is denoted as the transmit power. T is the time taken for channel estimation and is assumed to be much smaller than the channel coherence time T_c ($T << T_c$).

In order to generate uniformly distributed common secret key between Alice and Bob with the rate shown in Eq. 2.12, a Slepian-Wolf source coding technique is employed to send helper information between terminals through the public channel [50]. More specifically, in a random time period T_R, Alice observes $n = \lfloor T_R/T \rfloor$ of random variable $\tilde{h}_{AB}$, where $\lfloor . \rfloor$ denotes the largest integer that is smaller than its argument, resulting in a vector $\tilde{h}_{AB} = [\tilde{h}^{\delta}_{AB}(1), \ldots, \tilde{h}^{\delta}_{AB}(n)]$ to collect all observed random variables, where $\tilde{h}_{AB}(i)$ is quantized with quantization interval δ as $\tilde{h}^{\delta}_{AB}(i)$. $\tilde{h}^{\delta}_{AB}(1)$ are independent from each other. Using similar notation, Bob observes vector $\tilde{h}_{BA} = [\tilde{h}^{\delta}_{BA}(1), \ldots, \tilde{h}^{\delta}_{BA}(n)]$. Alice randomly divides the typical sequence $\tilde{h}_{AB}$ into non-overlapping bins. According to the information theory, each bin should have $2^{nI(\tilde{h}_{AB};\tilde{h}_{BA})}$ typical sequence and each sequence has two variables: bin number and index within the bin. Therefore, after observing the vector $\tilde{h}_{AB}$, Alice uses the index of this sequence within its bin as the key and sends the bin number as helper information ($H(\tilde{h}_{AB}, \tilde{h}_{BA})$ bits information) to Bob through the public channel. After Bob receives the helper data from the public channel, he can combine the helper data and his own observation $\tilde{h}_{BA}$) to recover $\tilde{h}_{AB}$ with probability close to 1. Hence, Bob can recover the key. Similarly, Alice can recover the $\tilde{h}_{BA}$ and key using the same method. The bin number and index within each bin can also be shown to be independent of each other. Therefore, even Eve has full access to the public channel, meaning that the transmitted bin number can be observed through the public channel. Eve is unaware

of the generated key. The quantization level is set to zero in order to achieve SKGR, as shown in Eq. 2.12.

According to Eq. 2.12, transmit power P and coherence time T are two significant factors for SKGR. SKGR increases at an order of $\frac{1}{2T}\log P$ with increased transmit power P. With increased coherence time T, meaning that the channel is more stable (channel changes slowly), SKGR decreases at an order of $\frac{1}{2T}\log T$. This discussion indicates that the next stage of PHY-SKG techniques evolution has two primary directions: (1) exploitation of common randomness in reciprocal channels using advanced network technology, such as MIMO, and (2) utilization of transmit power efficiency using advanced power allocation algorithm. This chapter primarily focuses on the first direction (i.e., SKG strategies in MIMO and co-op MIMO networks).

2.3 SKG Performance Metrics

This subsection introduces three frequently used SKG performance metrics [51].

2.3.1 Secret key generation rate

SKGR quantifies the rate at which legitimate users can agree upon a shared key sequence by exchanging messages via a public channel. For instance, considering an SKG scenario based on RSS, both Alice and Bob record RSS values of their corresponding signals in a specific time period t. A quantizer is employed to convert their RSS measurements into random bit strings with length L_t. Consequently, the SKGR is equal to L_t/t. According to the above analysis, SKGR measures the efficiency of an SKG scheme, but it is highly dependent on common randomness over wireless communication channels as well as SKG strategy.

2.3.2 Secret key disagreement probability

Prior defining secret key disagreement probability (SKDP), the definition of key disagreement should be introduced first. Considering a general SKG process based on RSS, assume both Alice and Bob have estimated their random bit strings (K_A, K_B). A reconciliation technique is deployed to assist Alice and Bob agree on an identical secret key. The difference between (K_A, K_B) is called key disagreement. Therefore, SKDP refers to the probability of the presence of different bits in the key bit string prior to error correction. A high SKDP dramatically decreases efficiency of key generation protocol and causes the protocol to fail due to failure of key reconciliation [25]. Experiments in [52] showed that SKDP of SKG schemes is influenced by variations in the wireless communication channel. In a stationary environment, SKG schemes demonstrate an unsatisfactory SKDP due to lack of common randomness in channel fading. For more detailed discussion of SKDP, readers are referred to [52] [20].

2.3.3 Secret key bit randomness

A cryptographic key should be substantially random to prevent an adversary from cracking the key with low time complexity. Randomness of a bit sequence can be measured using a National Institute of Standards and Technology (NIST) tes [53]. If the p value is greater than 0.01, the sequence is random. For traditional SKG schemes, a trade-off exists between secret key bit randomness (SKBR) and SKGR, in which keys should be extracted at different channel coherence time intervals to ensure SKBR since sampling the channel at a too high frequency produces a key with low entropy.

It is important to note that all performance metrics (SKDP, SKBR and SKGR) are impacted by limited common randomness in reciprocal channels. Consequently, the effect of artificially increasing common randomness using advanced network technology such as MIMO must be quantified. One goal of this dissertation is to evaluate the

maximum secret key generation rate (MSKGR is defined in following section) of various wireless communication networks, such as point-to-point communication network, MIMO, and coop MIMO.

2.4 Co-op MIMO networks

As discussed in previous research [54] [55] [56] [57], MIMO architectures have demonstrated potential to significantly improve throughput, diversity, and range of wireless communication systems. However, original MIMO systems require the transmitter and receiver of a communication link to be equipped with multiple antennas that must be separated by at least half the operating wavelength in order to prevent spatial and temporal interference. In practice, many wireless devices may not be able to support multiple antennas due to dimension, budget, and hardware limitations. Those limitations prevent such devices from efficiently taking advantage of MIMO gains. In order to reap the benefits of MIMO network without restricted by those limitations, co-op MIMO is proposed. Co-op MIMO fundamentally groups multiple devices into virtual antenna arrays (VAAs) in order to emulate MIMO communications. A detailed model of co-op MIMO is presented in Fig. 2.3. As shown in Fig. 2.3, the base station tower with multiple antennas is denoted as T_x with coverage region represented as a large circle with radius r_T. Mobile phones are denoted as U (target receivers with one antenna available) and single antenna bases are relay nodes that include picocell, femtocell, and other users (denoted as R_1 and R_2 in the Fig. 2.3). As communication is initiated, T_x broadcasts messages to the entire coverage region. Target user U groups all available relay nodes in a specific region, denoted as a small circle with radius r_D, into VAAs in order to emulate MIMO communication.

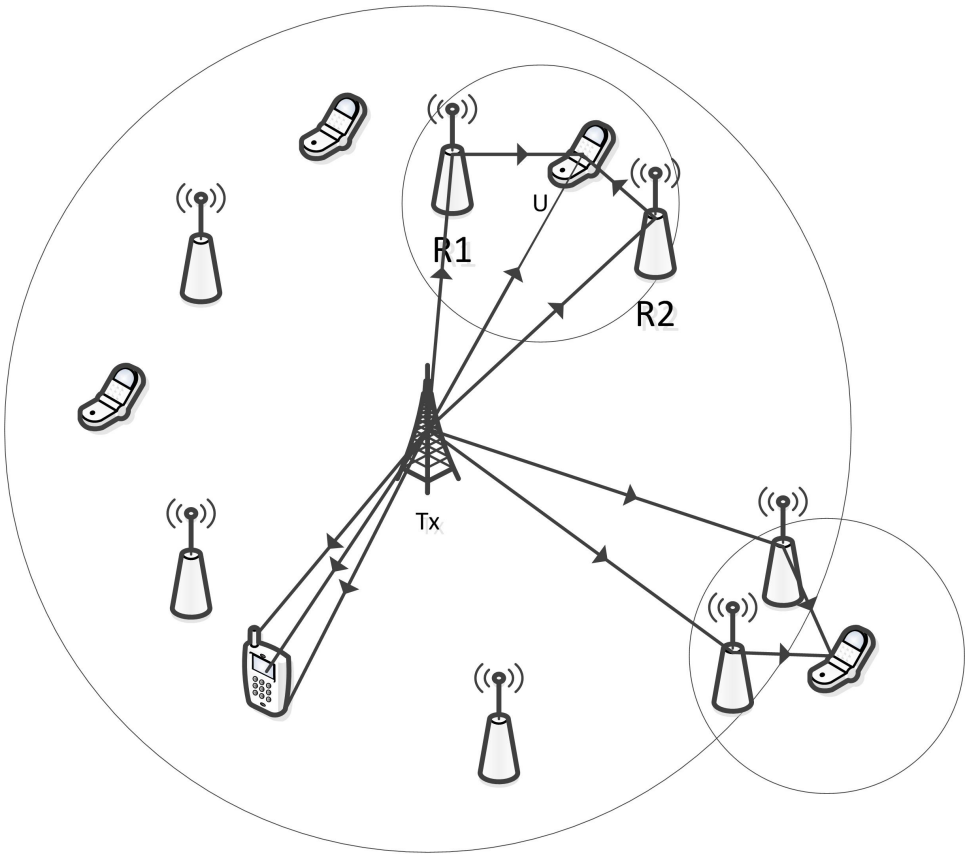

Figure 2.3: *A Co-op MIMO network model*

Chapter 3

Cooperative MIMO based Physical Layer Secret Key Generation Scheme

Relay nodes, which are low-power nodes that provide enhanced coverage and capacity at low cost, are an integral part of the LTE-A standard. In order to boost throughput, co-op MIMO techniques are proposed wherein relay nodes close to end users are recruited to operate as VAAs. In this chapter, we exploit the coop MIMO structure to design and implement a physical layer security scheme for LTE-A networks. Specifically, we consider two relay-based co-op MIMO architectures and propose novel secret key generation (SKG) schemes for those cases. Information-theoretic results regarding SKGR are presented. Results indicate that relay-based co-op MIMO schemes, traditionally used to enhance LTE-A network throughput and coverage, can also increase SKGR. Our work demonstrates the viability of SKG technique as a potential physical layer security scheme for LTE-A networks.

3.1 Introduction

In 2009, 3rd Generation Partnership Project (3GPP) proposed a new LTE-A standard that supports higher data rates, better coverage, and lower latencies. LTE-A incorporates picocells, femtocells, relays, and remote radio heads within a macrocell layout. These low-power nodes provide enhanced coverage and capacity in target areas at low cost. Additionally, it is possible to reap the capacity and performance benefits offered by an multiple input multiple output (MIMO) system, using co-op MIMO schemes that utilize distributed antennas on multiple devices to work together as VAAs. The question we seek to address in this work is the following "Is it possible to exploit relay-based co-op MIMO architectures to enhance security of LTE-A networks at physical layer? "

While a number of distinguished studies have been conducted on ways to improve LTE-A network performance, security issues have often been neglected. Due to the broadcast nature of wireless channels, wireless networks are threatened by eavesdropping, message modification, and node impersonation. In order to protect the confidentiality, integrity, and authenticity of transmitted data, secrecy at PHY-layer has recently attracted considerable attention. Following Shannon's fundamental work on information-theoretic security [58], Wyner introduced a new wire-tap channel model in [10]. Thereafter, Maurer presented a strategy that allows joint development of secret keys between transmitter and receiver with the help of a public and error-free feedback channel [11]. Since then the two main thrust areas in information theoretic security research are (1) keyless security based on the work of by Wyner, and (2) PHY-layer secret key generation (PHY-SKG) following the work of Shannon and Maurer. In this chapter, we focus on the latter problem. For wireless channel reciprocity based PHY-SKG technique, secret keys are generated by using common randomness that sources extract from channels between parties in a wireless communication system.

Eavesdroppers experience independent physical channels from legitimate users as long as they are a few wavelengths away from legitimate nodes. This is common in wireless networks. Therefore, keys are secure with an information theoretic guarantee [19].

Compared to a classical SKG algorithm, such as Diffie-Hellman protocol, PHY-SKG technique has the following advantages: (1) a computationally bounded adversary does not need to be assumed since secret keys are generated based on channel randomness [20]; (2) PHY-SKG avoids the requirement of key management, which is a challenging problem in traditional key generation schemes [21]; (3) secret keys can be dynamically replenished as wireless channels vary over time [19]. Additionally, PHY-SKG can be used to enhance existing security schemes as it operates independently of higher layers security schemes. Our work is based on the hypothesis that relay-based co-op MIMO, employed by the LTE-A network, can be leveraged to improve SKG performance and PHY-layer security.

However, previous studies of PHY-SKG indicate that low secret key generation rate (SKGR), a critical performance metric, is the primary limitation of PHY-SKG. This is because, the security strength of secret key is theoretically proportional to key length [22]. Therefore, the next stage of PHY-SKG evolution involves the exploitation of common randomness in reciprocal channels using advanced network technology, e.g, MIMO, etc.

In this work, we consider two practical scenarios of relay-based co-op MIMO in LTE-A networks: (1) no direct communication between source and destination, and (2) direct communication of source with destination. In this chapter, we restrict ourselves to a specific communication pair in both scenarios. However, our analysis is easily extended to the entire network. Two novel SKG schemes are presented. For both scenarios, we evaluate the information-theoretic expression of SKGR. Numerical results corresponding to theoretical analysis are also provided.

3.2 Introduction

3.2.1 Scenario 1: No direct communication between source S and destination D

In this subsection, we consider a communication scenario in which the end user (destination) cannot communicate with the source due to distance. As shown in 3.1, assume source S has N antennas. Destination D is a mobile user with one antenna. Since source S cannot communicate directly with destination D, M low-power relay nodes are deployed in this scenario. We assume that all relay nodes employ one antenna. In this chapter, we only focus on common randomness sharing, overheads, i.e., synchronization overhead of relay nodes, are not considered.

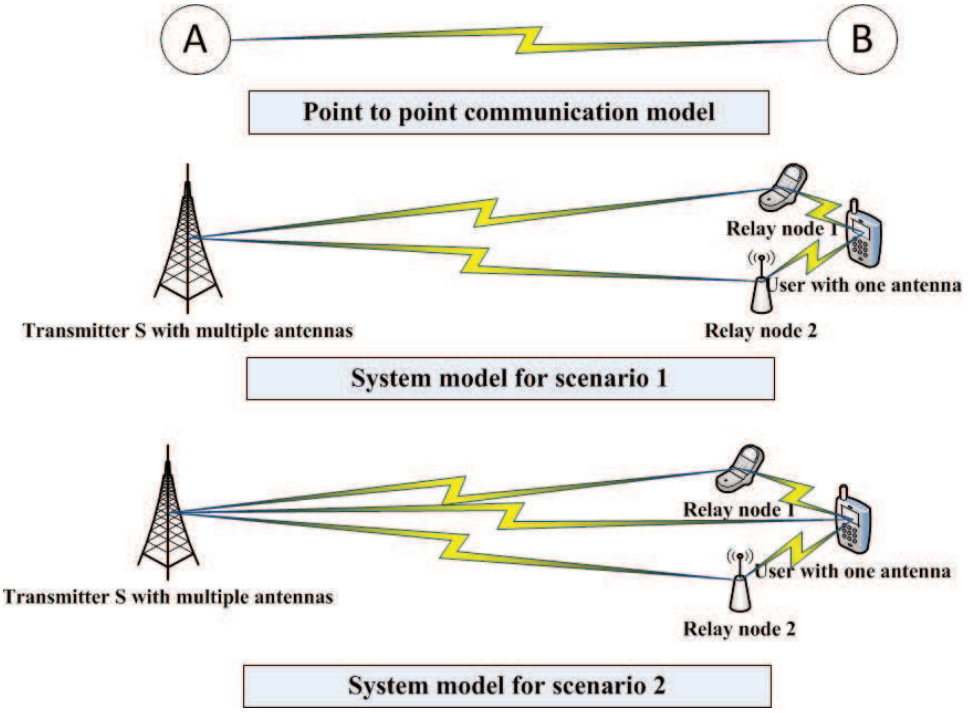

Figure 3.1: *System Model of PHY-SKG Scheme*

In order to evaluate the SKGR for this scenario, we propose a novel algorithm. Following the time frame described in Table 3.1, in the first timeslot T_1, S sends known

Table 3.1: *SKG schemes for Scenario* 1

Channel Estimation	
Timeslots	Action
timeslot 1	S sends known sequence matrix $\mathbf{S_S}$ to relay nodes with power P
timeslot 2	Relay nodes forward received sequence to D with total power equal to P. Then, D can estimate a virtual channel $\tilde{\mathbf{h}}_{\mathbf{SD}}$
timeslot 3	D sends a known sequence $\mathbf{s_D}$ to relay nodes with power P
timeslot 4	Relay nodes forward received sequence to S with total power equal to P. Therefore, S can estimate a virtual channel $\tilde{\mathbf{h}}_{\mathbf{DS}}$
Key Agreement	
Steps	Action
	S and D agree on keys $\mathbf{k_{SD}}$ from$(\tilde{\mathbf{h}}_{\mathbf{SD}}, \tilde{\mathbf{h}}_{\mathbf{DS}})$ using public channel.

matrix $\mathbf{S_s}$ with dimension of NXL to relay nodes. L ($L > N$) is denoted as the length of known sequence transmitted by each antenna. Assuming all antenna transmit sequences are orthogonal to each other, relay nodes received signal is

$$\mathbf{Y_{SR}} = \mathbf{H_{SR}}\mathbf{S_S} + \mathbf{N_R}, \tag{3.1}$$

where, $\mathbf{H_{SR}}$ and $\mathbf{N_R}$ denote the communication channel matrix between S and R and Gaussian noise matrix at relay nodes with dimensions MXN and MXL, respectively.

In the second timeslot T_2, relay nodes forward received information $\mathbf{S_{RD}}$ to D. The channel model can be written as:

$$\mathbf{y_{RD}} = \mathbf{h_{RD}}\mathbf{S_{RD}} + \mathbf{n_D} \tag{3.2}$$

Since the primary role of relay nodes is to forward the received sequence to destination, the reasonable assumption can be made that $\mathbf{S_{RD}} = \mathbf{Y_{SR}}$. Therefore, a virtual communication channel is constructed between S and D with the assistance of relay nodes. The received signal at D can be written as:

$$\mathbf{y_{RD}} = \mathbf{h_{RD}}\mathbf{H_{SR}}\mathbf{S_s} + \mathbf{h_{RD}}\mathbf{N_R} + \mathbf{n_D}, \tag{3.3}$$

where, $\mathbf{h_{RD}}$ and $\mathbf{n_D}$ denote the channel vector between relay nodes and D and Gaussian noise vector at D with dimension $1XM$ and $1XL$, respectively.

In the same manner, in the third slot T_3, D sends a known sequence (row vector) $\mathbf{s_D}$ of length L to relay nodes. The received signal at relay nodes is:

$$\mathbf{Y_{DR}} = \mathbf{h_{DR}}\mathbf{s_D} + \mathbf{N_R} \tag{3.4}$$

where, $\mathbf{h_{DR}}$ is $MX1$ channel vector between D and relay nodes.

In the last timeslot T_4, relay nodes forward received information $\mathbf{S_{RS}}(=\mathbf{Y_{DR}})$ to S to generate the virtual communication channel between D and S. Therefore, the received signal at S can be expressed as:

$$\mathbf{Y_{RS}} = \mathbf{H_{RS}}\mathbf{S_{RS}} + \mathbf{N_S} = \mathbf{H_{RS}}\mathbf{h_{DR}}\mathbf{s_D} + \mathbf{H_{RS}}\mathbf{N_R} + \mathbf{N_S} \tag{3.5}$$

where, $\mathbf{H_{RS}}$ is NXM channel matrix between relay nodes and S, and $\mathbf{N_S}$ denotes MXL Gaussian noise matrix at S.

Let $\mathbf{n_D^{'}} = \mathbf{h_{RD}}\mathbf{N_R} + \mathbf{n_D}$ and $\mathbf{N_S}^{'} = \mathbf{H_{RS}}\mathbf{N_R} + \mathbf{N_S}$. Assuming $T_1 + T_2 = T_3 + T_4 = T/2$, the virtual channel between D and S can be estimated as:

$$\tilde{\mathbf{h}}_{\mathbf{DS}} = \mathbf{Y_{RS}}\frac{\mathbf{s_D^T}}{\|\mathbf{s_D}\|^2} = \mathbf{H_{RS}}\mathbf{h_{DR}} + \mathbf{N_S}^{'}\frac{\mathbf{s_D^T}}{\|\mathbf{s_D}\|^2} = \begin{bmatrix} \sum_{i=1}^{M} h_{R_iS_1}h_{DR_i} + \frac{1}{TP}\sum_{l=1}^{L}(\sum_{i=1}^{M} h_{R_iS_1}N_{R_{i,l}} + N_{S_{1,l}})S_{D_l} \\ \sum_{i=1}^{M} h_{R_iS_2}h_{DR_i} + \frac{1}{TP}\sum_{l=1}^{L}(\sum_{i=1}^{M} h_{R_iS_1}N_{R_{i,l}} + N_{S_{2,l}})S_{D_l} \\ \vdots \\ \sum_{i=1}^{M} h_{R_iS_N}h_{DR_i} + \frac{1}{TP}\sum_{l=1}^{L}(\sum_{i=1}^{M} h_{R_iS_1}N_{R_{i,l}} + N_{S_{N,l}})S_{D_l} \end{bmatrix} \tag{3.6}$$

Similarly, the virtual channel between S and D can be estimated by using a least

square estimator as:

$$\tilde{\mathbf{h}}_{\mathbf{SD}} = \mathbf{h}_{\mathbf{SD}} + \mathbf{n}'_{\mathbf{D}}\mathbf{S}^{\dagger}_{\mathbf{S}} = \mathbf{h}_{\mathbf{RD}}\mathbf{H}_{\mathbf{SR}} + \frac{N}{TP}\mathbf{n}'_{\mathbf{D}}\mathbf{S}^{\mathbf{T}}_{\mathbf{S}} = \begin{bmatrix} \sum_{i=1}^{M} h_{R_iD}h_{S_1R_i} + \frac{N}{TP}\sum_{l=1}^{L}(\sum_{i=1}^{M} h_{R_iD}N_{R_{i,l}} + N_{D_l})S_{1,l} \\ \sum_{i=1}^{M} h_{R_iD}h_{S_2R_i} + \frac{N}{TP}\sum_{l=1}^{L}(\sum_{i=1}^{M} h_{R_iD}N_{R_{i,l}} + N_{D_l})S_{2,l} \\ \cdot \\ \cdot \\ \cdot \\ \sum_{i=1}^{M} h_{R_iD}h_{S_NR_i} + \frac{N}{TP}\sum_{l=1}^{L}(\sum_{i=1}^{M} h_{R_iD}N_{R_{i,l}} + N_{D_l})S_{N,l} \end{bmatrix}^{T} \tag{3.7}$$

Here, $\mathbf{S}^{\dagger}_{\mathbf{S}}$ denotes pseudo inverse matrix of $\mathbf{S}_{\mathbf{S}}$. The above analysis demonstrates that a secret key can be generated with rate:

$$R_{SD} = \frac{1}{T} I(\tilde{h}_{SD}; \tilde{h}_{DS}). \tag{3.8}$$

If we assume: (1) all channel gains are zero mean independent normal distribution; (2) $\mathbf{n}_{\mathbf{D}}$, $\mathbf{N}_{\mathbf{R}}$, and $\mathbf{N}_{\mathbf{S}}$ are zero mean independent Gaussian noise; and (3) additive noises and channel gains are uncorrelated, we obtain the SKGR for Scenario 1 as follows:

$$\begin{bmatrix} \sum_{i=1}^{M} \sigma^2_{R_iD}\sigma^2_{S_1R_i} + \frac{N}{TP}\sum_{l=1}^{L}(\sum_{i=1}^{M} \sigma^2_{R_iD}\sigma^2_{R_{i,l}} + \sigma^2_{D_l}) & \cdots & 0 \\ 0 & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & 0 \\ 0 & \cdots & \sum_{i=1}^{M} \sigma^2_{R_iD}\sigma^2_{S_NR_i} + \frac{N}{TP}\sum_{l=1}^{L}(\sum_{i=1}^{M} \sigma^2_{R_iD}\sigma^2_{R_{i,l}} + \sigma^2_{D_l}) \end{bmatrix} \tag{3.9}$$

$$\begin{bmatrix} \sum_{i=1}^{M} \sigma^2_{R_iS_1}\sigma^2_{DR_i} + \frac{1}{TP}\sum_{l=1}^{L}(\sum_{i=1}^{M} \sigma^2_{R_iS_1}\sigma^2_{R_{i,l}} + \sigma^2_{S_{1,l}}) & \cdots & 0 \\ 0 & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & 0 \\ 0 & \cdots & \sum_{i=1}^{M} \sigma^2_{R_iS_N}\sigma^2_{DR_i} + \frac{1}{TP}\sum_{l=1}^{L}(\sum_{i=1}^{M} \sigma^2_{R_iS_N}\sigma^2_{R_{i,l}} + \sigma^2_{S_{N,l}}) \end{bmatrix} \tag{3.10}$$

Theorem 1. The SKGR for Scenario 1 corresponds to:

$$R_{SD} = -\frac{1}{2T}\sum_{j=1}^{N} log(1 - \frac{a_j TP}{a_j TP + c_j}\frac{a_j TP}{a_j TP + Nb}) \tag{3.11}$$

where, $a_j = \sum_{i=1}^{M} \sigma_{R_i D}^2 \sigma_{S_j R_i}^2$, $b = \sum_{l=1}^{L}(\sum_{i=1}^{M} \sigma_{R_i D}^2 \sigma_{R_{i,l}}^2 + \sigma_{D_l}^2)$ and $c_j = \sum_{l=1}^{L}(\sum_{i=1}^{M} \sigma_{R_i S_j}^2 \sigma_{R_{i,l}}^2 + \sigma_{S_{j,l}}^2)$.

