博士論文
PhD Thesis

Study on Secrecy-Enhanced Data Transmission for Cooperative Relay Networks

（協力中継ネットワークのための高秘匿データ伝送に関する研究）

東京大学
THE UNIVERSITY OF TOKYO

The University of Tokyo
Graduate School of Information Science and Technology
Department of Information and Communication Engineering

48-127405　牛　瀬
Hao NIU

Supervisor　Prof. Kaoru SEZAKI

December 2015

Abstract

Recent years have witnessed an explosive increase in the research works on cooperative relay networks (CRNs) to improve the reliability and efficiency of wireless data transmission at the physical layer. Unlike these works, this thesis focuses on secrecy-enhanced data transmission for CRNs at the physical layer from the perspective of physical layer security (PLS). There are generally two kinds of eavesdropping attacks for CRNs: external eavesdropping attack from pure eavesdroppers and internal eavesdropping attack from untrusted relays. The thesis is thus divided into two parts by considering these two kinds of attacks.

In the first part of the thesis, the cooperative relaying for protecting from the external eavesdropping attack, also named cooperative security, is studied. 1) We first investigate the cooperative security for the typical two-user cooperation scenario within the framework of game theory. Due to the fact that the conventional cooperation may deteriorate the secrecy performance compared to the direct transmission (DT), an opportunistic user cooperation scheme (OUCS) is designed. The OUCS activates the cooperation only when it is regarded to be worthwhile according to the time-varying channel fading. It is proved that the OUCS consistently achieves a better secrecy performance than the DT, which motivates the users to cooperate with each other. 2) Then, we extend the OUCS to multi-user cooperation scenarios by jointly solving the questions of whether to cooperate and with whom to cooperate under the eavesdropping attack. It is derived that the full secrecy diversity performance is realized by the OUCS, which outperforms existing alternatives in the literature. 3) Moreover, we consider the application of cooperative security in a kind of specific sensor networks - wireless body area networks (WBANs). Based on the channel characteristics of WBANs, the secrecy outage probabilities for the DT and cooperative relaying are derived respectively. It is confirmed that the cooperative security is also feasible in WBANs.

In the second part of the thesis, the code assisted security for protecting from the internal eavesdropping attack is investigated. Because the cooperative relays themselves are the eavesdroppers in this case, the cooperative security analyzed above is no longer effective. Therefore, the code assisted security is introduced. 1) We first design a scheme of fountain code assisted security (FCAS). Because the receivers need a sufficient number of fountain packets to recover the original data for fountain coded transmission, the security can be achieved if the destination receives fountain packets faster than the eavesdropper. The channel fading and transmit power control are exploited by us to make a higher packet reception rate at the destination compared to the eavesdropper. It is observed that FCAS reduces the intercept probability to zero (near-)exponentially with increased number of source packets. Therefore, an arbitrarily small intercept probability can be realized by simply increasing the number of source packets. The conclusion is also held when we apply FCAS in the CRNs to resist an untrusted relay. 2) We further develop a fixed linear code assisted security (FLCAS) scheme based on FCAS, and use it to resist multiple untrusted relays. Because the randomness characteristics of fountain codes still results in a small quantity of data leakage, we are motivated to adopt a fixed linear code with a better secrecy performance. The intercept probability for FLCAS in the CRNs with multiple untrusted relays is then analyzed. It is found that FLCAS maintains the superiority of FCAS that the intercept probability is decreased to zero exponentially as the number of source packets increases. The destination based jamming strategy is also considered to accelerate the rate of decrease. In addition, the comparisons of FLCAS with FCAS and experiment evaluations are presented.

Overall, this thesis comprehensively studies how to enhance the secrecy of data transmission for the CRNs based on the concept of PLS. Both of the external and internal eavesdropping attacks are considered. The contributions herein can be also applied in the conventional multi-hop networks to improve the data transmission security.

Acknowledgements

First of all I would like to express my sincere gratitude to my supervisor Prof. Kaoru Sezaki for his excellent guidance and great support on my study life in Japan. He always gives me valuable suggestions and motivates me to do the cutting-edge research. From him I also learned how to effectively conduct and present the research work. I am truly grateful that I can carry out my Ph.D. study in Sezaki lab.

Furthermore, I am deeply indebted to Prof. H. Vincent Poor who guided my study in Princeton University. The collaborative research there broaden my research vision and improve my research ability very much.

I would also like to thank my advisors Prof. Tohru Asami and Prof. Hiroyuki Morikawa, who dedicated their time to discuss my research and gave me precious advices.