Since $\tilde{\mathbf{h}}_{\mathbf{SD}}$ and $\tilde{\mathbf{h}}_{\mathbf{DS}}$ are multivariate Gaussian, results from [59] can be used to write the mutual information between $\tilde{\mathbf{h}}_{\mathbf{SD}}$ and $\tilde{\mathbf{h}}_{\mathbf{DS}}$:

$$I(\tilde{\mathbf{h}}_{\mathbf{SD}}; \tilde{\mathbf{h}}_{\mathbf{DS}}) = -\frac{1}{2} log(\frac{\left|\mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{SD}},\tilde{\mathbf{h}}_{\mathbf{SD}}}\right| \left|\mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{DS}},\tilde{\mathbf{h}}_{\mathbf{DS}}}\right|}{|\mathbf{C}|}) \tag{3.12}$$

where, $|\cdot|$ represents the determinant of matrix, $\mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{SD}},\tilde{\mathbf{h}}_{\mathbf{SD}}}$ is the auto-correlation matrix of $\tilde{\mathbf{h}}_{\mathbf{SD}}$, as shown in Eq. 3.9 and Eq. 3.10 (located at the beginning of next page). $|\mathbf{C}|$ corresponds to:

$$|\mathbf{C}| = \begin{vmatrix} \mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{SD}},\tilde{\mathbf{h}}_{\mathbf{SD}}} & \mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{SD}},\tilde{\mathbf{h}}_{\mathbf{DS}}} \\ \mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{DS}},\tilde{\mathbf{h}}_{\mathbf{SD}}} & \mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{DS}},\tilde{\mathbf{h}}_{\mathbf{DS}}} \end{vmatrix} \tag{3.13}$$

According to [27], $\mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{SD}},\tilde{\mathbf{h}}_{\mathbf{DS}}} = \mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{DS}},\tilde{\mathbf{h}}_{\mathbf{SD}}} = \mathbf{C}_{\mathbf{h}_{\mathbf{SD}},\mathbf{h}_{\mathbf{SD}}} = \mathbf{C}_{\mathbf{h}_{\mathbf{DS}},\mathbf{h}_{\mathbf{DS}}}$. The SKGR of channel between S and D can be written as:

$$\begin{aligned} R_{SD} &= -\frac{1}{2T} log \\ &(\left|\mathbf{I} - \mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{DS}},\tilde{\mathbf{h}}_{\mathbf{DS}}}{}^{-1} \mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{DS}},\tilde{\mathbf{h}}_{\mathbf{SD}}} \mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{SD}},\tilde{\mathbf{h}}_{\mathbf{SD}}}{}^{-1} \mathbf{C}_{\tilde{\mathbf{h}}_{\mathbf{SD}},\tilde{\mathbf{h}}_{\mathbf{DS}}}\right|) \end{aligned} \tag{3.14}$$

A combination of Eqs. 3.9, 3.10, and 3.12 produces:

$$R_{SD} = -\frac{1}{2T} log(\prod_{j=1}^{N}(1 - \frac{a_j TP}{a_j TP + c_j}\frac{a_j TP}{a_j TP + Nb})) \tag{3.15}$$

3.2.2 Scenario 2: S with multiple antennas and direct communication with D

In this subsection, we consider a scenario in which no restriction exists between destination D, source S and relay nodes, i.e., they can spontaneously communicate with each other. As shown in Fig. 3.1, M relay nodes are deployed, all relay nodes employ one antenna. N antennas are assembled with source S. The destination is a mobile device with one antenna. Without considering overheads, we propose another SKG algorithm for this scenario and evaluate the SKGR.

Following the time frame shown in Table 3.2 , in the first timeslot T_1, each antenna of S sends a known matrix $\mathbf{S_s}$ to relay nodes and D. Assuming the sequences are orthogonal to each other, the signal received at D is:

$$\mathbf{y_{SD}} = \mathbf{h_{SD}}\mathbf{S_S} + \mathbf{n_D} \tag{3.16}$$

where $\mathbf{h_{SD}}$ and $\mathbf{S_S}$ denote the channels vector between S and D and known sequences matrix sent by S, respectively. $\mathbf{n_D}$ is the Gaussian noise vector at D. Using similar notation, relay nodes receive:

$$\mathbf{Y_{SR}} = \mathbf{H_{SR}}\mathbf{S_S} + \mathbf{N_R} \tag{3.17}$$

Assuming $T_1 = T_2 = T_3 = T/3$, the estimated channel $\tilde{\mathbf{h}}_{\mathbf{SD}}$ and $\tilde{\mathbf{H}}_{\mathbf{SR}}$ can be written

Table 3.2: *SKG schemes for Scenario* 2

Channel Estimation	
Timeslots	Action
timeslot 1	S sends known sequence matrix $\mathbf{S_S}$ to D and relay nodes with power P. Therefore, D and relay nodes can estimates $\tilde{\mathbf{h}}_{\mathbf{SD}}$ and $\tilde{\mathbf{H}}_{\mathbf{SR}}$, respectively
timeslot 2	D sends a known sequence $\mathbf{s_D}$ to S and relay nodes with power P. Then, S and relay nodes can estimate $\tilde{\mathbf{h}}_{\mathbf{DS}}$ and $\tilde{\mathbf{h}}_{\mathbf{DR}}$, respectively.
timeslot 3	Relay nodes send known sequence matrix $\mathbf{S_R}$ to S and D with power P. Thus, S and D can estimate $\tilde{\mathbf{H}}_{\mathbf{RS}}$ and $\tilde{\mathbf{h}}_{\mathbf{RD}}$, respectively.
Key Agreement	
Steps	Action
step 1	S and D agree on keys $\mathbf{k_{SD}}$ from $(\tilde{\mathbf{h}}_{\mathbf{SD}}, \tilde{\mathbf{h}}_{\mathbf{DS}})$ using public channel.
step 2	S and relay nodes agree on keys $\mathbf{k_{SR}}$ from $(\tilde{\mathbf{h}}_{\mathbf{SR}}, \tilde{\mathbf{h}}_{\mathbf{RS}})$ using public channel.
step 3	D and relay nodes agree on keys $\mathbf{k_{DR}}$ from $(\tilde{\mathbf{h}}_{\mathbf{DR}}, \tilde{\mathbf{h}}_{\mathbf{RD}})$ using public channel.
step 4	Setting $(\mathbf{k_{SD}}, \min(\mathbf{k_{SR}}, \mathbf{k_{DR}}))$ as the key, where (K_i, K_j) denotes the concatenation of K_i and K_j

as:

$$\tilde{\mathbf{h}}_{\mathbf{SD}} = \mathbf{h}_{\mathbf{SD}} + \frac{3N}{TP}\mathbf{n}_{\mathbf{D}}\mathbf{S}_{\mathbf{S}}^{\mathbf{T}} = \begin{bmatrix} h_{S_1D} + \frac{3N}{TP}\sum_{l=1}^{L} N_{D_l}S_{1,l} \\ . \\ . \\ . \\ h_{S_{t_N}D} + \frac{3N}{TP}\sum_{l=1}^{L} N_{D_l}S_{N,l} \end{bmatrix}^T \tag{3.18}$$

$$\tilde{\mathbf{H}}_{\mathbf{SR}} = \mathbf{H}_{\mathbf{SR}} + \frac{3N}{TP}\mathbf{N}_{\mathbf{R}}\mathbf{S}_{\mathbf{S}}^{\mathbf{T}} = \begin{bmatrix} h_{S_1R_1} + \frac{3N}{TP}\sum_{l=1}^{L} N_{R_{1,l}}S_{1,l} & . & h_{S_NR_1} + \frac{3N}{TP}\sum_{l=1}^{L} N_{R_{1,l}}S_{N,l} \\ . & . & . \\ . & . & . \\ . & . & . \\ h_{S_1R_M} + \frac{3N}{TP}\sum_{l=1}^{L} N_{R_{M,l}}S_{1,l} & . & h_{S_NR_M} + \frac{3N}{TP}\sum_{l=1}^{L} N_{R_{M,l}}S_{N,l} \end{bmatrix}^T \tag{3.19}$$

Similarly, at the second timeslot T_2, D sends $\mathbf{s_D}$ with length L to relay nodes and S. Received signals at S and relay nodes are:

$$\mathbf{Y}_{\mathbf{DS}} = \mathbf{h}_{\mathbf{DS}}\mathbf{s}_{\mathbf{D}} + \mathbf{N}_{\mathbf{S}} \tag{3.20}$$

$$\mathbf{Y}_{\mathbf{DR}} = \mathbf{h}_{\mathbf{DR}}\mathbf{s}_{\mathbf{D}} + \mathbf{N}_{\mathbf{R}} \tag{3.21}$$

In the same manner, estimated channel $\tilde{\mathbf{h}}_{\mathbf{DS}}$ and $\tilde{\mathbf{h}}_{\mathbf{DR}}$ are:

$$\tilde{\mathbf{h}}_{\mathbf{DS}} = \mathbf{Y}_{\mathbf{DS}}\frac{\mathbf{s}_{\mathbf{D}}^{\mathbf{T}}}{\|\mathbf{s}_{\mathbf{D}}\|^2} = \begin{bmatrix} h_{DS_{t_1}} + \frac{3}{TP}\sum_{l=1}^{L} N_{S_{1,l}}S_{D_l} \\ . \\ . \\ . \\ h_{DS_{t_N}} + \frac{3}{TP}\sum_{l=1}^{L} N_{S_{N,l}}S_{D_l} \end{bmatrix} \tag{3.22}$$

$$\tilde{\mathbf{h}}_{\mathbf{DR}} = \mathbf{Y}_{\mathbf{DR}} \frac{\mathbf{s}_{\mathbf{D}}^{\mathbf{T}}}{\|\mathbf{s}_{\mathbf{D}}\|^2} = \begin{bmatrix} h_{DR_1} + \frac{3}{TP} \sum_{l=1}^{L} N_{R_{1,l}} S_{D_l} \\ . \\ . \\ . \\ h_{DR_N} + \frac{3}{TP} \sum_{l=1}^{L} N_{R_{N,l}} S_{D_l} \end{bmatrix} \tag{3.23}$$

In the last timeslot T_3, relay nodes send $\mathbf{S_R}$ to S and D. Assuming all L length sequences are orthogonal, received signals are:

$$\mathbf{Y_{RS}} = \mathbf{H_{RS}} \mathbf{S_R} + \mathbf{N_S} \tag{3.24}$$

$$\mathbf{y_{RD}} = \mathbf{h_{RD}} \mathbf{S_R} + \mathbf{n_D} \tag{3.25}$$

Using the same method, the estimated channels, $\tilde{\mathbf{h}}_{\mathbf{RD}}$ and $\tilde{\mathbf{H}}_{\mathbf{RS}}$, can be written as:

$$\tilde{\mathbf{h}}_{\mathbf{RD}} = \mathbf{h_{RD}} + \frac{3M}{TP} \mathbf{n_D} \mathbf{S_R^T} = \begin{bmatrix} h_{R_1 D} + \frac{3M}{TP} \sum_{l=1}^{L} N_{D_l} S_{R_{l,l}} \\ . \\ . \\ . \\ h_{R_M D} + \frac{3M}{TP} \sum_{l=1}^{L} N_{D_l} S_{R_{M,l}} \end{bmatrix}^T \tag{3.26}$$

$$\tilde{\mathbf{H}}_{\mathbf{RS}} = \mathbf{H_{RS}} + \frac{3M}{TP} \mathbf{N_S} \mathbf{S_R^T} =$$

$$\begin{bmatrix} h_{R_1 S_1} + \frac{3M}{TP} \sum_{l=1}^{L} N_{S_{1,l}} S_{R_{1,l}} & . & h_{R_M S_1} + \frac{3M}{TP} \sum_{l=1}^{L} N_{S_{1,l}} S_{R_{M,l}} \\ . & . & . \\ . & . & . \\ . & . & . \\ h_{R_1 S_N} + \frac{3M}{TP} \sum_{l=1}^{L} N_{S_{N,l}} S_{R_{1,l}} & . & h_{R_M S_N} + \frac{3M}{TP} \sum_{l=1}^{L} N_{S_{N,l}} S_{R_{M,l}} \end{bmatrix} \tag{3.27}$$

With assumptions similar to that in the previous scenario, the SKGR for Scenario 2 is given by theorem below:

Theorem 2. The SKGR for Scenario 2 corresponds to:

$$R_{co-op} = \frac{1}{T} \left\{ I\left(\tilde{\mathbf{h}}_{\mathbf{SD}}; \tilde{\mathbf{h}}_{\mathbf{DS}}\right) + min\left\{ I\left(\tilde{\mathbf{H}}_{\mathbf{SR}}; \tilde{\mathbf{H}}_{\mathbf{RS}}\right), I\left(\tilde{\mathbf{h}}_{\mathbf{DR}}; \tilde{\mathbf{h}}_{\mathbf{RD}}\right)\right\}\right\} \tag{3.28}$$

where, mutual information terms are:

$$I\left(\tilde{\mathbf{h}}_{\mathbf{SD}}; \tilde{\mathbf{h}}_{\mathbf{DS}}\right) = -\frac{1}{2}\sum_{j=1}^{N} log \left(1 - \frac{\sigma^2_{S_jD} TP}{\sigma^2_{S_jD} TP + 3N\sum_{l=1}^{L}\sigma^2_{D_l}} \frac{\sigma^2_{S_jD} TP}{\sigma^2_{S_jD} TP + 3\sum_{l=1}^{L}\sigma^2_{S_{j,l}}}\right) \tag{3.29}$$

$$I\left(\tilde{\mathbf{h}}_{\mathbf{DR}}; \tilde{\mathbf{h}}_{\mathbf{RD}}\right) = -\frac{1}{2}\sum_{i=1}^{M} log \left(1 - \frac{\sigma^2_{DR_i} TP}{\sigma^2_{DR_i} TP + 3M\sum_{l=1}^{L}\sigma^2_{D_l}} \frac{\sigma^2_{DR_i} TP}{\sigma^2_{DR_i} TP + 3\sum_{l=1}^{L}\sigma^2_{R_{i,l}}}\right) \tag{3.30}$$

$$I\left(\tilde{\mathbf{H}}_{\mathbf{SR}}; \tilde{\mathbf{H}}_{\mathbf{RS}}\right) = -\frac{1}{2}\sum_{i=1}^{M}\sum_{j=1}^{N} log \left(1 - \frac{\sigma^2_{S_jR_i} TP}{\sigma^2_{S_jR_i} TP + 3M\sum_{l=1}^{L}\sigma^2_{S_{j,l}}} \frac{\sigma^2_{S_jR_i} TP}{\sigma^2_{S_jR_i} TP + 3N\sum_{l=1}^{L}\sigma^2_{R_{i,l}}}\right) \tag{3.31}$$

The proof follows arguments similar to that presented for Scenario 1.

3.3 Results

In this subsection, we numerically compute the SKGR for both scenarios and compare it to the SKGR of a point-to-point communication scenario. We set the coherence time to be $T_c = 1s$ and the length of training sequences $L = 10$. Without loss of

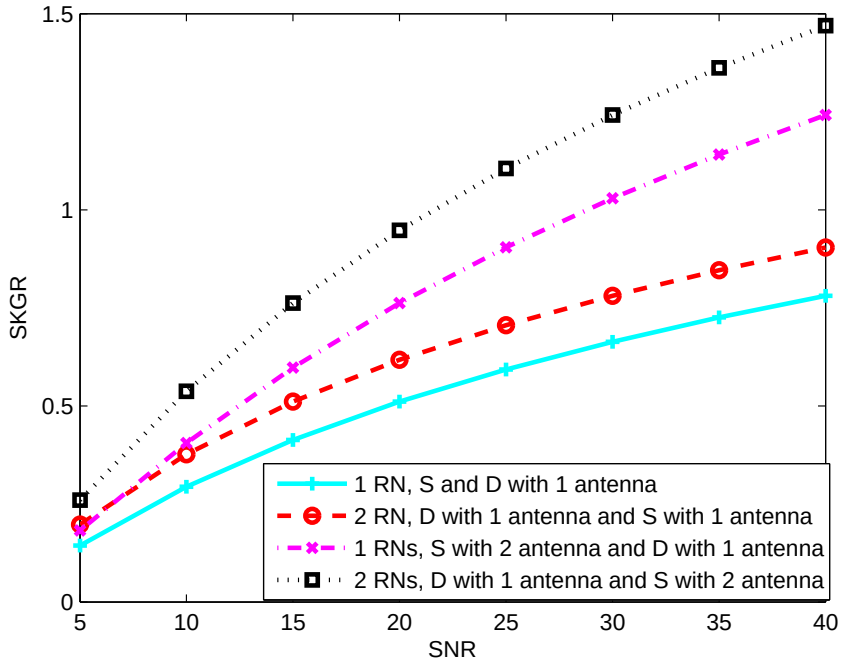

Figure 3.2: *Numerical Results for Scenario* 1

generality, we assume all channel gains are normally distributed with zero mean and variance equal to 1, and Gaussian noise sources are assumed to be zero mean with variance equal to 1. As seen in Fig. 3.2, in Scenario 1, we plot SKGR as a function of signal to noise ratio (SNR) corresponding to four cases: S with one antenna and one RN (original case), S with two antennas and one RN (co-op MISO), S with one antenna and two relay nodes (co-op SIMO), and S with two antennas and two relay nodes (co-op MIMO). Results in Fig. 3.2 indicate that an increased number of relay nodes or source antennas leads to improved SKGR. We also discovered that increasing the number of source antennas significantly improves SKGR as compared to increasing the number of relay nodes. This is because assembling more antennas in S increases the number of virtual channels. Deploying additional relay nodes also improves SKG performance by enhancing the randomness of the channel. However, the system is still a virtual single input and single out (SISO) model. Therefore, system with relay-based

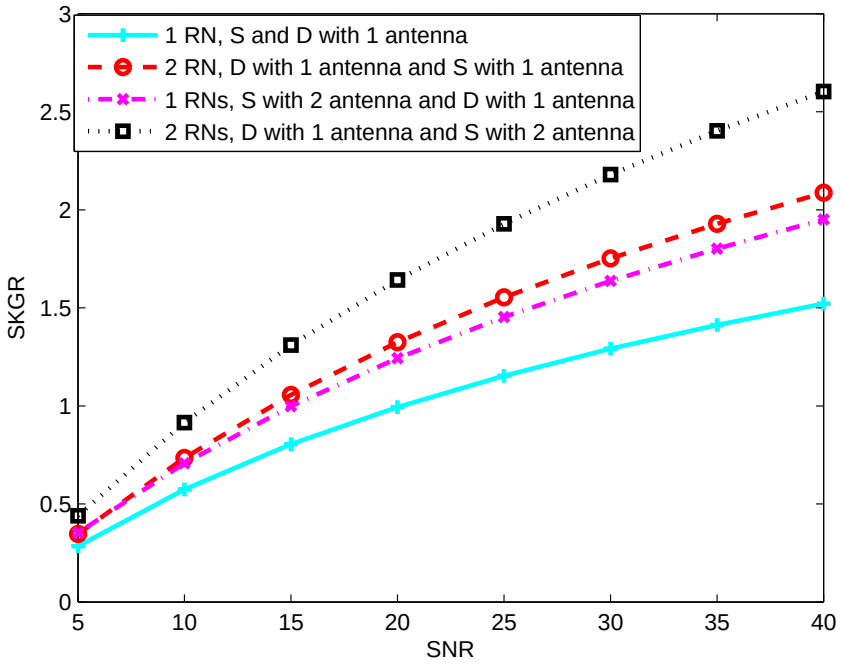

Figure 3.3: *Numerical Results for Scenario* 2

co-op MIMO architecture achieved the best SKG performance in Scenario 1.

Fig. 3.3 compares the SKGR corresponding to four cases, as mentioned above, in Scenario 2. The figure illustrates that SKGR increased with number of source antennas or relay nodes increased. This trend is especially useful as it suggests that relay-based SKG offers a way to generate large-size keys critical to secure the LTE-A network. Fig. 3.3 also demonstrates that a system with relay-based co-op MIMO architecture achieved the best SKG performance. However, the assembly of additional antennas at source or the deployment of additional relay nodes have identical impact on SKGR. This aspect is further investigated in the following discussion.

Fig. 3.4 and Fig. 3.5 indicate SKGR as a function of the number of antennas in S and a varying number of relay nodes with SNR=15 in both scenarios. In Scenario 1, Fig. 3.4 demonstrates that, for SKGR, the impact of the number of source antennas is more significant than the impact of the number of relay nodes. This can be explained as

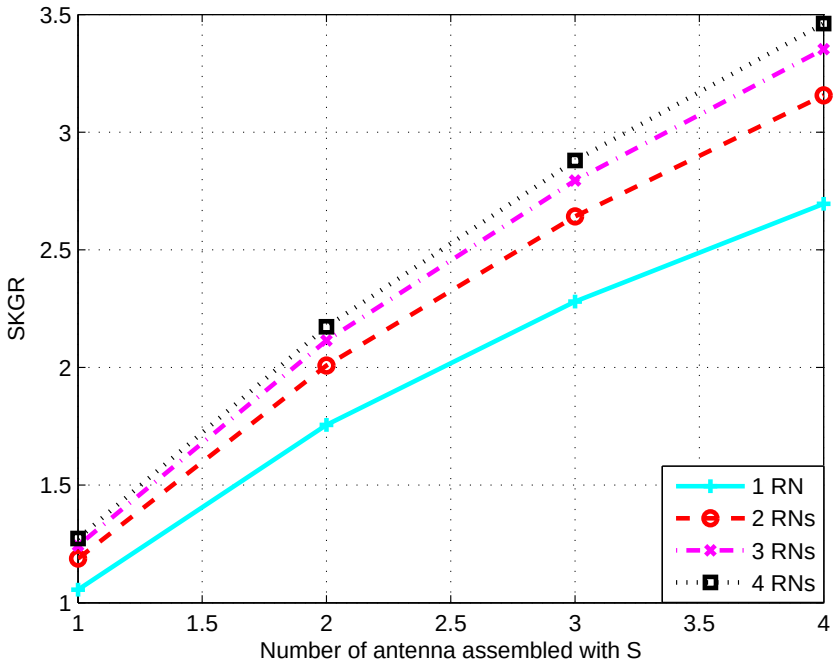

Figure 3.4: *Relation between SKGR and N,M for Scenario* 1

iiniin

Figure 3.5: *Relation between SKGR and N,M for Scenario* 2

follows: in Scenario 1, relay nodes were deployed to enhance the coverage of S as well as to enrich channel randomness. Nevertheless, additional source antennas increased the number of virtual channels between S and D. In Scenario 2, both the number of relay nodes and source antennas significantly impact SKGR since they played an equivalent role in the improvement of network throughput and the enrichment of channel randomness. Therefore, as shown in Fig. 3.5, the overall performance in Scenario 2 was much better than Scenario 1.

3.4 Conclusion

This chapter investigates SKG performance in LTE-A network with relay-based co-op MIMO architecture. We present two practical LTE-A scenarios and propose novel SKG schemes for each scenario. We evaluate the information theoretic result for SKGR. Numerical results on SKGR demonstrated the feasibility of relay-based SKG in PHY-Layer of LTE-A. Future work will involve trade-off analysis between energy/RN synchronization/overhead cost and SKG performance under our proposed relay based co-op MIMO schemes. Also, we will extend our PHY-SKG method to the entire network, including interference alignment and artificial noise injection techniques

Chapter 4

Chapter 4: Secret Key Generation Rate With Power Allocation in Relay-Based LTE-A Networks

LTE-A networks exploit low-power relay nodes, picocells and femtocells to boost throughput, enhance coverage, decrease latency, and reduce cost. End users in a relay-based LTE-A network can recruit relay nodes to cooperate as virtual antenna arrays, thereby reaping the benefits offered by MIMO techniques. Although relay-based cooperative MIMO (coop MIMO) implementation in LTE-A networks improves performance, security issues are often overlooked. This chapter introduces a physical layer (PHY-layer) security scheme for point-to-point networks and extends this scheme to MIMO networks. Two practical relay-based coop MIMO architectures and corresponding secret key generation (SKG) schemes are presented. For both the MIMO and coop MIMO networks, the impact of proposed power allocation on secret key generation rate is quantified via theoretical and numerical analysis. Results indicate that proposed power allocation scheme can offer $15\% - 30\%$ increase in secret key

generation rate (SKGR) relative to MIMO/coop MIMO networks with equal power allocation at low power region, thereby improve network security.

4.1 Introduction

In 2009, the 3rd Generation Partnership Project (3GPP) proposed the development of Long Term Evolution Advanced (LTE-A), deployed in a macro/microcell layout. Objectives of this project include providing improved system capacity and coverage, increasing peak data rates, decreasing latency, reducing operating costs, providing multi-antenna support, creating flexible bandwidth operation, and seamless integration with existing systems [54]. In addition, LTE-A supports heterogeneous deployments in which low-power nodes including picocells, femtocells, relays, and remote radio heads are placed in a macrocell layout. With these low-power nodes, LTE-A provides enhanced coverage and capacity in target areas at low cost. Additionally, LTE-A allows for cooperative MIMO (coop MIMO) where distributed antennas on multiple radio devices work together as virtual antenna arrays (VAAs) to emulate MIMO communications. This is especially useful as many wireless devices may not be able to support multiple antennas due to dimension, budget, and hardware limitations, thereby preventing such devices from reaping MIMO gains. Although a number of distinguished studies have focused on ways to improve LTE-A network performance by exploiting coop MIMO schemes [4], security issues have often been overlooked. Due to the broadcast nature of wireless channels, wireless networks are threatened by eavesdropping, message modification, and node impersonation. Adversarial users are modeled as unauthorized users attempting to extract information from legitimate users. To protect the confidentiality, integrity, and authenticity of transmitted data, secrecy at the physical layer (PHY-layer) has recently attracted significant interest among researchers [60–63].

Traditional key-based enciphering techniques are limited by key distribution and computational complexity [5]. Therefore, following the distinguished work by Shannon [58], wireless channel reciprocity-based physical layer secret key generation (PHY-SKG) techniques have garnered attention in wireless security community. These techniques generate secret keys using common randomness that is extracted from channels between parties in a wireless communication system. Eavesdroppers experience independent physical channels from legitimate users as long as they are a few wavelengths away from legitimate nodes. Therefore, the keys are secured with an information theoretic guarantee [19].

Our preliminary work in [41] indicates that relay-based coop MIMO architectures can significantly improve SKGR by exploiting common randomness. Reference [18] demonstrates that SKGR is highly depended on transmit power. Therefore, in this chapter, we quantify the effect of optimizing power allocations in relay based LTE-A network on SKGR.

In the context of prior efforts related to PHY-SKG schemes, it is evident that quantifying the effect of power allocation strategies on SKGR in coop MIMO architectures remains an open problem. We attempt to bridge this gap in this work.

In this work, we initially review the SKG algorithm for point-to-point networks. Then, we extend the basic algorithm to the MIMO case and provide a corresponding power allocation strategy. In addition, two SKG schemes with corresponding practical relay-based coop MIMO architectures are introduced. Case 1 corresponds to no direct connection between source and destination and Case 2 assumes that direct communication between source and destination is feasible. To further enhance SKGR, we propose two power allocation strategies for these two scenarios, respectively. Detailed theoretical analysis of proposed power allocation strategies are presented for MIMO and coop MIMO networks. We also provide numerical results to demonstrate the performance of our proposed power allocation strategies. Results demonstrate that

proposed power allocation scheme can offer $15\% - 30\%$ increase in SKGR relative to MIMO/coop MIMO networks with equal power allocation at low power region, thereby improve network security.

4.2 Secret Key Generation in MIMO Networks

It is easy to extend the SKG scheme of point-to-point networks discussed in Chapter 2 to MIMO networks. A MIMO channel model is presented in Fig. 4.1. Alice, a legitimate transmitter with M antennas, desires to securely communicate with Bob, a legitimate receiver with N antennas over a wireless channel. As mentioned earlier, assume a public channel with unlimited capacity is available to assist secret key generation. Therefore Alice and Bob can exchange information regarding to the secret keys using the public channel. To protect the communication between Alice and Bob, a similar SKG strategy based on the common fading channel is applied. Details are shown next.

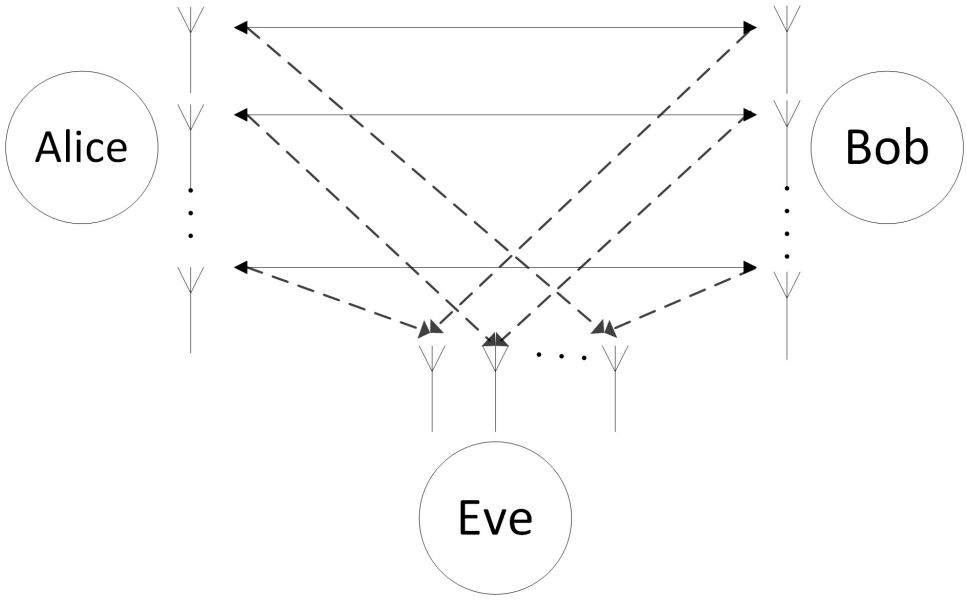

Figure 4.1: *Network model of MIMO system*

In the first time slot T_A, each antenna of Alice's transmitter sends a known sequence $\mathbf{s_{A_i}}$ of length L over a wireless channel. Assuming all antenna transmitted sequences are orthogonal to each other, Bob receives:

$$\mathbf{Y_B} = \mathbf{H_{AB}}\mathbf{S_A} + \mathbf{N_B} \tag{4.1}$$

where, $\mathbf{H_{AB}}$ denotes channel fading from Alice to Bob with dimension of $N \times M$; $\mathbf{S_A} = [\mathbf{s_{A_1}}, \mathbf{s_{A_2}}, ..., \mathbf{s_{A_M}}]$ is the probe signal with dimension of $M \times L$; $\mathbf{N_B}$ is Gaussian noise at Bob's receiver with dimension of $N \times L$. Using similar notation, each antenna of Bob's transmitter sends a known sequence $\mathbf{s_{B_i}}$ of length L over a wireless channel in the second timeslot T_B. Alice receives:

$$\mathbf{Y_A} = \mathbf{H_{BA}}\mathbf{S_B} + \mathbf{N_A} \tag{4.2}$$

where, $\mathbf{H_{BA}}$ denotes channel fading from Bob to Alice with dimension of $M \times N$; $\mathbf{S_B} = [\mathbf{s_{B_1}}, \mathbf{s_{B_2}}, ..., \mathbf{s_{B_N}}]$ is the probe signal with dimension of $N \times L$; $\mathbf{N_A}$ is Gaussian noise at Alice's receiver with dimension of $M \times L$. From results of point-to-point case, SKGR between Alice and Bob can be written as:

$$R_{S_{MIMO}} = I(\tilde{\mathbf{H}}_{\mathbf{AB}}; \tilde{\mathbf{H}}_{\mathbf{BA}}) \tag{4.3}$$

where, $\tilde{\mathbf{H}}_{\mathbf{AB}}$ and $\tilde{\mathbf{H}}_{\mathbf{BA}}$ denote estimated channel between Alice and Bob and estimated channel between Bob and Alice, respectively.

To generate secret key based on common randomness between forward and backward channels, Alice and Bob must generate estimates of $\mathbf{H_{AB}}$ and $\mathbf{H_{BA}}$, respectively. The assumption is made that the amount of time spent training for Alice and Bob is equal ($T_A = T_B = \frac{T}{2}$). The estimated channel from Alice to Bob and from Bob to Alice can

be written as:

$$\tilde{\mathbf{H}}_{\mathbf{AB}} = \mathbf{H}_{\mathbf{AB}} + \mathbf{N}_{\mathbf{B}}\mathbf{S}_{\mathbf{A}}^{\dagger} = \mathbf{H}_{\mathbf{AB}} + \frac{2N}{TP}\mathbf{N}_{\mathbf{B}}\mathbf{S}_{\mathbf{A}}^{\mathbf{T}} \tag{4.4}$$

$$\tilde{\mathbf{H}}_{\mathbf{BA}} = \mathbf{H}_{\mathbf{BA}} + \mathbf{N}_{\mathbf{A}}\mathbf{S}_{\mathbf{B}}^{\dagger} = \mathbf{H}_{\mathbf{BA}} + \frac{2M}{TP}\mathbf{N}_{\mathbf{A}}\mathbf{S}_{\mathbf{B}}^{\mathbf{T}} \tag{4.5}$$

where, $\mathbf{S}_{\mathbf{A}}^{\dagger}$ and $\mathbf{S}_{\mathbf{B}}^{\dagger}$ represent pseudo inverse matrices of training signal $\mathbf{S_A}$ and $\mathbf{S_B}$ ($\mathbf{S}_{\cdot}^{\dagger} = \mathbf{S}_{\cdot}^{\mathbf{T}}(\mathbf{S}_{\cdot}\mathbf{S}_{\cdot}^{\mathbf{T}})^{-1}$), respectively. The Gaussian assumptions for (1) the $\mathbf{H_{AB}}$ and $\mathbf{H_{BA}}$, and (2) noise $\mathbf{N_A}$ and $\mathbf{N_B}$ result in Gaussian random matrices $\tilde{\mathbf{H}}_{\mathbf{AB}}$ and $\tilde{\mathbf{H}}_{\mathbf{BA}}$. The elements of $\tilde{\mathbf{H}}_{\mathbf{AB}}$ and $\tilde{\mathbf{H}}_{\mathbf{BA}}$ are therefore independent Gaussian with mean zero and variance $\sigma^2_{A_jB_i}$ where j corresponds to the j^{th} antenna of Alice and i represents the i^{th} antenna of Bob. In the following lemma, we present the SKGR in a MIMO network (proof can be found in our previous work [64]).

Lemma 3. SKGR of Alice and Bob can be expressed as

$$\begin{aligned} I\left(\tilde{\mathbf{H}}_{\mathbf{AB}}; \tilde{\mathbf{H}}_{\mathbf{BA}}\right) &= -\frac{1}{2}\sum_{i=1}^{M}\sum_{j=1}^{N} log \\ &(1 - \frac{\sigma^2_{A_jB_i}TP_i}{\sigma^2_{A_jB_i}TP_i + 2N\sum_{l=1}^{L}\sigma^2_{A_{i,l}}} \frac{\sigma^2_{A_jB_i}TQ_j}{\sigma^2_{A_jB_i}TQ_j + 2M\sum_{l=1}^{L}\sigma^2_{B_{j,l}}}) \end{aligned} \tag{4.6}$$

where, P_i and Q_j are the transmit power of i^{th} antenna of Alice and the transmit power of j^{th} antenna of Bob, respectively. l=1...L is the index of the probe signal, therefore, $\sigma^2_{A_{i,l}}$ and $\sigma^2_{B_{j,l}}$ are the variances of Gaussian noise at the receiver of Alice and Bob at index l.

4.2.1 Sub-Optimum Power Allocation in MIMO networks

In our prior work, we assume that equal power is assigned to Alice and Bob and that power is evenly distributed to each antenna, respectively. However, in a practical case, antennas can simultaneously transmit data over multiple wireless channels by assigning power to the communication link according to power allocation schemes.

Observation of the derived expression of SKGR for MIMO networks (Eq. 4.6) reveals that SKGR is determined by power allocation and variance of channel estimators. Due to the training process, both Alice and Bob have the prior knowledge of channel estimators. Therefore, implementation of a power allocation algorithm is feasible in the MIMO case. Based on Eq. 4.6, it is easy to express the power allocation problem as follows:

$$\begin{aligned} \underset{\substack{P_i,Q_j \\ \forall i=1,...,M;j=1,...,N}}{\text{maximize}} \quad & R_{S_{MIMO}} \\ \text{subject to} \quad & \sum_{i=1}^{M} P_i \leq P_A \\ & \sum_{j=1}^{N} Q_j \leq P_B \\ & P_i \geq 0; Q_j \geq 0. \end{aligned}$$

Here, P_A and P_B are the total transmit power at Alice and Bob's transmitter, respectively.

We must verify convexity/concavity of the objective function in order to claim optimality of any optimization algorithm. A brief analysis of the above maximization problem indicates that the objective function is non-concave (see proof in Appendix A). Therefore, it is difficult to determine the optimal solution with reasonable complexity. However, Eq. 4.6 suggests that the objective function is concave in either P_i or $Q_j (i = 1, .., M$ and $j = 1, ..., N)$ when the other parameters are fixed. Therefore, in order to maximize the SKGR of MIMO networks, we employ an alternating maximization method [65] [66] to maximize SKGR as a function of each P_i and Q_j. This approach yields a suboptimal solution. We first examine the concavity of Eq. 4.6 as a function of P_i for fixed $Q_j; j = 1...N$ or Q_j for fixed $P_i; i = 1...M$.

Lemma 4. Assuming y (or x) is a fixed parameter, then

$$-\frac{1}{2}log[1- \frac{\sigma^2_{A_jB_i}Tx}{(\sigma^2_{A_jB_i}Tx + 2N\sum_{l=1}^{L}\sigma^2_{A_{i,l}})}\frac{\sigma^2_{A_jB_i}Ty}{(\sigma^2_{A_jB_i}Ty + 2M\sum_{l=1}^{L}\sigma^2_{B_{j,l}})}] \tag{4.7}$$

is a concave function of x (or y).

Proof. See Appendix B. □

Fixing Q_js, the optimization problem can be written as.

$$\begin{aligned} \underset{\substack{P_i \\ \forall i=1,\ldots,M}}{\text{maximize}} \quad & R_{S_{MIMO}} \\ \text{subject to} \quad & \sum_{i=1}^{M} P_i \leq P_A \\ & P_i \geq 0 \end{aligned}$$

We can apply the Lagrangian form on $R_{S_{MIMO}}$ as a function of P_is corresponding to

$$\mathfrak{L} = R_{S_{MIMO}} + \mu_1(P_A - \sum_{i=1}^{M} P_i) + \sum_{i=1}^{M} \mu_{i+2}P_i \tag{4.8}$$

The Karush Kuhn Tucker (KKT) conditions are:

$$\frac{\partial \mathfrak{L}}{\partial P_i} = \frac{\partial R_{S_{MIMO}}}{\partial P_i} - \mu_1 + \mu_{i+2} = 0 \tag{4.9}$$

$$\mu_1(P_A - \sum_{i=1}^{M} P_i) = 0; \tag{4.10}$$

$$\mu_{i+2}P_i = 0 \tag{4.11}$$

$$\mu_{i+2} \geq 0; \mu_1 \geq 0 \tag{4.12}$$

Eq. 4.9 demonstrate that $\mu_1 > \mu_{i+2} \geq 0$. Therefore, combining this equation with Eq. 4.10 and Eq. 4.12, we can show that $P_A - \sum_{i=1}^{M} P_i = 0$. Assuming all antennas are used for signaling, the powers P_i and Q_j should be greater than zero, $\mu_{i+2} = 0$.

Therefore, KKT conditions can be rewritten as the following equalities:

$$\begin{cases} \sum_{j=1}^{N} \frac{Q_j}{(P_i + a_{i,j})(Q_j + b_{i,j}(P_i + a_{i,j}))} - \mu_1 = 0 \\ P_A - \sum_{i=1}^{M} P_i = 0 \end{cases} \tag{4.13}$$

where $a_{i,j} = \frac{3M \sum_{l=1}^{L} \sigma^2_{A_j,l}}{\sigma^2_{A_j,B_i} T}$ and $b_{i,j} = \frac{3N \sum_{l=1}^{L} \sigma^2_{B_i,l}}{3M \sum_{l=1}^{L} \sigma^2_{A_j,l}}$. Assuming we have a equal power distribution at Bob's transmitter side (Q_j) in the initial state, Eq. 4.13 can be solved using a water-filling approach as described in Algorithm 1.

Algorithm 1 Water-filling Algorithm

1): Compute corresponding $a_{i,j}$ and $b_{i,j}$ for $i = 1, \ldots, M$ and $j = 1, \ldots, N$

2): Calculate $\mu_1 = \frac{4b_{i,j}NP_B}{(2b_{i,j}(P_B + a_{i,j}) + P_B)^2 - P_B^2}$

3): Using μ_1, compute $P_i = \left(\frac{-P_B + \sqrt{P_B^2 + \frac{4b_{i,j}NP_B}{\mu_1}}}{2b_{i,j}} - a_{i,j} \right)^+$ for $i = 1, \ldots, M$

4): If all $P_i s$ are non-negative, then end. Otherwise, set $P_i = 0$ and proceed to Step 3

The symmetric form of Eq. 4.6 allows us to write the Lagrangian in a similar form for all steps of the alternating maximization approach. Using the updated power allocation at Alice's transmitter side (from water-filling algorithm), we have the following optimization problem:

$$\begin{aligned} \underset{\substack{Q_j \\ \forall j=1,\ldots,N}}{\text{maximize}} \quad & R_{S_{MIMO}} \\ \text{subject to} \quad & \sum_{j=1}^{N} Q_j \leq P_B \\ & Q_j \geq 0 \end{aligned}$$

Applying the same approach, we have following equalities as a function of Q_j

$$\begin{cases} \sum_{i=1}^{N} \dfrac{P_i}{(Q_j + c_{i,j})(P_i + d_{i,j}(Q_j + c_{i,j}))} - \mu_2 = 0 \\ P_B - \sum_{j=1}^{N} Q_j = 0 \end{cases} \tag{4.14}$$

where $c_{i,j} = \frac{3N \sum_{l=1}^{L} \sigma^2_{B_i,l}}{\sigma^2_{A_j,B_i} T}$ and $d_{i,j} = \frac{3M \sum_{l=1}^{L} \sigma^2_{A_j,l}}{3N \sum_{l=1}^{L} \sigma^2_{B_i,l}}$.

Using the similar water-filling algorithm, we update the power allocation at Alice's transmitter side based on the derived power allocation at Bob's transmitter side from previous state. Continuing this forward and backward iterations, a local optimum power allocation at both Alice and Bob's transmitter can be achieved as proven in [67]. Consequently, the alternating maximization algorithm can be described as follows (Algorithm 2).

Algorithm 2 Alternating Maximization Algorithm

0): In the initial state 0, setting $Q_{j0} = \frac{P_B}{N}, \forall j = 1, 2, ..., N$ as a equal power distribution at Bob's transmitter side, the power allocation of Alice's transmitter side (P_{i0}) can be solved by using water-filling algorithm.
1): Calculate the power allocation at Bob's transmitter side (Q_{j1}) based on P_{i0} by using similar water-filling algorithm.
...
k): Update P_{ik} based on the Q_{jk}
$k+1$): Use P_{ik} to calculate the Q_{jk+1}
...
Terminate iterations when $\|P_{ik+1} - P_{ik}\|^2 \leq \varepsilon$ and $\|Q_{jk+1} - Q_{jk}\|^2 \leq \varepsilon$.

4.3 Secret Key Generation Schemes for Coop MIMO Networks

In this section, we extend our proposed power allocation schemes to coop MIMO networks. Based on our prior work [41], we propose two coop MIMO network models and corresponding novel power allocation strategies in the following subsections.

4.3.1 Coop MIMO network: Scenario 1

In this section, we consider a communication scenario in which the end user (destination) cannot communicate with the source due to distance. As shown in Fig. 4.2, Source S is assumed to have N antennas. Destination D is a mobile user with one antenna. Since Source S cannot communicate directly with Destination D, M low-power relay nodes (RNs) are deployed in this scenario. We assume that all RNs employ one antenna. In this chapter, we focus only on common randomness sharing overhead, i.e., synchronization overhead of RNs, are not considered. Using a similar notation as presented in Section III, we have the following lemma related to SKGR (proved in our earlier work [41]) in this scenario:

Lemma 5. According to the theoretical analysis in [41], SKGR for coop MIMO: Scenario 1 can be written as:

$$R_{coop_1} = -\frac{1}{2T}\sum_{j=1}^{N} log[1 - \frac{a_j T P_T}{(a_j T P_T + c_j)}\frac{a_j T Q_j}{(a_j T Q_j + Nb)}] \tag{4.15}$$

where, P_T is the total transmit power; $a_j = \sum_{i=1}^{M} \sigma^2_{R_i D}\sigma^2_{S_j R_i}$, $b = \sum_{l=1}^{L}(\sum_{i=1}^{M} \sigma^2_{R_i D}\sigma^2_{R_{i,l}} + \sigma^2_{D_l})$ and $c_j = \sum_{l=1}^{L}(\sum_{i=1}^{M} \sigma^2_{R_i S_j}\sigma^2_{R_{i,l}} + \sigma^2_{S_{j,l}})$.

As we can observe from Eq. 4.20, SKGR is determined by the assigned power to

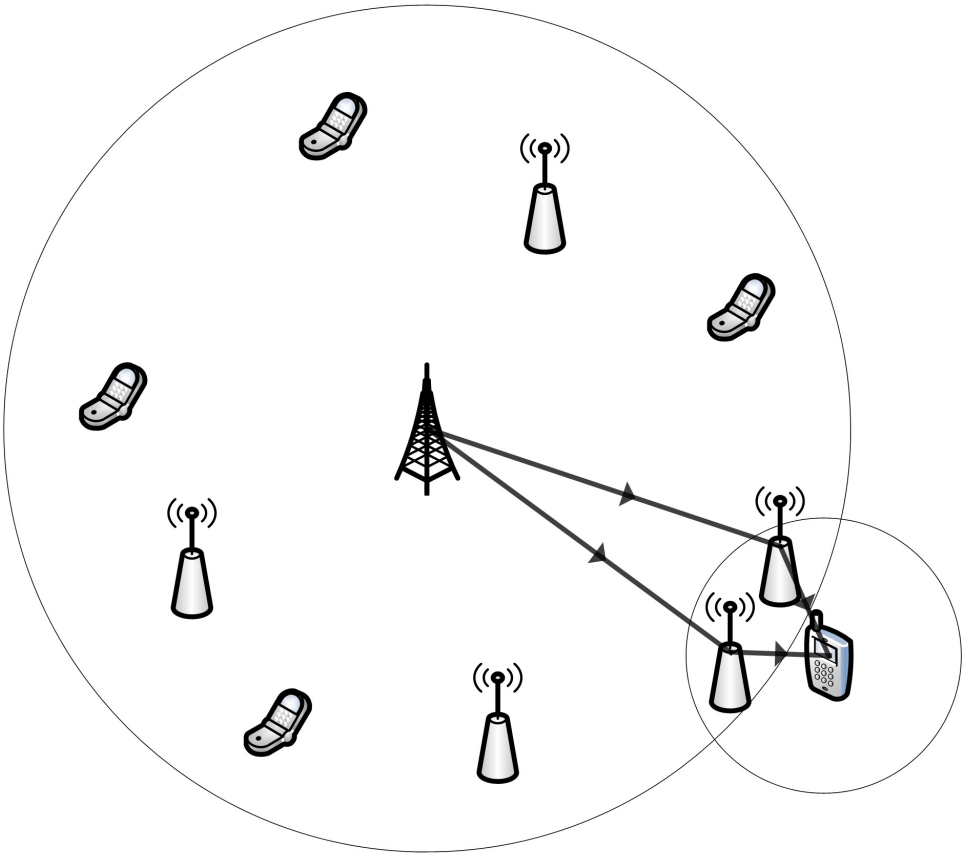

Figure 4.2: *Network model of coop MIMO architecture: Scenario* 1

each antenna/relay node and variance of channel estimators. Therefore, the power allocation problem for this scenario can be written as:

$$\begin{aligned} \underset{\substack{Q_j \\ \forall j=1,\ldots,N}}{\text{maximize}} \quad & R_{coop_1} \\ \text{subject to} \quad & \sum_{j=1}^{N} Q_j \leq P_S + P_R \\ & Q_j \geq 0 \end{aligned}$$

One thing we need to mention here is that it is possible to transfer our original coop MIMO architecture to a virtual MISO network (as shown in [41]). Consequently, in this case, we need to assign the total power P_T, a summation of transmit power of source P_S and transmit power of relay nodes P_R ($P_T = P_S + P_R$ and $P_R < P_S$) as the transmit power for the forward path.

In order to solve this power allocation problem, we need to examine the concavity of the objective function (Eq. 4.20). It is easy to figure out that Eq. 4.20 has a very similar form compared to the objective function in MIMO case. Using a similar approach, we can prove that Eq. 4.20 is a concave function of Q_j when P_T is fixed.

Application of Lagrangian form to the objective function allows the optimization problem to be written as:

$$\mathfrak{L} = R_{coop_1} + \mu_1(P_T - \sum_{j=1}^{N} Q_j) + \sum_{j=1}^{N} \mu_{j+1} Q_j \tag{4.16}$$

The KKT condition can be expressed as:

$$\frac{\partial \mathfrak{L}}{\partial P_i} = \frac{\partial R_{coop_1}}{\partial Q_j} - \mu_1 + \mu_{j+2} = 0 \tag{4.17}$$

$$\mu_1(P_T - \sum_{j=1}^{N} Q_j) = 0 \tag{4.18}$$

$$\mu_{j+1} Q_j = 0; \mu_1 \geq 0; \mu_{j+1} \geq 0 \tag{4.19}$$

Using an approach similar to the previous case, the optimization problem can be rewritten as:

$$\begin{cases} \dfrac{P_T}{(Q_j + d_j)(P_T + e_j(Q_j + d_j))} - \mu_1 = 0 \\ P_T - \sum_{j=1}^{N} Q_j = 0 \end{cases} \tag{4.20}$$

where $d_j = \frac{c_j}{b}$ and $e_j = \frac{b}{a_j}$. Eq. 4.21 can be solved using a similar water-filling approach as described in Algorithm 1.

4.3.2 Coop MIMO network: Scenario 2

In this section, we consider a scenario in which no restriction exists between Destination D, Source S, and RNs; i.e., they can spontaneously communicate with each other. As shown in Fig. 4.3, M RNs are deployed and all RNs employ one antenna. N antennas are assembled with Source S. The destination is a mobile device with one antenna. Without considering overheads and using similar notation as shown in scenario 1, we present the following result on the SKGR (which is proved in our earlier work [41]).

Lemma 6. The SKGR for coop MIMO: scenario 2 corresponds to [41]:

$$\begin{aligned} R_{coop2} &= \frac{1}{T} \\ &\left\{ I\left(\tilde{\mathbf{h}}_{\mathbf{SD}}; \tilde{\mathbf{h}}_{\mathbf{DS}}\right) + min\left\{ I\left(\tilde{\mathbf{H}}_{\mathbf{SR}}; \tilde{\mathbf{H}}_{\mathbf{RS}}\right), I\left(\tilde{\mathbf{h}}_{\mathbf{DR}}; \tilde{\mathbf{h}}_{\mathbf{RD}}\right)\right\}\right\} \end{aligned} \tag{4.21}$$

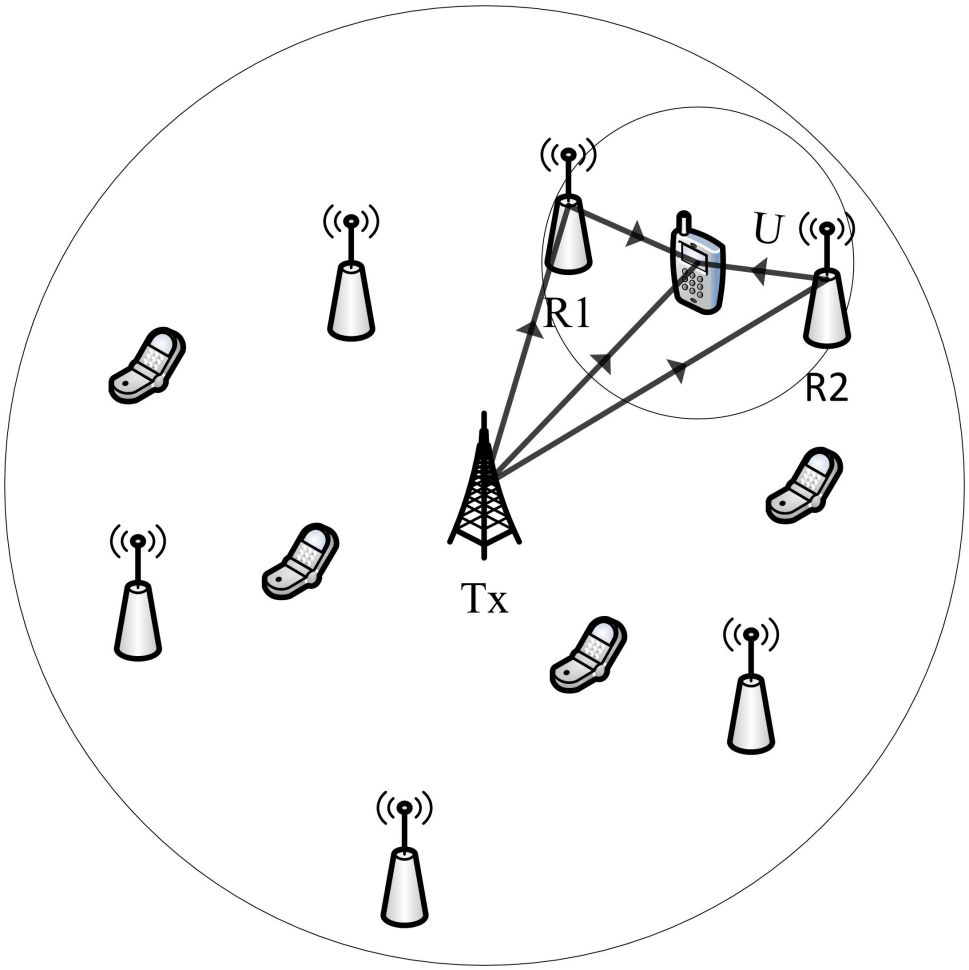

Figure 4.3: *Network model of coop MIMO architecture: Scenario* 2

where, the mutual information terms are:

$$I\left(\tilde{\mathbf{h}}_{\mathbf{SD}};\tilde{\mathbf{h}}_{\mathbf{DS}}\right) = -\frac{1}{2}\sum_{j=1}^{N} log \\ [1 - \frac{\sigma^2_{S_jD} TQ_j}{(\sigma^2_{S_jD} TQ_j + 3N\sum_{l=1}^{L}\sigma^2_{D_l})} \frac{\sigma^2_{S_jD} TP_S}{(\sigma^2_{S_jD} TP_S + 3\sum_{l=1}^{L}\sigma^2_{S_{j,l}})}] \tag{4.22}$$

$$I\left(\tilde{\mathbf{h}}_{\mathbf{DR}};\tilde{\mathbf{h}}_{\mathbf{RD}}\right) = -\frac{1}{2}\sum_{i=1}^{M} log \\ [1 - \frac{\sigma^2_{DR_i} TP_i}{(\sigma^2_{DR_i} TP_i + 3M\sum_{l=1}^{L}\sigma^2_{D_l})} \frac{\sigma^2_{DR_i} TP_D}{(\sigma^2_{DR_i} TP_D + 3\sum_{l=1}^{L}\sigma^2_{R_{i,l}})}] \tag{4.23}$$

$$I\left(\tilde{\mathbf{H}}_{\mathbf{SR}};\tilde{\mathbf{H}}_{\mathbf{RS}}\right) = -\frac{1}{2}\sum_{i=1}^{M}\sum_{j=1}^{N} log \\ [1 - \frac{\sigma^2_{S_jR_i} TP_i}{(\sigma^2_{S_jR_i} TP_i + 3M\sum_{l=1}^{L}\sigma^2_{S_{j,l}})} \frac{\sigma^2_{S_jR_i} TQ_j}{(\sigma^2_{S_jR_i} TQ_j + 3N\sum_{l=1}^{L}\sigma^2_{R_{i,l}})}] \tag{4.24}$$

According to the derived expression of SKGR for Scenario 2 (Eqs. 4.214.224.234.24) of coop MIMO network reveals that SKGR over all wireless channels is determined by power allocation and variance of channel estimators. A proper power allocation scheme can be implemented into the network to maximize SKGR. The power allocation problem corresponding to scenario 2 can be written as:

$$\begin{aligned} \underset{\substack{P_i,Q_j \\ \forall i=1,\ldots,M;j=1,\ldots,N}}{\text{maximize}} \quad & R_{coop_2} \\ \text{subject to} \quad & \sum_{j=1}^{N} Q_j \leq P_S, Q_j \geq 0 \\ & \sum_{i=1}^{M} P_i \leq P_R, P_i \geq 0 \end{aligned}$$

Since the optimization problem is a challenging max-min optimization problem, we transfer this problem into an equivalent linear program [68]

$$\begin{aligned}
\underset{\substack{P_i,Q_j \\ \forall i=1,\ldots,M;j=1,\ldots,N}}{\text{maximize}} \quad & Z \\
\text{subject to} \quad & Z \leq I_1 + I_2 \\
& Z \leq I_1 + I_3 \\
& Z \geq 0 \\
& \sum_{j=1}^{N} Q_j \leq P_S, Q_j \geq 0 \\
& \sum_{i=1}^{M} P_i \leq P_R, P_i \geq 0
\end{aligned}$$

A similar alternating maximization method can be applied for this scenario as well. Assuming equal power at the source, the optimization problem can be transformed as:

$$\begin{aligned}
\underset{\substack{P_i \\ \forall i=1,\ldots,M}}{\text{maximize}} \quad & Z \\
\text{subject to} \quad & Z \leq I_1 + I_2 \\
& Z \leq I_1 + I_3 \\
& Z \geq 0 \\
& \sum_{i=1}^{M} P_i \leq P_R, P_i \geq 0
\end{aligned}$$

Lagrangian form of Z as a function of P_i yields:

$$\begin{aligned}
\mathfrak{L} = & Z + \mu_1(I_1 + I_2 - Z) + \mu_2(I_1 + I_3 - Z) \\
& + \mu_3(P_R - \sum_{i=1}^{M} P_i)
\end{aligned} \tag{4.25}$$

Therefore, the KKT condition can be written as:

$$\frac{\partial \mathfrak{L}}{\partial Z} = 1 - \mu_1 - \mu_2 = 0 \tag{4.26}$$

$$\frac{\partial \mathfrak{L}}{\partial P_i} = \mu_1 \frac{\partial I_2}{\partial P_i} + \mu_2 \frac{\partial I_3}{\partial P_i} - \mu_3 = 0 \tag{4.27}$$

$$Z \leq I_1 + I_2, Z \leq I_1 + I_3, \sum_{i=1}^{N} P_i \leq P_R \tag{4.28}$$

$$\mu_1 \geq 0, \mu_2 \geq 0, \mu_3 \geq 0, \mu_1(Z - I_1 - I_2) = 0 \tag{4.29}$$

$$\mu_2(Z - I_1 - I_3) = 0, \mu_3(\sum_{i=1}^{N} P_i - P_R) = 0 \tag{4.30}$$

Eq. 4.27 show that $\mu_3 \neq 0$. Based on a combination of Eq. 4.27, Eq. 4.29 and Eq. 4.30, it is easy to figure out that:

$$\sum_{i=1}^{N} P_i - P_R = 0 \tag{4.31}$$

Therefore, the solution of this optimization problem is determined by the value of μ_1 and μ_2. According to equation Eq. 4.27 and Eq. 4.29, it is easy to figure out that $0 \leq \mu_1, \mu_2 \leq 1$ and $\mu_1 + \mu_2 = 1$. Three cases emerge for the optimization problem, namely,

Case 1: $\mu_1 = 1$ and $\mu_2 = 0$;

Case 2: $\mu_2 = 1$ and $\mu_1 = 0$;

Case 3: $\mu_1 \neq 0$ and $\mu_2 \neq 0$

In the following subsections, we discuss the implications of these three cases.

Case 1: $\mu_1 = 1$ and $\mu_2 = 0$

In this case, the optimization function can be rewritten as:

$$\begin{aligned} \underset{\substack{P_i \\ \forall i=1,\ldots,M}}{\text{maximize}} \quad & R_{coop_2} = I_1 + I_2 \\ \text{subject to} \quad & \sum_{i=1}^{N} P_i = P_R \\ & P_i \geq 0 \end{aligned}$$

Application of Lagrangian form to our optimization problem, we have:

$$\mathfrak{L} = R_{coop_2} + \lambda_2 (P_R - \sum_{i=1}^{M} P_i) + \sum_{i=1}^{M} \mu_i P_i \tag{4.32}$$

The KKT condition can be expressed as:

$$\frac{\partial \mathfrak{L}}{\partial P_i} = \frac{\partial R_{coop_1}}{\partial P_i} - \lambda_2 + \mu_i = 0 \tag{4.33}$$

$$P_R - \sum_{i=1}^{M} P_i = 0 \tag{4.34}$$

$$\mu_i P_i = 0; \mu_i \geq 0 \tag{4.35}$$

Similar to the previous case, the optimization problem corresponds to:

$$\begin{cases} \dfrac{P_D}{(P_i + h_i)(P_D + k_i(P_i + h_i))} - \lambda_2 = 0 \\ P_R - \sum_{i=1}^{M} P_i = 0 \end{cases} \tag{4.36}$$

where $h_i = \frac{\sum_{l=1}^{L} \sigma_{R_i,l}^2}{M \sum_{l=1}^{L} \sigma_{D_l}^2}$ and $k_i = \frac{3M \sum_{l=1}^{L} \sigma_{D_l}^2}{\sigma_{D,R_i}^2 T}$.

Since Eq. 4.36 is similar in form to Eq. 4.21, it is possible to solve the above optimization problem by exploiting a similar water-filling algorithm as shown in Algorithm

1.

Case 2: $\mu_2 = 1$ and $\mu_1 = 0$

In this case, the optimization problem is:

$$\begin{aligned} \underset{\substack{P_i \\ \forall i=1,\ldots,M}}{\text{maximize}} \quad & R_{coop_2} = I_1 + I_3 \\ \text{subject to} \quad & \sum_{i=1}^{N} P_i = P_R \\ & P_i \geq 0 \end{aligned}$$

Using a similar approach as in the previous case, we can rewrite the optimization problem as:

$$\begin{cases} \sum_{j=1}^{N} \dfrac{Q_j}{(P_i + o_{i,j})(Q_j + p_{i,j}(P_i + o_{i,j}))} - \lambda_3 = 0 \\ P_R - \sum_{i=1}^{M} P_i = 0 \end{cases} \tag{4.37}$$

where $o_{i,j} = \frac{3M \sum_{l=1}^{L} \sigma^2_{S_j,l}}{\sigma^2_{S_j,R_i} T}$ and $p_{i,j} = \frac{3N \sum_{l=1}^{L} \sigma^2_{R_i,l}}{3M \sum_{l=1}^{L} \sigma^2_{S_j,l}}$. The solution of Eq. 4.37 can be solved by exploiting the similar water-filling algorithm.

Case 3: $\mu_1 \neq 0$ and $\mu_2 \neq 0$

According to the expression of original "max-min" optimization problem, only two options exist for this case: $R_{coop_2} = I_1 + I_2$ and $R_{coop_2} = I_1 + I_3$. Therefore, the optimal power allocation falls into either Case 1 or Case 2.

Comparing above three cases, we select the power allocation (P_{j0}) corresponding to the maximum SKGR. Based on P_{j0}, we calculate the power distribution at the source.

This optimization problem can be written as follows.

$$\begin{aligned} \underset{\substack{Q_j \\ \forall j=1,\ldots,N}}{\text{maximize}} \quad & Z \\ \text{subject to} \quad & Z \leq I_1 + I_2 \\ & Z \leq I_1 + I_3 \\ & Z \geq 0 \\ & \sum_{j=1}^{N} Q_j \leq P_S, Q_j \geq 0 \end{aligned}$$

Similar to previous analysis, we have three cases as well.

Case i: $\mu_1 = 1$ and $\mu_2 = 0$

The optimization problem can be written as:

$$\begin{aligned} \underset{\substack{Q_j \\ \forall j=1,\ldots,N}}{\text{maximize}} \quad & R_{coop_2} = I_1 + I_2 \\ \text{subject to} \quad & \sum_{j=1}^{M} Q_J = P_S \\ & Q_j \geq 0 \end{aligned}$$

Implementing same approach as shown above, the optimization problem corresponding to

$$\begin{cases} \dfrac{P_S}{(Q_j + f_j)(P_S + g_j(Q_j + f_j))} - \lambda_1 = 0 \\ P_S - \sum_{j=1}^{N} Q_j = 0 \end{cases} \tag{4.38}$$

where $f_j = \frac{\sum_{l=1}^{L} \sigma_{S_j,l}^2}{N \sum_{l=1}^{L} \sigma_{D_l}^2}$ and $g_j = \frac{3N \sum_{l=1}^{L} \sigma_{D_l}^2}{\sigma_{S_j,D}^2 T}$.

A similar water-filling algorithm can be employed to solve this problem.

Case ii: $\mu_1 = 0$ and $\mu_2 = 1$

The corresponding optimization problem is:

$$\begin{aligned} \underset{\substack{Q_j \\ \forall j=1,\ldots,N}}{\text{maximize}} \quad & R_{coop_2} = I_1 + I_3 \\ \text{subject to} \quad & \sum_{j=1}^{M} Q_J = P_S \\ & Q_j \geq 0 \end{aligned}$$

Using the similar approach, we have

$$\begin{cases} \dfrac{P_S}{(Q_j + q_j)(P_S + r_j(Q_j + q_j))} \\ \quad + \displaystyle\sum_{i=1}^{M} \frac{P_i}{(Q_j + s_{i,j})(P_i + t_{i,j}(Q_j + s_{i,j}))} - \lambda_4 = 0 \\ P_S - \displaystyle\sum_{j=1}^{N} Q_j = 0 \end{cases} \tag{4.39}$$

where $q_j = \frac{3N\sum_{l=1}^{L}\sigma_{D_l}^2}{\sigma_{S_j,D}^2 T}$, $r_j = \frac{\sum_{l=1}^{L}\sigma_{S_j,l}^2}{N\sum_{l=1}^{L}\sigma_{D_l}^2}$, $s_{i,j} = \frac{3N\sum_{l=1}^{L}\sigma_{R_i,l}^2}{\sigma_{S_j,R_i}^2 T}$ and $t_{i,j} = \frac{3M\sum_{l=1}^{L}\sigma_{S_j,l}^2}{3N\sum_{l=1}^{L}\sigma_{R_i,l}^2}$. The power allocation can be achieved by exploiting water-filling algorithm as well.

Case iii: $\mu_1 \neq 0$ and $\mu_2 \neq 0$

As previous analysis shown, the optimal results of case *iii* should falls into either case i or case ii.

Therefore, the alternating maximization algorithm for scenario 2 of coop MIMO can be described as Algorithm 3.

Algorithm 3 Alternating Maximization Algorithm

0): In the initial state 0, setting $Q_{j0} = \frac{P_S}{N}, \forall j = 1, 2, ..., N$ as a equal power distribution at source, the power allocation of relay node (P_{i0}) can be solved by using water-filling algorithm. We select the P_is corresponding to the maximum SKGR among the three cases as P_{i0}.
1): Calculate the power allocation at the source (Q_{j1}) based on P_{i0} by using water-filling algorithm. The Q_js corresponding to the maximum SKGR are selected as Q_{j1}.
...
k): Update P_{ik} based on the Q_{jk}
$k+1$): Use P_{ik} to calculate the Q_{jk+1}
...
Terminate iterations when $\|P_{ik+1} - P_{ik}\|^2 \leq \varepsilon$ and $\|Q_{jk+1} - Q_{jk}\|^2 \leq \varepsilon$.

4.4 Results

In this section, we provide numerical results related to SKGR with the proposed power allocation strategies for multiple antenna networks.

4.4.1 SKGR for MIMO network

In this scenario, we assume that two antennas are assigned to both Alice and Bob. The predefined variances of channel estimators (i.e., $\sigma^2_{A,j}$ and $\sigma^2_{B,i}$, $i = 1, 2$; $j = 1, 2$.) of MIMO network used in simulation are shown in Table 4.1. We set $\varepsilon = 0.001$ [66]. Fig. 4.4 shows a comparison of SKGR in a MIMO network with the proposed power allocation and equal power distribution. As expected, Fig. 4.4 demonstrates that our power allocation scheme improves SKGR at the low-power region. However, SKGR improvement of the power allocation algorithm is less significant with increased transmit power. This phenomenon can be explained as follows: when transmit power is low, the power allocation algorithm is forced to assign more power to channels with better channel quality. On the other hand, equal power distribution case continues to allocate the same power to each channel. Therefore, our power allocation case outperforms the equal power distribution case. Nevertheless, when transmit power is

high, the difference between SKGR due to variance of channel estimator is negligible [69]. Consequently, SKGR of equal power distribution case is close to that of our power allocation case.

Table 4.1: *The variance of channel estimator of MIMO case*

Alice/Bob	Antenna #1	Antenna #2
Antenna #1	$\sigma^2_{1,1} = 3.6$	$\sigma^2_{1,2} = 1.1$
Antenna #2	$\sigma^2_{2,1} = 0.8$	$\sigma^2_{2,2} = 0.7$

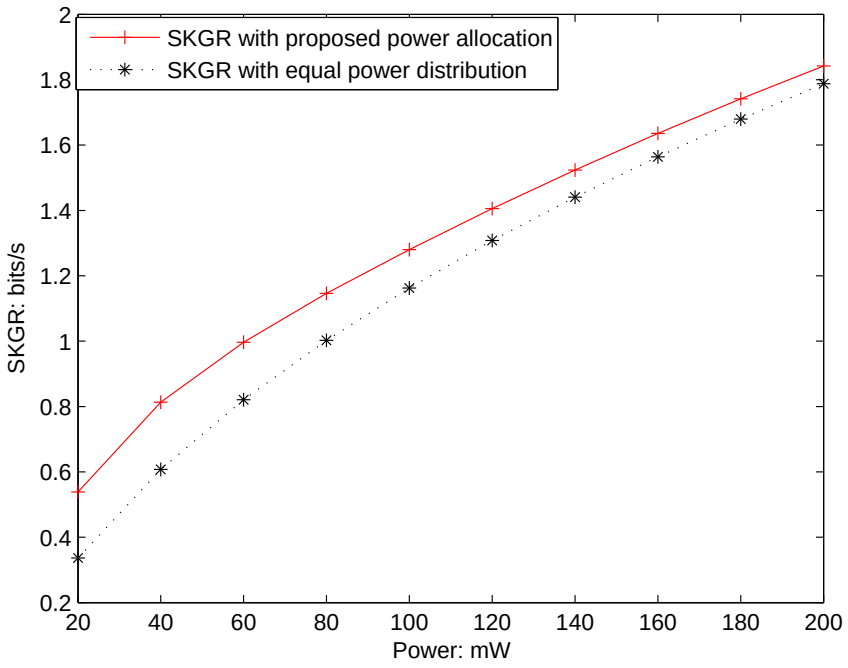

Figure 4.4: *Comparison of SKGR with proposed power allocation and SKGR with equal power distribution for MIMO networks*

4.4.2 SKGR for coop MIMO network Scenario 1

In this scenario, we assume that two antennas are employed by the source and two relay nodes are deployed in the network. Table 4.2 shows variances of channel estimators between source and relay nodes (S-R links) and variances of channel estimators

between relay nodes and destination (R-D links). A comparison of SKGR performance with proposed power allocation and equal power distribution is shown in Fig. 4.5 . It demonstrates performance improvement of our power allocation algorithm at low transmit power region. An interesting problem occurs when we compare the numerical result of MIMO networks and Scenario 1 of coop MIMO networks. Results shows that even with an increase in power to 200 mW, SKGR of the proposed power allocation approach remains greater than SKGR of equal power distribution case in MIMO networks. However, for Scenario 1 of coop MIMO networks, SKGR of the proposed power allocation approach is equal to SKGR of equal power distribution case when power increases to 70 mW. This phenomenon occurs because Scenario 1 of coop MIMO networks reduce to a virtual multiple input single output (MISO) network. The variance of channel estimator between source and destination (S-D Links) is a function (product) of the variances of channel estimators between S-R links and the variance of channel estimator between R-D links [41]. Due to the product of the variances of channel estimators, our choice of channel estimator variances yields a reduction of the variation of channel estimators between S-D links. Therefore, comparing to the MIMO case, the performance gap between our power allocation strategy and an equal power distribution case decreases with increase in power.

Table 4.2: *The variance of channel estimator of coop MIMO case: Scenario* 1 *and Scenario* 2

Source, Destination/Relay nodes	Relay node #1	Relay node #2
Source #1	$\sigma^2_{S_1,R_1} = 2.7$	$\sigma^2_{S_1,R_2} = 0.9$
Source #2	$\sigma^2_{S_2,R_1} = 0.5$	$\sigma^2_{S_2,R_2} = 2.1$
Destination	$\sigma^2_{D,R_1} = 0.7$	$\sigma^2_{D,R_2} = 3.3$

4.4.3 SKGR for coop MIMO network Scenario 2

In this scenario, we assume that two antennas are employed by the source and two relay nodes are deployed in the network. We assume the same channel estimator variances

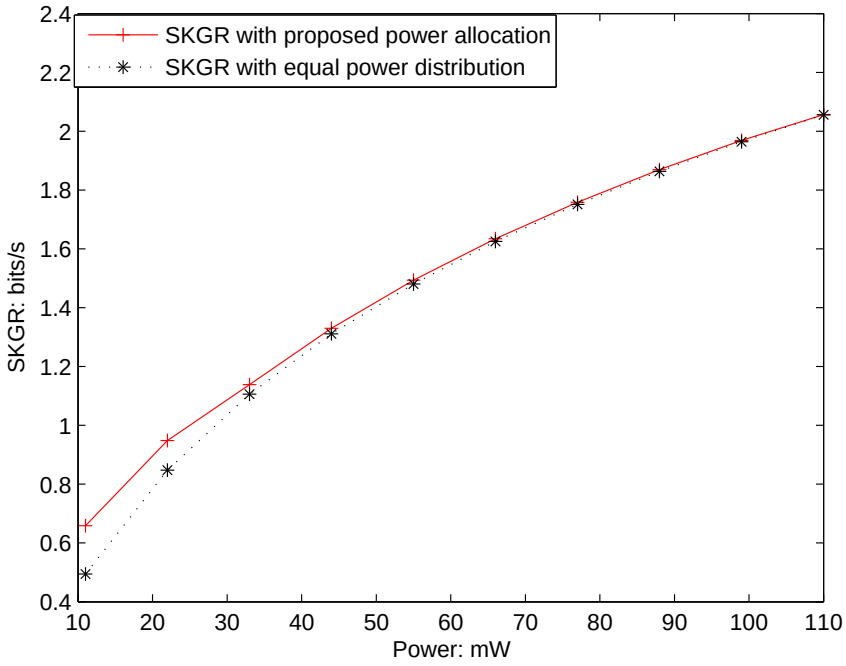

Figure 4.5: *Comparison of SKGR with proposed power allocation and SKGR with equal power distribution for coop MIMO networks: Scenario* 1

for S-R and R-D links. The channel estimator variances for S-D links is given in Table 4.3.Fig. 4.6 compares SKGR with the proposed power allocation and equal power distribution in Scenario 2 of the coop MIMO network. In this scenario, SKGR of our power allocation method outperforms the SKGR of equal power distribution case at low transmit power range. A comparison of Fig. 4.5 and Fig. 4.6 shows that the overall SKGR of Scenario 2 of coop MIMO network is greater than the overall SKGR of a MIMO network because with the deployment of relay nodes, Scenario 2 of coop MIMO has more common randomness between S-D links compared to MIMO networks. Therefore, coop MIMO networks has the ability to extract longer secret keys by exploiting common randomness in wireless channels.

Table 4.3: *The variance of channel estimator of coop MIMO case: Scenario* 2

Source/Destination	Source #1	Source #2
Destination	$\sigma^2_{D,S_1} = 0.6$	$\sigma^2_{D,S_2} = 3.1$

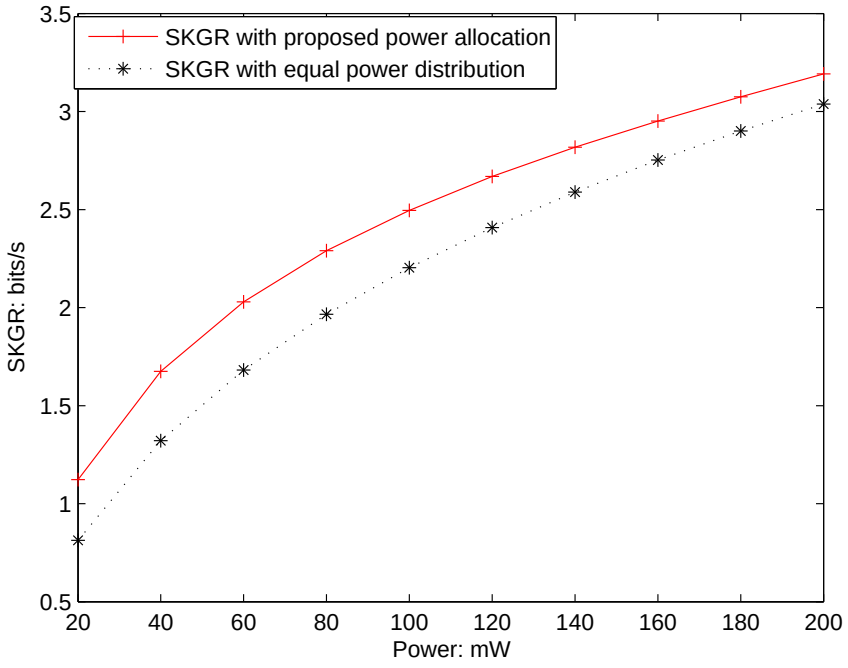

Figure 4.6: *Comparison of SKGR with proposed power allocation and SKGR with equal power distribution for coop MIMO networks: Scenario* 2

4.5 Conclusion

In this chapter, we investigate our proposed power allocation strategies to further increase the performance of the PHY-SKG technique in multiple-antenna networks. We present information theoretic results of SKGR in MIMO networks and derive the corresponding power allocation strategy. Based on previous research in coop MIMO networks, we propose two novel power allocation strategies for two scenarios, respectively. Theoretical analysis and numerical results demonstrate the effect of our power allocation strategies on SKGR for multiple-antenna networks. Future work will focus on two aspects: (1) extending our PHY-SKG scheme to multi-cell coop MIMO networks, including artificial noise injection and interference alignment techniques, and (2) considering relay nodes synchronization/overhead cost, to quantify trade-off between synchronization/overhead cost and SKGR.

Chapter 5

Chapter 5: Evaluating Node Reliability in Cooperative MIMO Networks

Cooperative multiple input multiple output (Co-MIMO) strategies represent one approach to meet the growing requirements (i.e., higher throughput, enhanced coverage, low latencies, and reduced cost) of wireless communication services. In Co-MIMO networks, low power relay nodes (RNs) are recruited by mobile users to cooperate as virtual antenna arrays. Although Co-MIMO architectures can offer significant improvement in both performance and security of wireless networks, they are susceptible to attacks. In this chapter, we propose a novel node reliability evaluation scheme to enhance the security of Co-MIMO networks. Leveraging the probe signal transmissions involved in physical layer secret key generation (PHY-SKG) schemes, two distributed node level reliability detection methods (one-shot and dynamic) are proposed to detect relay nodes that are non-cooperative. Based on the fusion of information from relay nodes, an overall reliability evaluation can be accomplished at a central server. Mo-

bile users interested in collaboration can access this central server to determine which nodes to recruit for cooperation. Both theoretical analysis and simulation results are presented to illustrate the proposed node reliability evaluation schemes.

5.1 Introduction

In order to provide higher data rates, better coverage, and lower latencies, the Long Term Evolution Advanced (LTE-A) standard incorporates picocells, femtocells, relays, and remote radio heads within a macro-cell layout. By allowing for cooperation with low-power relay nodes, LTE-A networks provide an efficient approach to enhance coverage and capacity at low cost. Researchers have proposed the concept of cooperative MIMO (Co-MIMO) networks [1], where distributed antennas on multiple devices work together as virtual antenna arrays.

A number of distinguished studies have been conducted on Co-MIMO networks and demonstrated their performance benefits. Additionally, in our previous research [70] [71], we demonstrate that Co-MIMO architectures can improve physical layer security (e.g., wireless channel reciprocity based physical layer secret key generation) by providing rich common randomness among wireless channels. Although Co-MIMO architectures offer benefits in performance and physical layer security, it is still vulnerable. In Co-MIMO architectures, mobile users are allowed to recruit relay nodes (such as idle users, femtocells and picocells) and physical layer secret key generation schemes (PHY-SKG) are not adequate to protect the communication. While PHY-SKG provides protection against eavesdropping, it is very difficult to detect misbehavior of relay nodes that have already joined the cooperative communication. Selfish or malicious intentions of relay nodes may manifest as non cooperation. Selfish nodes may suddenly choose not to cooperate in order to preserve their battery resources or prioritize other services. Malicious nodes, on the other hand, attempt to prevent

communication between source and destination nodes at any cost. Note that an adversary may control malicious nodes to attack cooperative networks, i.e., a denial of service attack at the physical layer. Therefore, understanding how to measure and monitor the reliability of relay nodes is one of the critical challenges in Co-MIMO based physical layer security schemes.

In this research, we attempt to address this issue by developing novel node reliability evaluation schemes for Co-MIMO networks. The proposed schemes allow us to generate and regularly update a reliability database that includes information about all relay nodes and is accessible by mobile users that are interested in cooperation. The node reliability evaluation used in conjunction with our previously proposed cooperative PHY-SKG scheme [70], [42] can significantly enhance security of Co-MIMO networks.

In this work, we propose novel node reliability evaluation schemes to enhance security of Co-MIMO networks. We are primarily interested in measuring the level of non cooperation of relay nodes. This type of misbehavior is detected by leveraging the first stage in our previously proposed PHY layer secret key generation scheme [42,70]. Specifically, consider a practical relay based Co-MIMO network model as shown in Fig. 2.3. For simplicity, focus on a single communication pair including the transmitter, mobile user and M relay nodes. By utilizing the identical probe signal that is initially transmitted by all participating nodes in any PHY-SKG scheme, we employ two distributed node level reliability detection methods: (1) a one-shot instantaneous reliability detection and (2) a Bayesian framework based dynamic reliability detection that incorporates history of node behavior. This node level reliability information can be fused at a central server in order to derive an overall measure of reliability. The metrics stored in the central server can be accessed by other mobile users who are interested in recruiting trustworthy nodes for cooperative operations. The proposed node reliability evaluation scheme used in conjunction with our previously proposed

cooperative PHY-SKG strategies [42, 70] can significantly enhance security of cooperative networks. To the best of our knowledge, this is the first work to address this important issue in Co-MIMO networks.

5.2 Node Level Reliability Evaluation

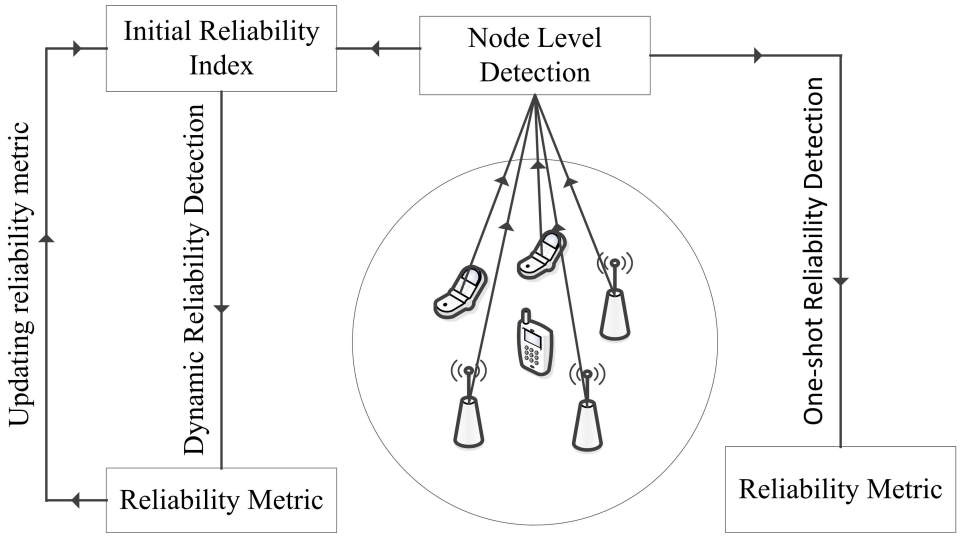

Figure 5.1: *Node Reliability Evaluation Method*

Our proposed one-shot and dynamic node level reliability evaluation schemes are shown in Fig. 5.1. Assume there are M relay nodes that cooperate to establish the communication between the transmitter and the mobile user. Prior to data transmission, a secret key is generated based on the process described in Section II. The first stage of secret key generation involves transmission of probe signals by the transmitter, mobile user and relay nodes. Therefore, at this stage, it is possible to identify nodes that are non cooperative via sensing their probe signal transmissions or lack thereof. For example, when the transmitter sends a probe signal to the mobile user, all the recruited relay nodes should forward their received probe signal to the mobile user. If any of these nodes refuse to forward, other nodes will not detect transmitted

power from the malicious nodes. Therefore, in order to detect if a particular relay node is performing its duty and participating in the cooperative transmission process, a simple binary hypothesis test based on received power levels can be conducted at all other nodes in a distributed fashion. For testing the j^{th} relay node, at time slot T, we can use the signal received by i^{th} relay node given by:

$$\begin{aligned} H_0 : Y_i &= \sum_l s_l + N_i; j^{th} \text{ relay node is not cooperating} \\ H_1 : Y_i &= \sum_l s_l + s_j + N_i; j^{th} \text{ relay node is cooperating} \end{aligned} \tag{5.1}$$

where, $i, j = 1, \ldots, M$ and $i \neq j$. H_0 and H_1 denote the hypotheses corresponding to whether the j^{th} relay node is forwarding the probe signal or not; $s_l, l \in M \backslash N$ (N is the number of non cooperative nodes) denotes the signal received from other cooperating relay nodes; s_j is the received signal from j^{th} relay node (target node), and N_i is the additive white Gaussian noise at i^{th} relay node. For simplicity in analysis, we assume all the noise terms are Gaussian distributed with zero mean and known variance σ^2. Since the probe signals are deterministic signals, we can write the distribution of Y_i as.

$$Y_i = \begin{cases} \sim N(\sum_{l=1}^{M \backslash N} s_l, \sigma^2); \text{ under } H_0 \\ \sim N(\sum_{l=1}^{M \backslash N} s_l + s_j, \sigma^2); \text{ under } H_1 \end{cases} \tag{5.2}$$

At i^{th} relay node, detected power under both hypotheses corresponds to

$$X_i = |Y_i|^2 = \begin{cases} P_{S_i} + P_{N_i} \sim \sigma^2 \chi^2(x; 1; \delta_0); \text{ under } H_0 \\ P_{S_i} + P_{s_j} + P_{N_i} \sim \sigma^2 \chi^2(x; 1; \delta_1); \text{ under } H_1 \end{cases} \tag{5.3}$$

where, P_{S_i} is the total received power (except j^{th} relay node) at i^{th} relay node, P_{N_i} is the noise power at i^{th} relay node, and P_{s_j} is the power of the received signal from

j^{th} relay node. We assume small scale fading power gain h_{ij} is i.i.d exponential distribution (Rayleigh fading); the path loss function is given by $g\left(d_{i,j}\right) = \|d_{i,j}\|^{-\alpha}$, where $\alpha > 2$ is the path loss exponent; d is the distance between communication parties. Therefore, the received power at the i^{th} relay node, from j^{th} relay node, can be written as $P_{T_{s_j}} h_{ji}. \|d_{ji}\|^{-\alpha}$, where $P_{T_{s_j}}$ is transmit power of the j^{th} relay node. Since the received signal is complex Gaussian as shown in equation (2), the distribution of our detected power corresponds to a non-central χ^2 with degrees of freedom $V_{0/1} = 1$ and noncentrality parameter $\delta_0 = (\frac{\sum_{l=1}^{M} s_l}{\sigma})^2$ and $\delta_1 = (\frac{\sum_{l=1}^{M} s_l + s_j}{\sigma})^2$ (denoted as $\chi^2(x; 1; \delta_0)$ and $\chi^2(x; 1; \delta_1)$, respectively). Therefore, each node can perform a binary hypothesis test based on the likelihood ratio. For example, the i^{th} relay node can compute the likelihood ratio for the test of the j^{th} node as

$$l_{i,j} = \frac{p_1(x)}{p_0(x)} \tag{5.4}$$

where, $p_1(x)$ and $p_0(x)$ are the density function corresponding to $\chi^2(x; 1; \delta_0)$ and $\chi^2(x; 1; \delta_1)$, respectively. These likelihood values serve as the basis of relay node reliability evaluations as explained in the following subsections.

Since every relay node is monitored by other relay nodes, it is important to note that our power sensing scheme not only works for the case of single non-cooperative node, but also works for multiple non-cooperative nodes. As we have explained earlier in this section, for a target node, there are $M - 1$ pair wise tests performed by other relay nodes, making it straightforward to extend this approach to detect multiple non-cooperative relay nodes.

5.2.1 One-shot Reliability Detection

In a one-shot measurement scheme, the task of interest is to decide whether the observation X (received power) is generated under H_0 or H_1. Typically, this is accomplished

by first forming a test statistic (e.g.,log likelihood ratio) and then comparing it with a predetermined threshold τ_l as follows.

$$L(x) = \log \frac{p_1(x)}{p_0(x)} \underset{H_0}{\overset{H_1}{\gtrless}} \tau_l \tag{5.5}$$

where, L is denoted as log likelihood ratio. If L is invertible, which is the case for the power sensing problem, the equivalent test is

$$X \underset{H_0}{\overset{H_1}{\gtrless}} \tau_x \tag{5.6}$$

where, $\tau_x = L^{-1}(\tau_l)$. In order to determine the threshold and quantify the performance of this binary decision process, two metrics namely, probability of detection P_D and probability of false alarm P_{FA} are commonly employed. P_D is the probability of detecting a signal from the target relay node when it truly is cooperating and corresponds to $P_D = Pr\{L(x) > \tau_l \mid H_1\} = Pr\{X > \tau_x \mid H_1\} = \int_{\tau_x}^{\infty} p_1(x)dx$ where, $p_1(x)$ is the probability density function (pdf) of scaled non-central χ^2 when H_1 is true. That is,

$$\begin{aligned} p_1(x) &= \sigma^2 f_X(x; k; \delta_1) \\ &= \frac{\sigma^2}{2} e^{-(x+\delta_1)/2} \frac{x}{\delta_1}^{(k/4-1/2)} I_{k/1-1}(\sqrt{\delta_1 x}), \end{aligned} \tag{5.7}$$

where, $I_v(x)$ is a modified Bessel function of the first kind. P_{FA} is the probability that the test incorrectly decides that the considered relay node is transmitting and it can be written as $P_{FA} = Pr\{L(x) > \tau_l \mid H_0\} = Pr\{X > \tau_x \mid H_0\} = \int_{\tau_x}^{\infty} p_0(x)dx$ where,

$p_0(x)$ is the pdf of scaled non-central χ^2 when H_0 is true, i.e.,

$$\begin{aligned} p_0(x) &= \sigma^2 f_X(x; k; \delta_0) \\ &= \frac{\sigma^2}{2} e^{-(x+\delta_0)/2} \frac{x}{\delta_0}^{(k/4-1/2)} I_{k/1-1}(\sqrt{\delta_0 x}) \end{aligned} \tag{5.8}$$

The optimum decision threshold τ_x can be found via a Neyman Pearson criterion that maximizes P_D subject to a constraint on P_{FA} [72]. However, this threshold evaluation is not trivial as there is no easy and accurate way to express the CDF ($F(x; k, \delta)$) of non-central χ^2 distributions [73] required to compute P_D and P_{FA}. An approximation based on the CDF of normal distribution has been proposed in [74]. That is

$$F(x; k, \delta) \approx \Phi(f(x)) \tag{5.9}$$

where $f(x) = \frac{(x/k+\delta)^h - (1+hp(h-1-0.5(2-h)mp))}{h\sqrt{2p}(1+0.5mp)}$, $h = 1 - \frac{2(k+\delta)(k+3\delta)}{3(k+2\delta)^2}$, $p = \frac{(k+2\delta)}{(k+\delta)^2}$ and $m = (h-1)(1-3h)$. Therefore, for $P_{FA} \leq \alpha$, we require that $1 - \sigma^2\Phi(f(x)) \leq \alpha$. Thus, we can approximate the threshold τ_x as $\tau_x = f^{-1}(\Phi^{-1}((1-\alpha)\frac{1}{\sigma^2}))$. At each relay node, either soft or hard decisions can be made. The log likelihood ratio value can be used as a soft decision metric that quantifies the degree of node non cooperation. For hard decisions, if the received power greater or equal to τ_x, the target node is considered as a cooperative relay node. Otherwise, the target node is deemed to be non-cooperative.

5.2.2 Dynamic Reliability Detection

An alternative approach to evaluating node reliability exploits historical behavior by relying on a Bayesian framework. Assume that it is possible to associate prior probabilities π_0 and π_1 for the hypotheses H_0 and H_1. The objective in this framework is to minimize the so-called Bayesian risk. According to [75], the Bayesian test corresponds

to,

$$l(x) = \frac{p_1(x)}{p_0(x)} \underset{H_0}{\overset{H_1}{\gtrless}} \frac{\pi_0(C_{10} - C_{00})}{\pi_1(C_{01} - C_{11})} \tag{5.10}$$

where, l is the likelihood ratio; C_{ij}, for $i = 0, 1$ and $j = 0, 1$, is the cost incurred by choosing hypothesis H_i when hypothesis H_j is true; π_j is the prior probability that hypothesis H_j is true unconditioned on the value x. A uniform cost assignment ($C_{11} = C_{00} = 0$ and $C_{10} = C_{01} = 1$) [76] is employed in this research.

In dynamic reliability detection, at each time instant, in order to minimize the Bayesian risk, we calculate the posterior probabilities ($\pi_0(x)$ and $\pi_1(x)$) given the power measurement $X = x$ and prior probabilities π_0 and π_1 (initially are assumed to be equally likely, i.e., $\pi_0 = \pi_1 = 0.5$). In a Bayesian framework, optimum decision is based on posterior probabilities, and we can think of our proposed dynamic node reliability metric evaluation scenario as being a mechanism for updating the prior probabilities of the hypothesis into posterior probabilities. In the next time slot, we employ the posterior probabilities calculated in previous time slot as the new prior probabilities. Thus, we can obtain the updated posterior probabilities for time slot 2 and so on. This process is described in Algorithm 4. The dynamic reliability detection algorithm involves the update of posterior probabilities by exploiting historical behavior (prior probabilities) based on a Bayesian framework. The calculated posterior probabilities are optimal at every step and does not involve any iterative computation. The steps mentioned in Algorithm 4, refer to time epochs. That is, while the metric is optimal in each step, over time, we incorporate historical behavior of cooperating nodes.

Similar to the one-shot scenario, both soft and hard decisions can be made in the dynamic scenario. In each time slot, the likelihood ratio can be employed as the soft decision statistic that quantifies the degree of node cooperation. Alternately, the $\pi_j(x), j = 0, 1$ can be treated as soft decisions characterizing the probability that a

Algorithm 4 Node Reliability Update Algorithm

Timeslot 0): Assume $\pi_0 = \pi_1 = \frac{1}{2}$

Timeslot 1): Calculate the posterior probabilities $(\pi_j(x), j = 1, 2)$ based on the prior probabilities using the following equation

$$\pi_j(x) = P(H_j \text{ is true} \mid X = x) = \frac{p_j(x)\pi_j}{\pi_0 p_0(x) + \pi_1 p_1(x)} \tag{5.11}$$

Timeslot 2): Let $\pi_j = \pi_j(x)$. Update the posterior probabilities $(\pi_j(x), j = 1, 2)$ using (11)

$\vdots$

Timeslot t): Set π_j based on posterior probabilities from time slot $t-1$, calculate posterior probabilities $(\pi_j(x), j = 1, 2)$ based on (11)

$\vdots$

Terminate at last time slot.

node is cooperative or not. In the hard decision case, we compare the posterior probabilities $(\pi_j(x))$ in each time slot. If $\pi_1(x)$ is greater or equal than $\pi_0(x)$, we consider the target node is cooperating. Otherwise, the target node is a non-cooperative node.

5.3 Centralized Reliability Evaluation

An alternative to node based evaluation is a centralized approach for characterizing reliability. Here, each node transfers their local node reliability information to a central server (e.g., basestation). It is important to note that the basestation is well suited to act as a central server in our proposed reliability evaluation scheme. The idea of reliability information fusion at a basestation is a natural choice in cellular network since every end user node and/or relay node exchange control plane information with the basestation on a consistent basis. Additionally, basestations are not typically power constrained and have adequate computational capacity to fulfill the role of a central server. Systematic fusion of data or decisions from relay nodes can be used to derive an overall reliability measure for all nodes in the network. This information is accessible to all nodes that seek to engage in cooperative communication. As shown in

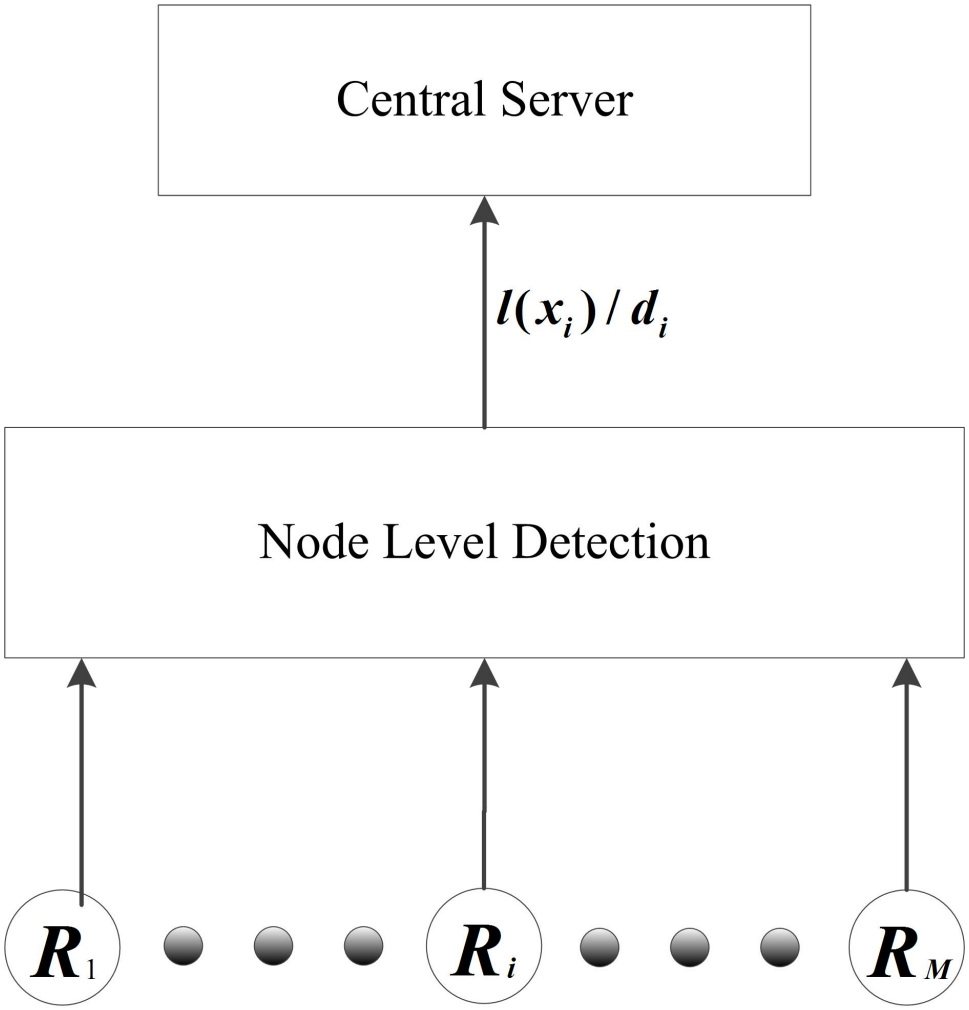

Figure 5.2: *Centralized Reliability Evaluation Scheme*

Fig. 5.2, in a data fusion scenario, relay nodes send the soft decisions, i.e., evaluated likelihood ratios to the central server. If one-shot reliability detection is deployed at each relay node independently, it is reasonable to write the likelihood ratio, to test whether i^{th} relay node is cooperating, as

$$l(\mathbf{x_i}) = \frac{p_1(\mathbf{x_i})}{p_0(\mathbf{x_i})} = \frac{\prod_{l=1}^{N} p_1(x_{il})}{\prod_{l=1}^{M-1} p_0(x_{il})} = \prod_{l=1}^{M-1} l(x_{il}) \tag{5.12}$$

where, x_{il} is the received signal from l^{th} relay node at target relay node (i^{th}). $l(x_i)$ is compared to a global threshold (τ_{iG}) to decide if the target node is cooperative. Applying one-shot reliability detection, the overall/global probability of false alarm corresponds to

$$\begin{aligned} P_{FA_G} &= \int_{l(\mathbf{x_i})>\tau_{iG}} p_0(\mathbf{x_i}) d\mathbf{x_i} \\ &\approx 1 - \sigma^{2(M-N)} \prod_i \Phi(f(\mathbf{x_i})) = g(\mathbf{x_i}) \end{aligned} \tag{5.13}$$

Based on a Neyman Pearson criterion where $P_{FA_G} \leq \alpha_G$, the global threshold can be calculated as $\tau_{iG} = g^{-1}(\alpha_G)$. In this manner, a global decision can be made at central server for each relay node. As we mention in section II, the proposed reliability evaluation scheme is implemented during the probing stage of PHY-SKG scheme. Therefore,a global decision on node reliability can be made when PHY-SKG scheme generate new secret keys. The frequency of generating new secret keys depends on the required security levels and the computational power available at the disposal of an adversary. If the system has a high security level requirement and/or the system faces a adversary with high computational power, we may need to generate secret keys more frequently. This in turn will lead us to a more frequent monitoring/calculation of node reliability.

In the dynamic case, the relay nodes send the corresponding data (such as prior probabilities, posterior probabilities and likelihood ratios) to the central server. The Bayesian test corresponding to the i^{th} relay node can be expressed as:

$$l(\mathbf{x_i}) = \frac{p_1(\mathbf{x_i})}{p_0(\mathbf{x_i})} = \prod_{l=1}^{N} \frac{p_1(x_{il})}{p_0(x_{il})} \underset{H_0}{\overset{H_1}{\gtrless}} \frac{\pi_{0_{Gi}}(C_{10} - C_{00})}{\pi_{1_{Gi}}(C_{01} - C_{11})} \tag{5.14}$$

where, $\pi_{j_{Gi}}$ is the overall/global prior probability that hypothesis H_j is true. Thus,

the posterior probabilities can be calculated as

$$\begin{aligned}\pi_{0_{Gi}}(\mathbf{x_i}) &= \frac{p_0(\mathbf{x_i})\pi_{0_{Gi}}}{\pi_{0_{Gi}}p_0(\mathbf{x_i}) + \pi_{1_{Gi}}p_1(\mathbf{x_i})};\\ \pi_{1_{Gi}}(\mathbf{x_i}) &= \frac{p_1(\mathbf{x_i})\pi_{1_{Gi}}}{\pi_{0_{Gi}}p_0(\mathbf{x_i}) + \pi_{1_{Gi}}p_1(\mathbf{x_i})}\end{aligned} \tag{5.15}$$

Applying a similar algorithm as shown in Algorithm 4, the central server can measure and monitor the reliability of relay nodes. Alternatively, the central server can also make a global decision by exploiting the local decision made by each relay node (decision fusion). As shown in Fig. 5.2, in decision fusion scenario, for both of one-shot and dynamic cases, each relay node makes a local decision (d_i) and communicates these decisions to the central server. Therefore, the central server can make a global decision using standard decision fusion rules such as majority voting, AND and OR rules [77].

We only consider a centralized scenario in this work. This is because the relay node reliability evaluation scheme is envisioned for every cooperative relay based transmission. A single cooperative link typically consists of one transmitter, one receiver, and a small set of relay nodes. Therefore, the scale of the network considered is not large. Consequentially, deployed in every single cell of co-op MIMO network. As introduced in section II, each cell of co-op MIMO network is not a large scale network. Therefore, a totally distributed implementation is not necessary.

5.4 Simulation Results

In this section, we present simulation results to illustrate the performance of our proposed node reliability evaluation schemes. The one-shot node level reliability evaluation is completely characterized via P_D and P_{FA} given in Eq. **??** and Eq. **??**. Therefore, the simulations mainly focus on the performance of dynamic node relia-

bility metric evaluation. In all simulations, a two-tier wireless network is considered. Both relay nodes and mobile users are distributed as homogenous Poisson Point Process (PPP) [78] with density $\lambda_R = 1.5$ and density $\lambda_U = 0.5$ (independent of relay nodes), respectively. The simulations focus on a single communication pair, where the target mobile user recruits 3 relay nodes. We assume the corresponding power fading parameter h_{ji} follows a exponential distribution with parameter 1 and path loss exponent $\alpha = 4$. We implement our proposed dynamic node reliability metric evaluation scheme for 20 time slots and repeat this simulation for 1000 realizations of the underlying PPP. We investigate two general malicious strategies of relay nodes: (1) periodic non cooperation and (2) random non cooperation. In addition,we analyze the reliability performance under different distance distribution between communication parties.

In a periodic non cooperation scenario, we assume that the target relay node is not cooperating in the first 5 time slots and works normally in the following 5 time slots. This node behavior repeats periodically. The performance of our proposed dynamic node reliability evaluation scheme is shown in Fig. 5.3. Subplot 5.3(a) shows the strategy of malicious relay nodes. Subplots 5.3(b), 5.3(c) and 5.3(d) indicate the performance of proposed dynamic node reliability evaluation scheme as a function of time instants when corresponding relay nodes (such as R_1, R_2 and R_3) are treated as malicious nodes. In order to illustrate the relationship in a proper way, we use the probability of cooperation as the performance metric. The simulation results demonstrate that, in the first 5 time slots, as the relay node is not cooperating, the performance metric decreases. In the following 5 time slots, the performance metric increases since the relay node works as expected. The observed variation of our reliability metric can be attributed to the Bayesian framework that incorporates the past history of relay node cooperation.

In random non cooperation scenario, we assume that the target relay node behavior

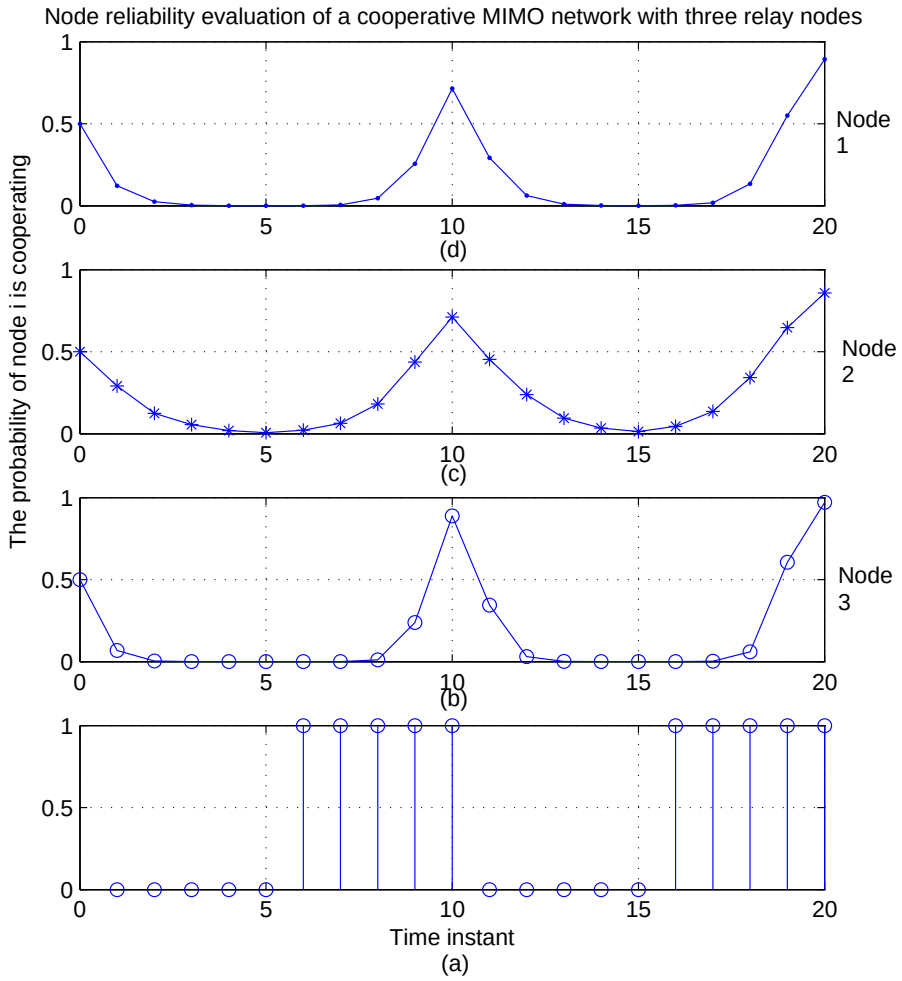

Figure 5.3: *Node reliability evaluation for relay node refuses to work periodically scenario*

is random. Fig. 5.4 and 5.5 indicate the performance of the proposed dynamic node reliability evaluation scheme. In the same manner, Subplot 5(a) indicates the malicious strategy of target relay node. Subplots 5.4(b), 5.4(c) and 5.4(d) represent the performance of the proposed reliability scheme when the corresponding relay node follows the malicious strategy. It is obvious that proposed reliability scheme adequately monitors the misbehavior of target relay nodes even in this random scenario. One phenomenon we want to point out is that in a certain period of time (such as from time slot 14 to time slot 18 as shown in Fig. 5.4), the reliability scheme indicates that

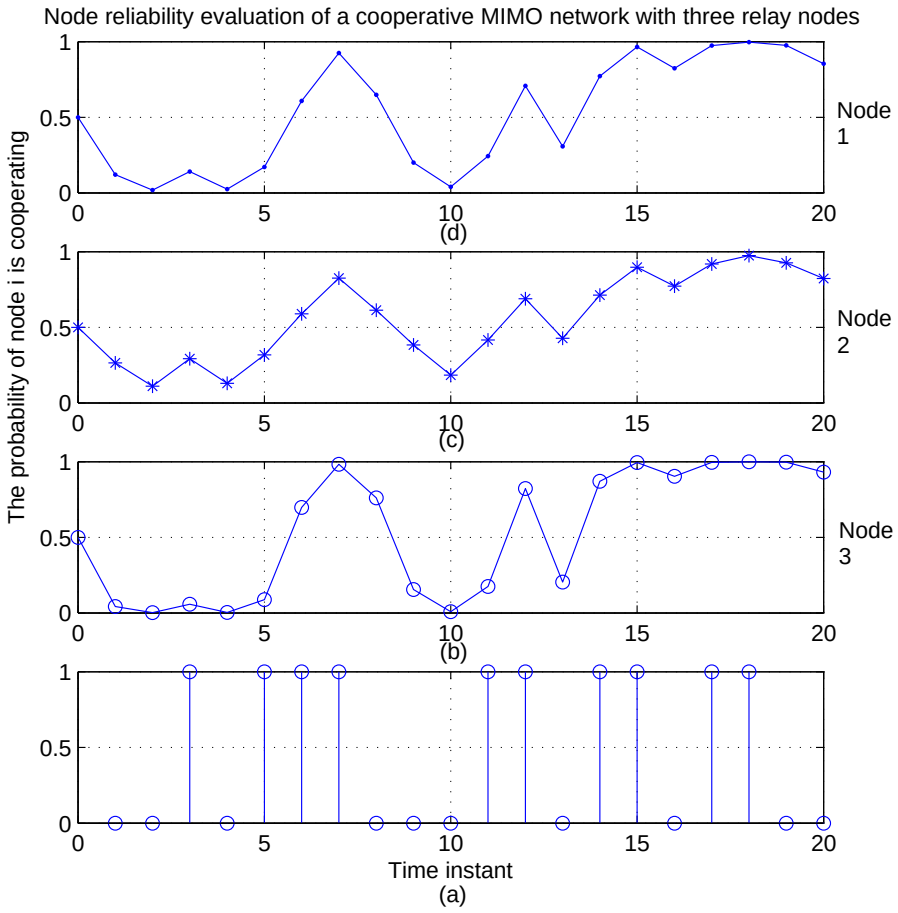

Figure 5.4: *Node reliability evaluation for relay node refuses to work randomly scenario*

the target relay node is cooperating. However, at time slot 16, the target relay node does not cooperate as shown in subplot 5.4(a). This momentary non cooperation does not significantly devalue the node's reliability metric as the node does show a history of cooperation prior to and post time slot 16. This feature mimics the evolution of trust amongst collaborators in a team where momentary non cooperation does not completely undo a history of positive cooperation. It is, however, incorrect to state that this history-aware approach fails to detect non cooperation. This is because, the reliability metric does decrease but does so in a gradual manner. Repeated non cooperation after maintaining a significant level of cooperation would be required to

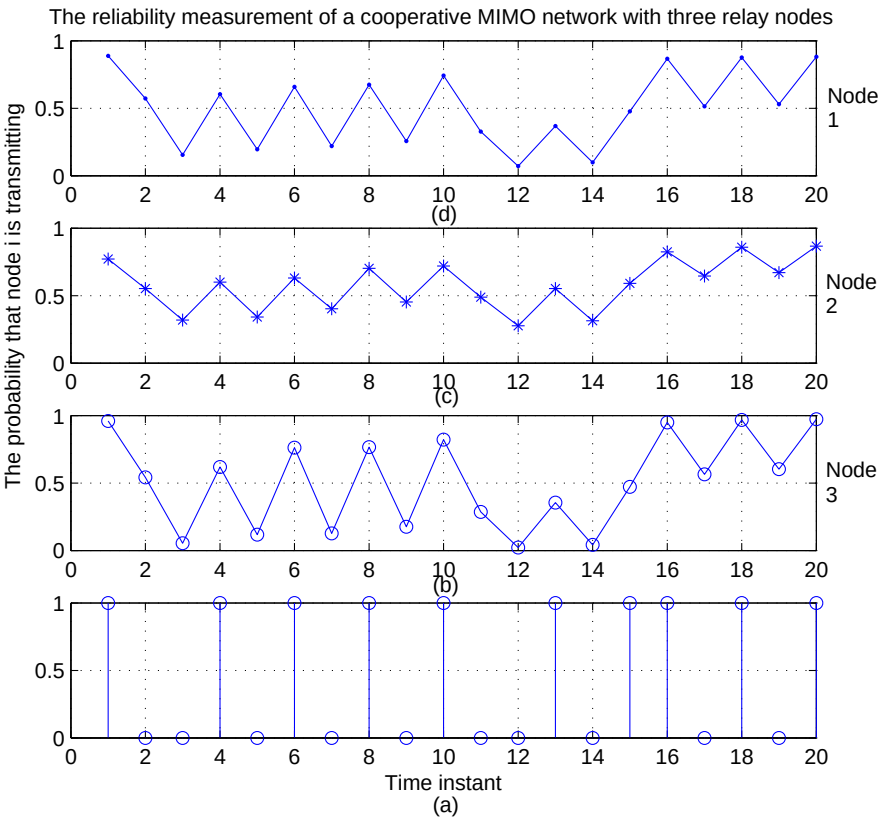

Figure 5.5: *Node reliability evaluation for relay node refuses to work randomly scenario*

break the trust earned and the reliability metric will degrade. Of course, depending on the preference of the system manager, one can adjust the rate of degradation of the reliability metric. For example, the classical Bayesian framework can be adapted to include "weights" that reflect a "forgetting" factor. This approach can ensure that the history of cooperation is not valued highly and momentary non cooperation will be immediately reflected in a poor reliability metric.

Since our node reliability evaluation scheme is based on a power sensing algorithm, both distance between relay nodes and transmit signal strength will impact the received power. For example, consider a scenario where the reliability of relay node A is being evaluated by relay node B and C that are at different distance from A. B and C node will arrive at different reliability metric values for node A. This vari-

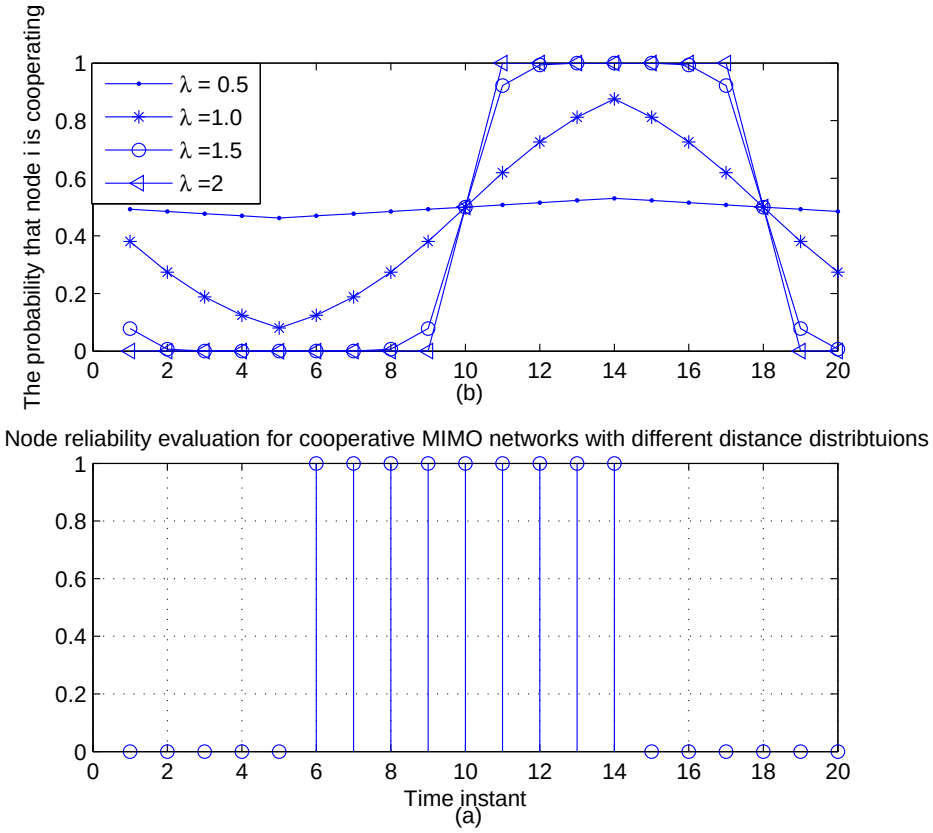

Figure 5.6: *Relationship between distance distribution and reliability performance*

ability further motivates the value of fusing reliability information at a central serve (e.g., at the basestation). This phenomenon is demonstrated in the simulation results. From Figs. 5.3, 5.4 and 5.5, we can observe that the exact performances metric (e.g., probability of cooperation) of dynamic node reliability evaluation schemes can vary widely depending on the target relay node. This is due to the variation in distance distribution among relay nodes that in turn impacts the received signal strengths that guide the power sensing based decision process. In order to present the relationship between reliability performance and distance distribution, we vary the relay node spatially distribution, Poisson point process (PPP), density (λ_R) from 0.5 to 2. The performance of node reliability evaluation scheme with different distance distributions are shown in Fig. 5.6. Subplot 5.6(a) presents the malicious behavior of target re-

lay node. Subplot 5.6(b) provides the reliability metric across the same time frame. As plot 5.6(b) indicates, increasing the density λ_R of PPP significantly improves the performance of reliability scheme. This is because the higher distribution density leads to a smaller distance between relay nodes and stronger received signals for the power sensing algorithm. In contrast, with increasing distance between relay nodes, the received power decreases, making it challenging for the power sensing algorithm to distinguish between background noise and the transmitted signals.

5.5 Conclusion

In this chapter, we propose novel relay node reliability evaluation schemes, including node level reliability detection and centralized reliability metric evaluation, for use in Co-MIMO networks. The reliability metrics stored in the central server can be used as a guide for mobile users interested in collaboration with relay nodes. Theoretical analysis and simulation results are presented to illustrate the proposed node reliability evaluation schemes. The reliability evaluation scheme used in conjunction with our previously proposed cooperative PHY-SKG strategies [42,70] can significantly enhance security of cooperative networks. Future work will focus on a more general scenario of misbehavior of relay nodes, built on time delay distribution of internal links estimated via network tomography.

Chapter 6

Chapter 6: Network Tomography based Node Reliability Evaluation in Cooperative MIMO Networks

Cooperative multiple input multiple output (co-op MIMO) networks proposed as one potential solution to meet our growing data rate requirements, allow mobile users to recruit low-power relay nodes to cooperate as virtual antenna arrays. Although co-op MIMO architectures offer significant performance improvement compared to traditional wireless networks, they are vulnerable to attacks. In this chapter, we propose a novel node reliability evaluation scheme that is based on the internal link characteristics among the cooperating nodes. While monitoring internal link characteristics such as link delay is usually challenging, we propose an active probe signal driven network tomography to estimate these characteristics based on end-to-end measurements. Specifically, by leveraging the probe signal transmissions involved in our previously proposed physical layer secret key generation schemes, we measure end-to-end delay in a coop MIMO network. Then, an expectation maximization (EM) algorithm is used to

derive a maximum likelihood estimate of the individual internal link delay characteristics. The effectiveness of the proposed node reliability evaluation is demonstrated via simulations of a single and two layer co-op MIMO network architecture. Simulation results demonstrate that our proposed node reliability evaluation scheme accurately identifies non-cooperative nodes.

6.1 Introduction

To meet the growing demand for wireless services, future 5G networks, must provide higher data rates, lower latency, enhanced security, reduced operating cost, multi-antenna support, flexible bandwidth operation, and seamless integration with existing systems. Cooperative multiple input multiple output (co-op MIMO) networks [1] [2], currently incorporated into 4G LTE , offer one potential solution for meeting these challenges [3]. A co-op MIMO network typically utilizes distributed antennas on multiple radio devices in order to boost network throughput, conserve energy, and improve network coverage. Co-op MIMO fundamentally groups multiple devices into virtual antenna arrays (VAAs) in order to emulate MIMO communications. A co-op MIMO transmission involves multiple points-to-point radio links, including links within a VAA and links between various VAAs. In practice, many wireless devices may not be able to support multiple antennas due to dimension, budget, and hardware limitations. Co-op MIMO networks allow these devices to reap the benefits provided by MIMO networks. Although a number of distinguished studies have focused on ways to improve wireless network performance by exploiting co-op MIMO architecture [4] [2] [1], security issues have often been overlooked.

Due to the broadcast nature of wireless channels and the open architecture of co-op MIMO networks, these networks are threatened by eavesdropping, message modification, and node impersonation. Previous research [20] [11] [5] indicate that tradi-

tional key-based enciphering techniques are limited by key distribution and computational complexity. Following the distinguished work by Shannon [58], wireless channel reciprocity-based physical layer secret key generation (PHY-SKG) techniques, which can generate keys with an information theoretic guarantee, have garnered attention in the wireless security community. In our previous research [70] [42] [43], we demonstrate that co-op MIMO architectures can improve physical layer security (e.g., wireless channel reciprocity-based PHY-SKG) by providing rich common randomness among wireless channels. Although co-op MIMO network provides benefits to performance and physical layer security, it is still vulnerable. Even if the transmitted information is secured, it is difficult but essential to monitor the behavior of relay nodes since mobile users are allowed to recruit relay nodes (i.e., idle users, femtocells, and picocells) during communication. Selfish or malicious intentions of relay nodes may manifest as non-cooperation. Selfish nodes may suddenly choose not to cooperate in order to preserve their resources or prioritize other services. Malicious nodes, on the other hand, may attempt to prevent communication between source and destination nodes at any cost, and an adversary may control malicious nodes in order to attack cooperative networks (i.e., denial of service attack at the physical layer). Therefore, understanding how to measure and monitor relay node reliability is one of the critical challenges in co-op MIMO architecture-based physical layer security schemes. In our previous research[Our under review paper], we propose a node reliability evaluation scheme based on power sensing. In this chapter, we attempt to evaluate relay node reliability based on internal link delay. However, internal link behavior between relay nodes in a co-op MIMO network is difficult to characterizeas only end-to-end measurements are typically available. Fortunately, sophisticated methods of active network probing or passive traffic monitoring can generate network statistics that indirectly relate to required performance metrics. Consequently, we can apply inference techniques, derived in the context of other statistical inverse problems, in order to extract the hidden

information of interest. Network tomography, a new method is considered a promising alternative to internal link delay estimation [79]. In this chapter, we demonstrate the feasibility of evaluating relay node reliability based on network tomography. Additionally, the node reliability evaluation used in conjunction with our previously proposed cooperative PHY-SKG scheme [70] [42] [43] can significantly enhance security of co-op MIMO networks.

In this research, we propose a new method to evaluate and characterize node reliability within a co-op MIMO architecture. While other performance criteria may be used, in this chapter, we focus on measuring node reliability via estimates of internal link delay. An active network tomography is implemented to estimate internal link delay based on measurement of end-to-end delays. It is easy to collect end-to-end delay measurements by leveraging the probing stage in our proposed PHY-SKG scheme [70] [42] [43]. Since link delays and occurrences of dropped packets are inherently random, it is reasonable to model the delays at each link as a independent multinomial distribution. An EM algorithm is developed for determining the maximum likelihood estimators (MLEs) of the delay distribution of internal links. Both theoretical analysis and simulation results are provided to demonstrate the performance of our proposed node reliability evaluation schemes. The results demonstrate that the proposed scheme accurately identifies the non-cooperative node. In addition, the proposed node reliability evaluation scheme used in conjunction with our previously proposed cooperative PHY-SKG strategies [70] [42] [43] can provide a cross-layer security scheme to significantly enhance security of cooperative networks.

6.2 Network Tomography

Network tomography is considered a potential approach to monitor large-scale networks. Network tomography is a statistical methodology to infer internal link char-

acteristics by exploiting observed end-to-end characteristics. Compared to the traditional expensive direct measurement method, network tomography allows for a cheap, indirect way to monitor large-scale networks without impacting network load. [79] presents an excellent overview of network tomography and recent developments in the area. Implementation of network tomography in order to infer internal network characteristics is illustrated in [80]. In this section, we describe how network tomography can be used in the context of co-op MIMO networks.

A wireless network with a tree topology is shown in Fig. 6.1. The root node represents the base-station, the leaf nodes denote the end users, and the other nodes are relay nodes deployed to assistant connection between the base-station and end users. We consider a connection between two nodes to be a path. We define a link as a direct connection with no intermediate nodes, thereby allowing a path to consist one or more links, e.g., a path between the root node and a end user may consist of three links. Depending on the problem and level of abstraction, the links can be unidirectional or bidirectional. Information is exchanged by sending signals along a path from base-station to end users.

Two forms of network tomography are considered in the research community: network delay tomography [81] and traffic demand tomography [82]. Network delay tomography focuses on estimation of link-level characteristics, consisting of counts of packets transmitted and/or received between source and destination nodes or time delays between packet transmissions and receptions based on end-to-end measurements. The goal of network delay tomography is to estimate the loss rate or queuing delay on each link. Traffic demand tomography primarily focuses on predicting end-to-end path-level traffic intensities (i.e., how much traffic originated from a specified node and was destined for a specified receiver) based on link-level traffic measurements such as counts of packets that pass through nodes in the network. Based on characteristics of each tomography, we can also classify network tomography as active tomography and

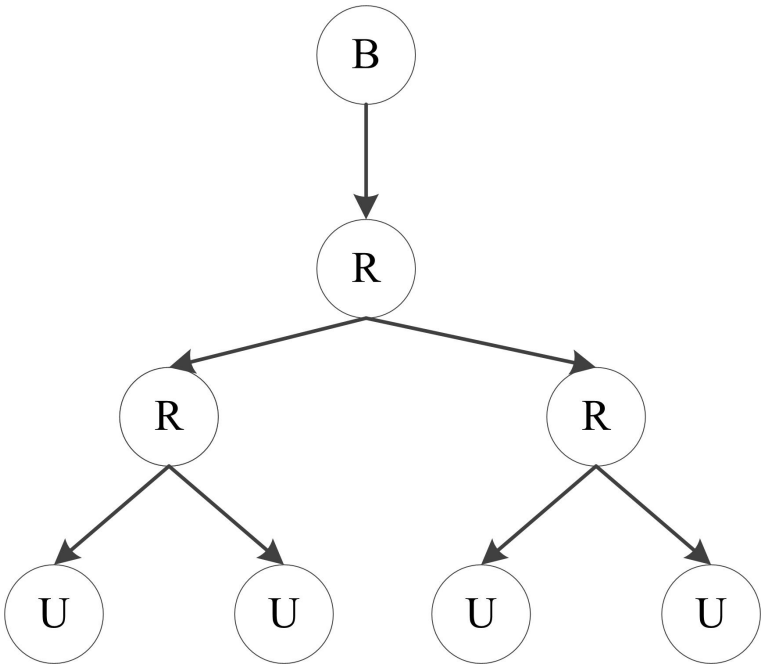

Figure 6.1: *Four-leaf tree topology*

passive tomography [83], respectively. In active tomography, we actively probe the network by sending signals from a base-station to several end users, and end-to-end path-level performance information is easily collected. The goal of active tomography is to estimate individual link-level information by exploiting path-level information. However, probing in active tomography may disturb normal network traffic. In passive tomography, we infer network performance information from passive observations of normal network traffic. The most common application is estimation of the origin-destination traffic matrix of a network [81]. Compared to active tomography, passive tomography does not introduce wasteful traffic. However, it does inevitably waste limited computation and storage resources and causes delays [84] because there is a need to collect large amounts of traffic data in order to derive performance information. In addition, passive tomography is not suitable for dynamic networks.

In this chapter, we are interested in reliability evaluation of relay nodes in co-op MIMO networks that can be dynamic in nature. Therefore, we restrict our attention

to active tomography. Additionally, our previously proposed PHY-SKG scheme lends itself naturally to probe-based active tomography. In PHY-SKG, we implement an active probing step in order to generate secret keys by exploiting randomness between wireless channels. Therefore, we can collect corresponding data (such as end-to-end delay measurements) from the probing step in the PHY-SKG to avoid disturbing the regular network traffic. Since link delays and occurrences of dropped packets are inherently random, statistical methodologies for large-scale network inference and tomography is preferred. In general, the network tomography problem can be roughly approximated via a linear model:

$$\mathbf{Y} = \mathbf{A}\mathbf{X} + \delta \tag{6.1}$$

where $\mathbf{X}$ is the vector of independent but unobserved internal delays over each internal link with dimension of $L \times 1$ (as shown in Fig. 6.2(a)) and $\mathbf{Y}$ is the vector of observed path-level delays (as shown in Fig. 6.2(b)) at each end receiver with a dimension of $P \times 1 (P < R)$. $\mathbf{A}$ is $P \times L$ routing matrix with elements 0 or 1 determined by network topology; δ is a noise vector with zero mean and finite variance.

A toy example to illustrate our approach is given as follows. As shown in Fig. 6.1, probe signals are sent from root node (base-station) to leaf nodes (end users) through a four-leaf tree topology. Let X_i denote the link delay for each internal link. Y_1 to Y_4

represents end-to-end delays from root node to leaf nodes, respectively, resulting in

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \\ X_6 \\ X_7 \end{pmatrix} + \begin{pmatrix} \delta_1 \\ \delta_2 \\ \delta_3 \\ \delta_4 \end{pmatrix} \tag{6.2}$$

The goal of active network tomography is to estimate the distribution of $\mathbf{X}$ given independent observations from the distribution of $\mathbf{Y}$. It is easy to observe that L is usually much larger than P in co-op MIMO networks and the problem is ill-posed for matrix inversion.

6.3 Estimation of Internal Links Delay Distribution in Cooperative MIMO Networks

As mentioned in Section II, our research focuses on active network tomography where delay distribution of internal links are considered to reflect the reliability of relay nodes. Therefore, in this section, we concentrate on estimating delay distribution of internal links by exploiting network tomography.

We transfer the physical network model shown in Fig. 2.3 into a graph model, as presented in Fig. 6.2(a). In this specific cell, we assume that R relay nodes and P end receivers are deployed. Fig. 6.2(b) shows the logic network model (path level) of the co-op MIMO network. By leveraging the probing stage of our previously proposed PHY-SKG scheme, we are able to identify network topology and to collect delay dis-

tributions from end-to-end users simultaneously without increasing redundancy such as overheads. Based on the knowledge of network topology (Matrix A) and delay distributions from end-to-end users, it is feasibly to implement an active network topography to infer the delay distribution of internal links, which can be used as an indicator of reliability of corresponding relay nodes. Comparison of the original delay distribution with respective estimated delay distribution of each internal link allows us to scale difference as the reliability metric of corresponding relay node. Details of an active network tomography scheme are shown as below.

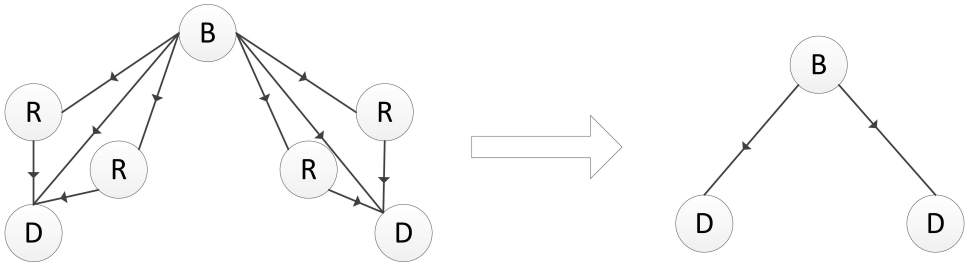

Figure 6.2: *(a) graph model of co-op MIMO networks. (b) logic model of co-op MIMO networks.*

In general, the network tomography problem can be roughly approximated as a linear model as mentioned in Section II (without considering noise):

$$\mathbf{Y} = \mathbf{AX} \tag{6.3}$$

In previous research [85], elements in $\mathbf{X}$, X_l, are assigned from finite possible values $[0, q, 2q, ..., mq]$, where q is bin width and m is a constant. Therefore, X_l is a discrete random variable whose possible values are $[0, q, 2q, ..., mq]$ with probability of $\mathbf{p_l} = [p_{l0}, p_{l1}, p_{l2}, ..., p_{lm}]$. Therefore we can write X_l as

$$X_l \sim f_l(p_l) \tag{6.4}$$

where f_l is the probability mass function (pmf).

In order to infer link-level delay of each internal link, our goal is to find a maximum likelihood of $\mathbf{p_l}$. However, a direct calculation of MLE is not feasiable. This is because, while $\mathbf{Y}$ is observed, $\mathbf{p_l}$ is a probability distribution of unobserved parameters $\mathbf{X}$. Therefore, we treat this problem as a missing data problem. We assume $\mathbf{Z}$ as the complete data, including $\mathbf{X}$ and $\mathbf{Y}$. The likelihood function of complete data can be expressed as

$$l(\mathbf{Z};\mathbf{p}) = l(\mathbf{X},\mathbf{Y};\mathbf{p}) = f(\mathbf{Y} \mid \mathbf{X}) l(\mathbf{X};\mathbf{p}) \tag{6.5}$$

where $f(\mathbf{Y} \mid \mathbf{X})$ is the conditional probability density function (pdf) of $\mathbf{Y}$ given $\mathbf{X}$ and $l(\mathbf{X};\mathbf{p})$ is the likelihood function of $\mathbf{X}$. Since the pdf does not depend on parameter $\mathbf{p}$, if we are able to measure the unobserved data, then the maximum likelihood estimators we seek will be trivially obtained by maximizing the complete data likelihood. Therefore, maximization of $l(\mathbf{X};\mathbf{p})$ should be equivalent to the solution that maximizes $l(\mathbf{Z};\mathbf{p})$. We solve the MLEs of $l(\mathbf{X};\mathbf{p})$ instead of $l(\mathbf{Y};\mathbf{p})$ in this problem.

We model X_i as a multinomial distribution with K bins, with the pmf corresponding to

$$p(\mathbf{X} \mid \mathbf{p}) = \prod_{k=1}^{K} p_k^{X_k}. \tag{6.6}$$

Considering a scenario with T time slots, we have T independent observations. Therefore, the likelihood $l(\mathbf{X};\mathbf{p})$ is

$$l(\mathbf{X_1},\ldots,\mathbf{X_T} \mid \mathbf{p}) = \prod_{t=1}^{T}\prod_{l=1}^{L}\prod_{k=1}^{K} p_{lk}^{X_{ltk}} = \prod_{l=1}^{L}\prod_{k=1}^{K} p_{lk}^{\sum_{t=1}^{T} X_{ltk}} \tag{6.7}$$

and log-likelihood corresponds to

$$L(\mathbf{X_1},\ldots,\mathbf{X_T} \mid \mathbf{p}) = \sum_{l=1}^{L}\sum_{k=1}^{K}(\sum_{t=1}^{T} \mathbf{1}_{X_{lt}=kq}) \log p_{lk} \tag{6.8}$$

We assume $n_{lk} = \sum_{t=1}^{T} \mathbf{1}_{X_{lt}=kq}$ is the number of packets (out of all packet pair mea-

surements) that experience a delay of k on link l.

In order to arrive at the MLEs, an expectation maximization (EM) algorithm is implemented. Let $\mathbf{p^i}$ be the parameter estimated in the i^{th} step of EM algorithm. Therefore, the target function to be maximized in the $\mathbf{p^{i+1}}$ step is

$$Q(\mathbf{p^i}, \mathbf{p^{i+1}}) = \sum_{l=1}^{L} \sum_{k=1}^{K} \log p_{lk} E_{\mathbf{p^i}}(\sum_{t=1}^{T} \mathbf{1}_{X_{lt}=kq} \mid \mathbf{Y_t}) \tag{6.9}$$

The E-step corresponds to

$$\tilde{n}_{lk} = E_{\mathbf{p^i}} \left[\sum_{t=1}^{T} \mathbf{1}_{X_{lt}=kq} \mid \mathbf{Y_t} \right] \tag{6.10}$$

The M-step is to update $\mathbf{p^i}$ by

$$p_{lk}^{i+1} = \frac{\tilde{n}_{lk}}{\sum_{r \in R} \tilde{n}_{lr}} \tag{6.11}$$

where $R = \{0, 1 \ldots, m, \infty\}$. Therefore, the EM algorithm can be summarized as follows:

Algorithm 5 Expectation Maximization Algorithm

```
1: procedure EM
2:     Initialize p^0 and generate delay distribution of end-to-end node Y_t using p^0
3:     for each link do
4:         for each bin do
5:             compute ñ_lk = E_{p^i}(Σ_{t=1}^{T} 1_{X_lt=kq} | Y_t)
6:             update p_lk^1 = ñ_lk / Σ_{r∈R} ñ_lr
7:         end for
8:     end for
9:     Iterate the above steps until converge
10: end procedure
```

Previous research [79] indicates that the likelihood computation involves high order convolution, that is computationally expensive, especially when the dimension of $\mathbf{X}$

is high. [86] propose a pseudo likelihood approach to decrease computational expense by forming simple subproblems and constructing a product of marginal likelihood of subproblems by ignoring their dependencies, resulting in a good balance between computational complexity and statistical efficiency of the parameter estimation. [87] proposes a novel mixture model for link delays and develops a fast algorithm for estimation based on the general method of moments. [88] propose a new estimation approach for solving a class of inverse problems in network tomography based on marginal distributions of a sequence of one-dimensional linear projections of observed data. Fortunately, implementation of network tomography in co-op MIMO networks does not suffer from this computational complexity problem. Although, co-op MIMO networks are consider to be large-scale networks, the entire network can be divided into small co-op networks, as shown in Fig. 2.3. Therefore, the above simple delay estimation scheme can be deployed to each small network in order to avoid high computational complexity.

6.4 Reliability Evaluation

In order to determine if a node is cooperative, we use a decision statistic that is a function of the distance D between estimated $\hat{\mathbf{p}}$ and the "nominal/true" delay distribution $\mathbf{p_t}$. We can use different measures such as L_1, L_2 and Kullback-Leibler distance to calculate D. That is $D_{L_1} = |\hat{\mathbf{p}} - \mathbf{p_t}|$ or $D_{L_2} = \|\hat{\mathbf{p}} - \mathbf{p_t}\|$ or $D_{KL} = \sum_i \hat{p}(i) \log \frac{\hat{p}(i)}{p_t(i)}$. The binary hypothesis test then corresponds to

$$\begin{aligned} H_0 &: D \leq \tau; \text{target node is cooperative} \\ H_1 &: D > \tau; \text{target node is non-cooperative} \end{aligned} \tag{6.12}$$

In order to determine the decision threshold τ, we can use a Neyman Pearson criterion

where we limit the probability of false alarm and maximize probability of detection. This approach requires knowledge of the distribution of the decision statistic under H_o and H_1. For some measures such as the L_2 distance, the asymptotically properties of MLE can be used to infer that D is asymptotically normal with mean 0 under H_0 and non-zero mean d under H_1.

6.5 Simulation Results

In this section we present simulation results to illustrate the performance of our proposed node reliability evaluation schemes. Two network models, shown in Fig. 6.3, are investigated: (1) simple co-op network and (2) multi-layer co-op network.

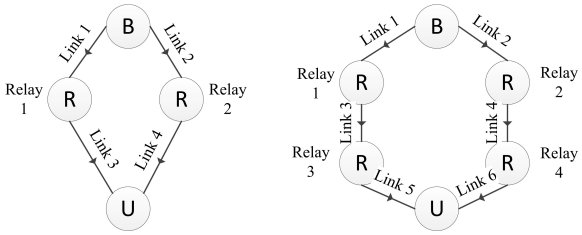

Figure 6.3: *(a) a simple co-op network model. (b) a multi-layer co-op network.*

Since we primarily focus on evaluating reliability of relay nodes, it is reasonable to assume that base-station is a reliable node. Based on this assumption, all the internal links which connect to the base-station are considered as reliable links. Therefore, if we detect any abnormal delay distribution from a specific link other than these links, the corresponding relay node (i.e., subroot relay node connected by the link) can be detected as a non-cooperative node. For the simple cooperative network, we assume that one layer of relay nodes (two node) are deployed in order to assist communication between base-station and end user, as shown in Fig. 6.3.(a). Since the base-station is treated as reliable node (link 1 and link 2 should be reliable links), we only focus on estimate the delay distribution of Link 3 and Link 4. Thus, for each internal link

we assume the bin width $q = 1$, and the number of bins is set to 3. The initial values of delay distribution of each link are : $p_3^0 = [2/15, 7/15, 6/15]$, $p_4^0 = [9/18, 3/18, 6/18]$. We set the true delay distribution of each link to be $p_{t3} = [1/7, 2/7, 4/7]$, $p_{t4} = [2/5, 2/5, 1/5]$. Therefore, based on these prior knowledge, in order to estimate the delay distribution of each internal link, an EM algorithm is applied.

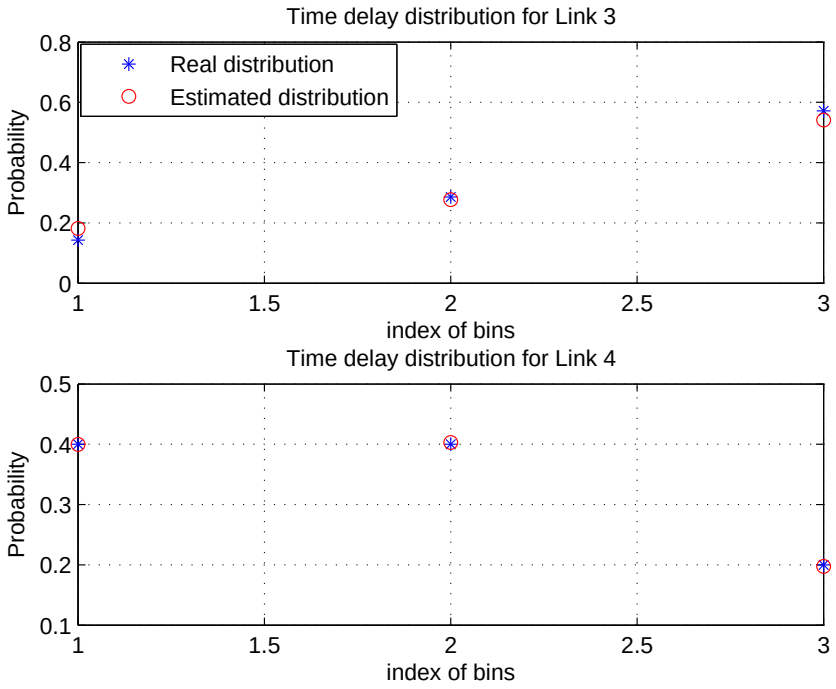

Figure 6.4: *Performance of proposed network tomography (estimated delay distribution)*

Fig. 6.4 shows delay distribution estimates of the two internal links along with their true delay distribution in one of the 50 independent simulations. 6.4 demonstrates the accurately identification of our proposed internal delay distribution estimation scheme for a simple co-op network. Table 6.1 shows the L_1 error norm of estimated delay

Table 6.1: *Averaged L_1 norm error of estimated delay distribution*

Links	L_1 norm error
Link 3	0.0417
Link 4	0.0012

distribution for each link, as averaged over 50 independent simulations. For each link, the L_1 error norm is simply the sum of the absolute differences between probability estimates and true probabilities. As a common measure of the performance of density estimates, the L_1 error norm enjoys several theoretical advantages, as discussed in [89]. The plot shows that the proposed network tomography technique demonstrate good estimation performance for tracking link delay distributions in a simple co-op network scenario.

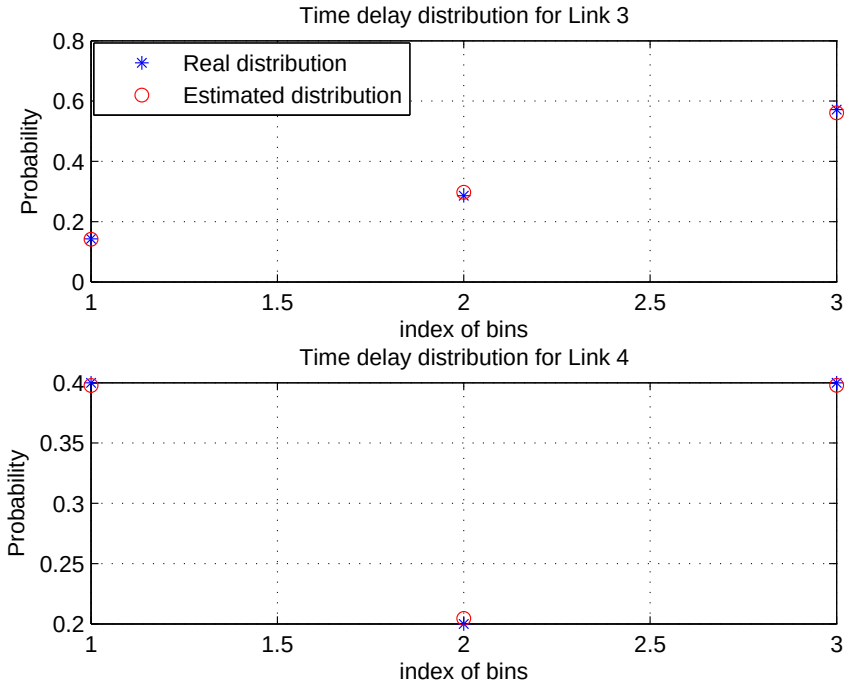

Figure 6.5: *Estimated delay distribution of non cooperative scenario (Link 2)*

In order to demonstrate node reliability evaluation of our proposed scheme, we assume that link 4 has an abnormal delay distribution: $p_{t4} = [2/5, 1/5, 2/5]$. The estimated delay distribution of internal links along with their true delay distribution are shown in Fig. 7. As shown in the figure, our algorithm accurately estimates the abnormal delay distribution of link 4.

Table 6.2 illustrates the distance between estimated delay distribution of a simple

cooperative network (link 4 is the abnormal link) in cooperative and non-cooperative scenarios by measuring in L_1 norm, L_2 norm, and absolute KullbackLeibler (KL) distance. All measurements demonstrate a significant difference at link 4 providing us the ability to identify the non cooperative node as relay node 2.

Table 6.2: *Reliability Evlauation*

Links	L_1 norm error	L_1 norm error	Absolute KL distance
Link 3	0.0668	0.0466	0.0316
Link 4	0.3967	0.2798	0.1377

For the multi-layer co-op network, we assume that two layers of relay nodes (two nodes at each layer) are deployed to assist communication between the base-station and end user. As shown in Fig. 6.3(b), we attempt to infer delay distribution of 4 internal links since the base-station is considered as a reliable node. Thus, for each internal link we assume that the bin width to be $q = 1$, and the number of bins is set to 3. The initial value of delay distributions of each link are : $p_3^0 = [5/15, 2/15, 8/15]$, $p_4^0 = [9/19, 4/19, 6/19]$, $p_5^0 = [2/11, 6/11, 3/11]$, and $p_6^0 = [4/17, 5/17, 8/17]$. We set the real delay distribution of each link to be $p_{t3} = [3/8, 1/8, 4/8]$, $p_{t4} = [5/9, 2/9, 2/9]$, $p_{t5} = [1/7, 4/7, 2/7]$, and $p_{t6} = [3/11, 2/11, 6/11]$. Based on these prior knowledge, in order to estimate the delay distribution of each internal link, an EM algorithm is implemented.

Fig. 6.6 shows delay distribution estimates of four internal links along with their true delay distribution in one of the 50 independent simulations. Based on our prior knowledge that link 4 and link 6 work properly, Fig. 6.6 demonstrates that our proposed node reliability evaluation scheme performs good for multi-layer co-op MIMO networks as well. Table 6.3 shows the L_1 error norm of estimated delay distribution for each link, as averaged over 50 independent simulations. The plot shows that the proposed network tomography technique demonstrate a good estimation performance for tracking link delay distributions in multi-layer co-op network scenario as well.

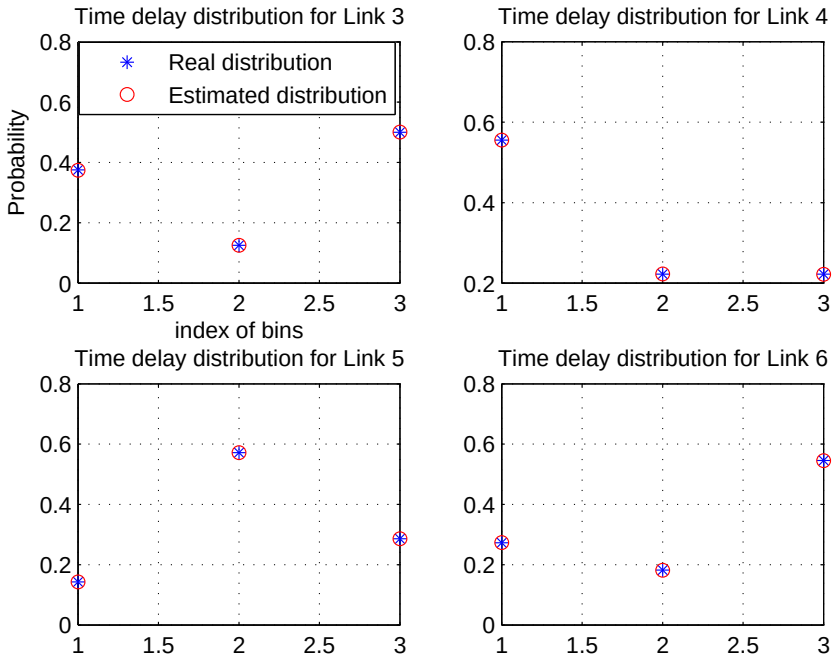

Figure 6.6: *Performance of proposed network tomography (estimated delay distribution)*

Table 6.3: *Averaged L_1 norm error of estimated delay distribution*

Links	L_1 norm error
Link 3	0.0016
Link 4	0.0008
Link 5	0.0003
Link 6	0.0020

Similar to the simple co-op MIMO scenario, in order to demonstrate node reliability evaluation of our proposed scheme for multi-layer co-op MIMO, we assume that link 5 has an abnormal delay distribution: $p_{t5} = [1/9, 5/9, 3/9]$. The estimated delay distribution of internal links along with their true delay distribution are shown in Fig. 6.7. As shown in the figure, our algorithm accurately estimated delay distribution of internal links. Table **??** illustrates the distance between estimated delay distribution of a multi-layer cooperative network (link 5 is the abnormal link) in cooperative and non-cooperative scenarios by measuring in L_1 norm, L_2 norm and, absolute Kullback-

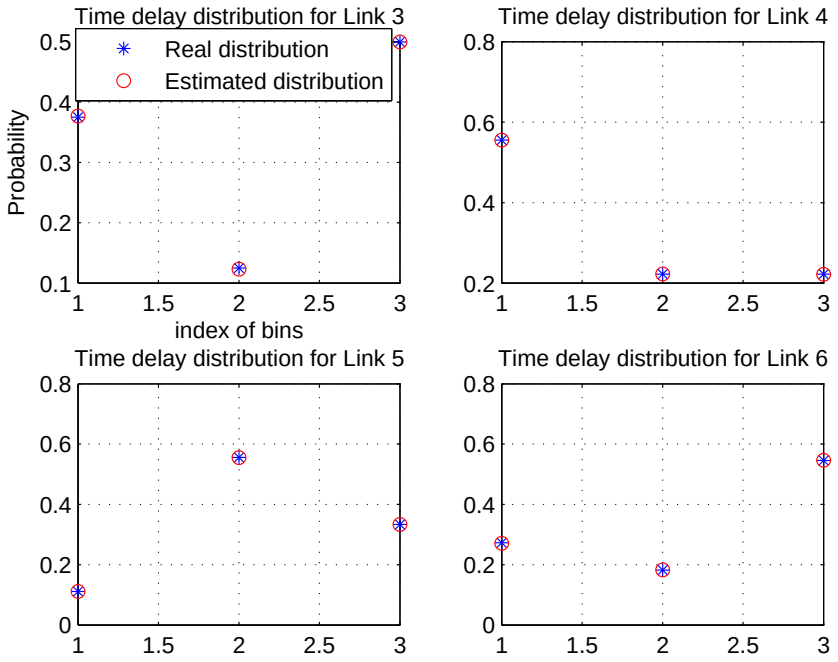

Figure 6.7: *Estimated delay distribution of non cooperative scenario (Link* 3*)*

Leibler (KL) distance. All measurements demonstrate a significant difference at link 5 providing us the ability to identify the non cooperative node as node 3.

Table 6.4: *Reliability Evlauation*

Links	L_1 norm error	L_1 norm error	Absolute KL distance
Link 3	0.0013	0.0009	0.0007
Link 4	0.0018	0.0013	0.0009
Link 5	0.0955	0.0594	0.0442
Link 6	0.0032	0.0021	0.0016

6.6 Conclusion

In this chapter, we propose an innovative reliability evaluation scheme for relay nodes within a co-op MIMO architecture. We employ internal link delay distribution as the measurement for node reliability. In order to estimate/infer internal link characteris-

tics, we implement an active probing network tomography by exploiting end-to-end delay characteristics. These delay characteristics can be collected by leveraging the probe signal transmissions involved in PHY-SKG schemes. Based on measuring end-to-end delays, we estimate the internal link delay characteristics via a maximum likelihood approach. An EM algorithm is developed to maximize the log-likelihood. Simulation results illustrate the applicability of the proposed reliability evaluation scheme for two scenarios of co-op MIMO networks. Results demonstrate that our proposed reliability evaluation scheme accurately identifies the non-cooperative node in both scenarios.

Chapter 7

Conclusion and Future Work

This chapter concludes the dissertation with a summary of research results and future research directions.

7.1 Summary

This dissertation proposes novel PHY-SKG strategies for co-op MIMO networks to address the low SKGR issues (the primary limitation of the PHY-SKG scheme) . In order to further improve the security level of dynamic wireless networks, innovative reliability evaluation schemes are proposed to measure and monitor the behavior of relay nodes using power sensing and network tomography. The proposed node reliability evaluation schemes used in conjunction with proposed cooperative PHY-SKG strategies represent a novel cross-layer security protocol that can significantly enhance security of cooperative networks. Key research contributions of this dissertation are summarized as below.

– The co-op MIMO structure is exploited to design and implement a physical layer (PHY-layer) security scheme for LTE-A networks. Specifically, two relay-based

co-op MIMO architectures are considered, and novel PHY-SKG schemes are proposed for those cases.

- A physical layer security scheme for point-to-point networks is introduced, and this scheme is extended to MIMO networks. Two practical relay-based co-op MIMO architectures and corresponding PHY-SKG schemes are presented. For both the MIMO and co-op MIMO networks, the impact of proposed power allocation on SKGR is quantified via theoretical and numerical analysis.
- A novel node reliability evaluation scheme is proposed to enhance the security of co-op MIMO networks. Leveraging probe signal transmissions involved in PHY-SKG schemes, two distributed node level reliability detection methods (one-shot and dynamic) are proposed to detect relay nodes that are non-cooperative. Based on the fusion of information from relay nodes, an overall reliability evaluation can be accomplished at base station. Mobile users interested in collaboration can access this information to determine which nodes to recruit for cooperation.
- A novel node reliability evaluation scheme based on internal link characteristics among cooperating nodes is proposed. While monitoring internal link characteristics such as link delay is usually challenging, an active probe signal driven network tomography is proposed to estimate these characteristics based on end-to-end measurements (by leveraging probe signal transmissions involved in previously proposed PHY-SKG schemes). An EM algorithm is employed to derive a maximum likelihood estimation of individual internal link delay characteristics.

Based on the research accomplished in this dissertation, future research directions are highlighted in the next section.

7.2 Future Work

Many open problems exist in the domain of MIMO and co-op MIMO based SKG schemes and node reliability evaluation schemes. This dissertation provides a brief overview of a few selected approaches, the associated key generation rates and corresponding node reliability evaluation schemes. However, no security scheme is foolproof and no security protocol is completely secure. Our proposed physical layer security schemes have weaknesses as well. Some drawbacks of our approach and how the proposed schemes can be attacked are briefly introduced in this subsection. Based on these vulnerabilities, a plethora of new problems and a rich set of fundamental questions could still be addressed. A subset of possible directions is presented below.

- As we mentioned in Chapter 1, theoretically, eavesdroppers experience independent physical channels from legitimate users as long as they are a few wavelengths away from legitimate nodes. However, in practical experiment [], researcher claim that eavesdroppers are able to estimate a partial amount of CSI. Therefore, it is reasonable to assume that eavesdroppers can estimate the entire CSI, thereby eavesdropping transmitted information between communication parties. Consequentially, how to minimize the leaked information is one of the topic that we are interested in.
- Interference attack is considered as one of the most dangerous attack for wireless communication. Instead of eavesdropping transmitted information, the attacker is trying to terminate the wireless communication by injecting strong interference/noise. It is very difficult to prevent this kind of attack; however, for SKG via wireless fading channel, interference enhances the variation of wireless fading channel and increases common randomness between communication parties. Therefore, it is reasonable to investigate how to utilize to increase SKGR by applying advanced interference alignment techniques or artificial noise/interference

injection techniques. In addition, large-scale networks such as multi-cell co-op MIMO networks which are suffered by the interference can reap the benefits of this topic as well.

- In this dissertation, the assumption is made that Eve, as an eavesdropper, is a passive attacker. Based on this assumption, SKG strategies were proposed to protect communication between parties. However, if active eavesdroppers are present in the communication system, the proposed security schemes may fail. Therefore, topics concerning physical layer security schemes for wireless communication under active attack are beneficial for further research.
- As illustrated in this dissertation, common randomness and subsequent SKGR can be enhanced by exploiting co-op MIMO schemes. However, implementation of any co-op MIMO scheme requires local communication and synchronization overhead. Therefore, a trade-off exists between cost for cooperation as captured via synchronization/overhead costs and SKG performance. How to balance this trade-off may be a potential direction for future research.
- In this dissertation, the assumption is made that the base station and end users are considered to be reliable nodes. Based on this assumption, determining which relay nodes are non-cooperative nodes is relatively easy. However, if an attacker can hack the basestation or end user, how can we protect the entire communication network? Therefore, a more intelligent method is needed to locate misbehaving nodes based on non-cooperative links when base station and end node user are treated as potential selfish or malicious nodes.
- How to implement machine learning and artificial intelligence techniques into the proposed reliability evaluation schemes to automatically detect and locate the non-cooperative relay node is a problem that is worth investigating.

Bibliography

[1] A. Nosratinia, T. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *Communications Magazine, IEEE*, vol. 42, no. 10, pp. 74–80, Oct 2004.

[2] D. Nguyen and M. Krunz, "Cooperative mimo in wireless networks: recent developments and challenges," *Network, IEEE*, vol. 27, no. 4, pp. 48–54, July 2013.

[3] C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. Aggoune, H. Haas, S. Fletcher, and E. Hepsaydir, "Cellular architecture and key technologies for 5g wireless communication networks," *Communications Magazine, IEEE*, vol. 52, no. 2, pp. 122–130, February 2014.

[4] H. Taoka, S. Nagata, K. Takeda, Y. Kakishima, X. She, and K. Kusume, "Mimo and comp in lte-advanced," *NTT DOCOMO Technical Journal*, vol. 12, no. 2, pp. 20–28, 2012.

[5] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[6] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[7] F. Osorio, "State of wireless security implementations in the united states and europe - empirical data," in *Malicious and Unwanted Software, 2008. MALWARE 2008. 3rd International Conference on*, Oct 2008, pp. 92–97.

[8] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *Signal Processing, IEEE Transactions on*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[9] A. Pierrot and M. Bloch, "Strongly secure communications over the two-way wiretap channel," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 595–605, Sept 2011.

[10] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[11] U. Maurer, "Secret key agreement by public discussion from common information," *Information Theory, IEEE Transactions on*, vol. 39, no. 3, pp. 733–742, May 1993.

[12] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The misome wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[13] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 8, pp. 4961–4972, Aug 2011.

[14] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, May 1978.

[15] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *Information Theory, IEEE Transactions on*, vol. 39, no. 4, pp. 1121–1132, Jul 1993.

[16] S. Ur Rehman, K. Sowerby, C. Coghill, and W. Holmes, "The analysis of rf fingerprinting for low-end wireless receivers with application to ieee 802.11a," in *Mobile and Wireless Networking (iCOST), 2012 International Conference on Selected Topics in*, July 2012, pp. 24–29.

[17] S. Rehman, K. Sowerby, and C. Coghill, "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios," *Communications, IET*, vol. 8, no. 8, pp. 1274–1284, May 2014.

[18] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 30, no. 8, pp. 1578–1588, September 2012.

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

[20] 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*, April 2011, pp. 1422–1430.

[21] 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*, March 2008, pp. 3013–3016.

[22] D. Stinson, *Cryptography: Theory and Practice,Second Edition*, 2nd ed. CRC/C&H, 2002.

[23] C.-X. Wang, X. Hong, X. Ge, X. Cheng, G. Zhang, and J. Thompson, "Cooperative mimo channel models: A survey," *Communications Magazine, IEEE*, vol. 48, no. 2, pp. 80–87, February 2010.

[24] M. Di Renzo and M. Debbah, "Wireless physical-layer security: The challenges ahead," in *Advanced Technologies for Communications, 2009. ATC '09. International Conference on*, Oct 2009, pp. 313–316.

[25] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *Wireless Communications, IEEE*, vol. 18, no. 4, pp. 6–12, August 2011.

[26] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *INFOCOM, 2013 Proceedings IEEE*, April 2013, pp. 3048–3056.

[27] J. Wallace and R. Sharma, "Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 3, pp. 381–392, Sept 2010.

[28] C.-X. Wang, X. Hong, X. Ge, X. Cheng, G. Zhang, and J. Thompson, "Cooperative mimo channel models: A survey," *Communications Magazine, IEEE*, vol. 48, no. 2, pp. 80–87, February 2010.

[29] H. Zhou, L. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 3, pp. 476–488, March 2014.

[30] C.-X. Wang, X. Hong, X. Ge, X. Cheng, G. Zhang, and J. Thompson, "Cooperative mimo channel models: A survey," *Communications Magazine, IEEE*, vol. 48, no. 2, pp. 80–87, February 2010.

[31] B. Wang, J. Zhang, and A. Host-Madsen, "On the capacity of mimo relay channels," *Information Theory, IEEE Transactions on*, vol. 51, no. 1, pp. 29–43, Jan 2005.

[32] Y. Fan and J. Thompson, "Mimo configurations for relay channels: Theory and practice," *Wireless Communications, IEEE Transactions on*, vol. 6, no. 5, pp. 1774–1786, May 2007.

[33] S. Pan, B. Ji, and Y. Luan, "Reliability research of wireless sensor network node," in *Computer Supported Cooperative Work in Design (CSCWD), 2010 14th International Conference on*, April 2010, pp. 444–447.

[34] M. Kubo, M. Sun, K. Yanagihara, and S. Hara, "A multiple cooperative nodes selection method for reliable wireless multi-hop data transmission," in *Wireless*

Communication Systems (ISWCS), 2012 International Symposium on, Aug 2012, pp. 486–490.

[35] M. Kubo, D. Anzai, and S. Hara, "Selection criteria of cooperative nodes for reliable wireless multi-hop data transmission," in *Wireless Communication Systems (ISWCS), 2010 7th International Symposium on*, Sept 2010, pp. 345–349.

[36] B. Mainaud, V. Gauthier, and H. Afifi, "Cooperative communication for wireless sensors network : A mac protocol solution," in *Wireless Days, 2008. WD '08. 1st IFIP*, Nov 2008, pp. 1–5.

[37] K. El-Darymli, "Amplify-and-forward cooperative relaying for a linear wireless sensor network," in *Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on*, Oct 2010, pp. 106–112.

[38] H.-S. Yang and S.-J. Yoo, "Authentication techniques for improving the reliability of the nodes in the manet," in *IT Convergence and Security (ICITCS), 2014 International Conference on*, Oct 2014, pp. 1–3.

[39] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *Vehicular Technology, IEEE Transactions on*, vol. 62, no. 7, pp. 3339–3348, Sept 2013.

[40] K. Chen and B. Natarajan, "Evaluating node reliability in cooperative mimo networks (under review)," *Information Forensics and Security, IEEE Transactions on*, 2015.

[41] K. Chen, B. Natarajan, and S. Shatti, "Relay-based secret key generation in LTE-A," in *Communications and Network Security: Physical Layer security workshop. IEEE Conference on*, Oct 2014.

[42] K. Chen and B. Natarajan, "Mimo-based secret key generation strategies: Rate analysis," *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, vol. 6, no. 3, pp. 22–55, Jan 2015.

[43] K. Chen, B. Natarajan, and S. Shattil, "Secret key generation rate with power allocation in relay-based lte-a networks," *Information Forensics and Security, IEEE Transactions on*, vol. 10, no. 11, pp. 2424–2434, Nov 2015.

[44] K. Chen and B. Natarajan, "Network tomography based node reliability evaluation in cooperative mimo networks (under review)," *Special Issue on Physical Layer Security for Emerging Wireless Networks: From Theory to Practice*, 2015.

[45] R. Ahlswede and I. Csiszar, "The role of common randomness in information theory and cryptography, part 1: Secrecy constraints," in *Information Theory, 1991 (papers in summary form only received), Proceedings. 1991 IEEE International Symposium on (Cat. No.91CH3003-1)*, Jun 1991, pp. 265–265.

[46] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion." Springer-Verlag, 1994, pp. 410–423.

[47] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. 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*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 128–139. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409960

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

[49] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," in *Ultra-Wideband, 2007. ICUWB 2007. IEEE International Conference on*, Sept 2007, pp. 270–275.

[50] L. Lai, Y. Liang, and W. Du, "Phy-based cooperative key generation in wireless networks," in *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on*, Sept 2011, pp. 662–669.

[51] J. B. Matthieu Bloch, *Physical-Layer Security: From Information Theory to Security Engineering*. New York, NY, USA: Cambridge University Press, 2011.

[52] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *Mobile Computing, IEEE Transactions on*, vol. 12, no. 5, pp. 917–930, May 2013.

[53] B. Azimi-sadjadi, A. Mercado, B. Yener, and et al., "Robust key generation from signal envelopes in wireless networks," 2007.

[54] A. Ghosh and R. Ratasuk, "Multi-antenna systems for lte enodeb," in *Vehicular Technology Conference Fall (VTC 2009-Fall), 2009 IEEE 70th*, Sept 2009, pp. 1–4.

[55] D. Gesbert, M. Shafi, D. shan Shiu, P. Smith, and A. Naguib, "From theory to practice: an overview of mimo space-time coded wireless systems," *Selected Areas in Communications, IEEE Journal on*, vol. 21, no. 3, pp. 281–302, Apr 2003.

[56] A. Paulraj, D. GORE, R. Nabar, and H. Bolcskei, "An overview of mimo communications - a key to gigabit wireless," *Proceedings of the IEEE*, vol. 92, no. 2, pp. 198–218, Feb 2004.

[57] A. Goldsmith, S. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of mimo channels," *Selected Areas in Communications, IEEE Journal on*, vol. 21, no. 5, pp. 684–702, June 2003.

[58] Shannon, "Communication theory of secrecy system," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.

[59] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley-Interscience, 1991.

[60] A. Pierrot and M. Bloch, "Strongly secure communications over the two-way wiretap channel," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 595–605, Sept 2011.

[61] J. Wallace and R. Sharma, "Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 3, pp. 381–392, Sept 2010.

[62] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 17–30, Jan 2010.

[63] C. Chen and M. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 2, pp. 205–215, Feb 2011.

[64] K. Chen and B. Natarajan, "Mimo-based secret key generation strategies: Rate analysis," in *Innovative Algorithms and Techniques for Securing Wireless Networks*, ser. Advances in Information Security, Privacy, and Ethics (AISPE) Book Series. Hershey, PA: IGI Global, 2015.

[65] I. Hammerstrom and A. Wittneben, "Power allocation schemes for amplify-and-forward mimo-ofdm relay links," *Wireless Communications, IEEE Transactions on*, vol. 6, no. 8, pp. 2798–2802, August 2007.

[66] Z. Fang, Y. Hua, and J. Koshy, "Joint source and relay optimization for a non-regenerative mimo relay," in *Sensor Array and Multichannel Processing, 2006. Fourth IEEE Workshop on*, July 2006, pp. 239–243.

[67] Y. Rong and Y. Hua, "Optimality of diagonalization of multi-hop mimo relays," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 12, pp. 6068–6077, December 2009.

[68] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K: Cambridge Univ. Press, 2004.

[69] D. Palomar, J. Cioffi, and M.-A. Lagunas, "Uniform power allocation in mimo channels: a game-theoretic approach," *Information Theory, IEEE Transactions on*, vol. 49, no. 7, pp. 1707–1727, July 2003.

[70] K. Chen, B. Natarajan, and S. Shattil, "Relay-based secret key generation in lte-a," in *Communications and Network Security (CNS), 2014 IEEE Conference on*, Oct 2014, pp. 139–144.

[71] ——, "Secret key generation rate with power allocation in relay-based lte-a networks," *Information Forensics and Security, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[72] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *Communications Surveys Tutorials, IEEE*, vol. 11, no. 1, pp. 116–130, First 2009.

[73] M. Sankaran, "Approximations to the non-central chi-square distribution," *Biometrika*, vol. 50, no. 1/2, pp. pp. 199–204, 1963. [Online]. Available: http://www.jstor.org/stable/2333761

[74] ——, "On the non-central chi-square distribution," *Biometrika*, vol. 46, no. 1/2, pp. pp. 235–237, 1959. [Online]. Available: http://www.jstor.org/stable/2332828

[75] I. Hoballah and P. Varshney, "Distributed bayesian signal detection," *Information Theory, IEEE Transactions on*, vol. 35, no. 5, pp. 995–1000, Sep 1989.

[76] H. V. Poor, *An Introduction to Signal Detection and Estimation (2Nd Ed.)*. New York, NY, USA: Springer-Verlag New York, Inc., 1994.

[77] N. Gnanapandithan, "Data detection and fusion in decentralized sensor networks," Ph.D. dissertation, Kansas State University, 2005.

[78] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *Communications Surveys Tutorials, IEEE*, vol. 15, no. 3, pp. 996–1019, Third 2013.

[79] R. Castro, M. Coates, G. Liang, R. Nowak, and B. Yu, "Network tomography: recent developments," *Statistical Science*, vol. 19, pp. 499–517, 2004.

[80] M. Coates and R. Nowak, "Network tomography for internal delay estimation," in *Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference on*, vol. 6, 2001, pp. 3409–3412 vol.6.

[81] A. Tsang, M. Coates, and R. D. Nowak, "Network delay tomography," *IEEE Transactions on Signal Processing*, vol. 51, pp. 2125–2136, 2003.

[82] Y. Vardi, "Network tomography: Estimating source-destination traffic intensities from link data," *Journal of the American Statistical Association*, vol. 91, no. 433, pp. pp. 365–377, 1996. [Online]. Available: http://www.jstor.org/stable/2291416

[83] Y. Tsang, M. Coates, and R. Nowak, "Passive network tomography using em algorithms," in *Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference on*, vol. 3, 2001, pp. 1469–1472 vol.3.

[84] V. N. Padmanabhan, L. Qiu, and H. J. Wang, "Passive network tomography using bayesian inference," in *Proceedings of the 2Nd ACM SIGCOMM Workshop on Internet Measurment*, ser. IMW '02. New York, NY, USA: ACM, 2002, pp. 93–94. [Online]. Available: http://doi.acm.org/10.1145/637201.637214

[85] G. Sharma, S. Jaggi, and B. Dey, "Network tomography via network coding," in *Information Theory and Applications Workshop, 2008*, Jan 2008, pp. 151–157.

[86] G. Liang and B. Yu, "Maximum pseudo likelihood estimation in network tomography," *Signal Processing, IEEE Transactions on*, vol. 51, no. 8, pp. 2043–2053, Aug 2003.

[87] A. Chen, J. Cao, and T. Bu, "Network tomography: Identifiability and fourier domain estimation," *Signal Processing, IEEE Transactions on*, vol. 58, no. 12, pp. 6029–6039, Dec 2010.

[88] A. Chen and J. Cao, "Network tomography based on 1-d projections," pp. 45–61.

[89] D. W. Scott, *Multivariate Density Estimation: Theory, Practice, and Visualization.* New York, NY, USA: Wiley-Interscience, 1992.

[90] J. P. Keener, *Principles of Applied Mathematics: Transformation and Approximation.* Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1988.

Appendix A

Proof of the non-concavity of Eq. 4.6

For simplicity in developing the argument, we assume only one antenna and one relay node is involved in the proposed SKGR scheme (it is straightforward but notationally tedious to expand the arguments to multiple antenna and multiple relay nodes case). Since all the other parameters are known (except P and Q), we can rewrite the objective function (Eq. 4.6) as follows.

$$f(x,y) = -\log(1 - \frac{axcy}{(ax+b)(cy+d)}) \tag{A.1}$$

In order to proof the concavity of Eq. A.1, we need to examine its Hessian [90], which is defined as:

$$H = \begin{pmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{pmatrix}, \tag{A.2}$$

where

$$f_{xx} = \frac{\partial^2 f}{\partial x^2} = -\frac{a^2bcy(2adx+bcy+2bd)}{(ax+b)^2(adx+bcy+bd)^2} \tag{A.3}$$

$$f_{xy} = \frac{\partial^2 f}{\partial x \partial y} = -\frac{abcd}{(adx + b(cy + d))^2} \tag{A.4}$$

$$f_{yx} = \frac{\partial^2 f}{\partial y \partial x} = -\frac{abcd}{(adx + b(cy + d))^2} \tag{A.5}$$

$$f_{yy} = \frac{\partial^2 f}{\partial y^2} = -\frac{ac^2dx(adx + 2bcy + 2bd)}{(cy + d)^2(adx + bcy + bd)^2} \tag{A.6}$$

According to [90], Eq. A.1 is concave if and only if H is negative semi-definite. The sub-determinates of matrix H correspond to,

$$det(H_1) = f_{xx} < 0, \tag{A.7}$$

$$det(H_2) = f_{xx}f_{yy} - f_{xy}f_{yx}. \tag{A.8}$$

It is easy to observe that Eq. A.7 is less than zero. However, for Eq. A.8, the sign depends on the term

$$\begin{aligned}&(a^3bc^3dxy(adx + 2b(cy + d))(2adx + b(cy + 2d)))\\ &- (ax + b)^2(cy + d)^2(a^2b^2c^2d^2),\end{aligned} \tag{A.9}$$

which can be negative for some admissible values of x and y. Therefore, Eq. A.1 is not a concave function of x and y.

Appendix B

Proof of the Lemma 4

Since y is fixed and other parameters are known, the objective function can be written as:

$$R_{S_{MIMO}} = -\frac{1}{2}\sum_{i=1}^{M}\sum_{j=1}^{N}\log(1 - \frac{a_{i,j}x}{a_{i,j}x + b_i} * C_j) \tag{B.1}$$

In order to maximize equation (9), we must maximize all the *log* terms in the summation. Therefore, It is important to check the concavity of the following expression.

$$f(x) = -\log(1 - \frac{a_{i,j}x}{a_{i,j}x + b_i} * C_j) \tag{B.2}$$

where, $a_{i,j}$, b_i, and C_j are known positive numbers. The first derivative of $f(x)$ is:

$$f^{'}(x) = \frac{a_{i,j}b_iC_j}{(a_{i,j}x + b_i)(b_i - a_{i,j}(C_j - 1)x)} \tag{B.3}$$

It is easy to observe that equation (54) is differentiable. Therefore, the second derivative of equation (53) can be calculated as:

$$f^{''}(x) = \frac{a_{i,j}^2b_iC_j2a_{i,j}^2(C_j - 1)x + b_i(C_j - 2)}{(a_{i,j}x + b_i)^2(b_i - a_{i,j}^2x)^2} \tag{B.4}$$

where, $C_j = \frac{a'_{i,j}y}{a'_{i,j}y+b'_j}$. Since $a'_{i,j}$, y, and b'_j are known positive numbers, C_j should be less than 1. Therefore, $C_j - 1 < 0$, $C_j - 2 < 0$, and $f''(x) < 0$.

Therefore, equation (10) is a concave function of x. Using a similar approach, we can demonstrate that equation (10) is also a concave function of y.