I further want to thank all the defense committee members Prof. Tohru Asami, Prof. Hiroyuki Morikawa, Prof. Yoichi Sato, Prof. Kanta Matsuura and Prof. Yoshihiro Kawahara. Their constructive comments and suggestions help me improve my research and the thesis greatly.

Appreciation continues to Prof. Masaki Ito and Prof. Masayuki Iwai for their great help in my research. I would also appreciate the assistance from Dr. Hongyang Chen, and co-researchers Prof. Li Sun, Prof. Athanasios V. Vasilakos, and Dr. Nanhao Zhu. Especially, almost all of my research works got many advices from Prof. Li Sun. I would also want to thank the research fellows in Princeton University, Dr. Rafael Schaefer and Dr. Gayan Amarasuriya, who gave me many worthwhile comments on my research.

I would like to thank all the lab mates at Sezaki lab, especially, Guangwen

Liu, Matekenya Dunstan, Yao Sun and Tiantian Jiang. Thanks a lot to Ms. Kaho Matsumoto and Ms. June Naito, who helped me deal with a lot of paperworks.

Finally I wish to express special thanks to my families. Their encouragement is one of the main factors that help me finish this thesis.

December 2015

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Information communication is a fundamental need for the development of our human society. From the use of drums and smoke signals at the prehistoric era to the cable & wireless communications nowadays, new technologies are continually invented to pursue a faster transmission speed, a higher transmission reliability and a longer transmission distance. Especially in recent years, the mature of wireless digital communications makes the information transfer more flexibly and conveniently. Wireless devices nowadays have been employed widely to serve our daily lives, industries and other areas.

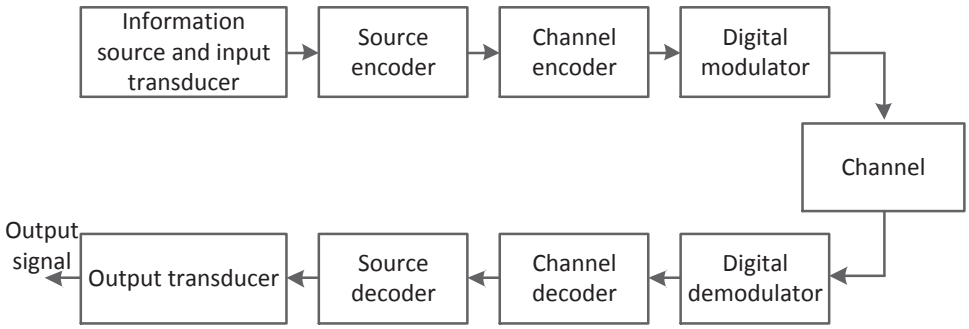

Figure 1.1: Basic architecture of modern digital communication systems [1].

Fig 1.1 shows the basic architecture of modern digital communication systems. At the transmitter, the source information is processed first by the source

encoder and channel encoder, and then sent to the receiver through the communication channel after digital modulator. The receiver obtains the information via a reverse process. For a communication system, the transmission performance is affected greatly by the quality of the channel. In the milestone work of Shannon [2], channel capacity was pioneered that provides the maximum transmission rate at which reliable communication over a channel is possible[1] [1]. The shannon capacity of a point-to-point communication system with additive white Gaussian noise (AWGN) channel is given by $C = W\log_2\left(1+\frac{\tilde{P}}{N_0 W}\right)$ (bit-s/s), where W is the bandwidth of the channel, $\tilde{P}$ is the received signal power and N_0 is the noise power spectral density[2].

Compared to the cable networks, the wireless communications suffer a lot from the channel fading. The popular wireless systems, e.g., cellular networks, WiFi networks and satellite systems, are all using the radio wave to perform the data transmission. During the transmission, the radio signal experiences path loss, shadowing effect and multipath propagation. When it arrives at the receiver, the power has been attenuated greatly and also becomes randomly fluctuating. This kind of attenuation and random fluctuation is know as the channel fading in the wireless systems. Assuming that the transmit power is P and the channel fading coefficient is h, $\tilde{P}$ is derived as $P|h|^2$, which indicates that the instantaneous channel capacity is proportional to the channel gain. That is to say, a larger channel gain $|h|^2$ supports a higher transmission rate of the reliable communication, and similarly the temporary deep fade may result in transmission failures.

Since the random fluctuations of the channel fading in wireless systems yields an unstable transmission performance, how to deal with channel fading is one central topic for the design of wireless communication systems [3,4]. The diversity strategy is regarded as a powerful tool to mitigate the effects of fading

[1]Shannon second theorem - the noisy channel coding theorem: Reliable communication over a discrete memoryless channel is possible if the communication rate R satisfies $R < C$, where C is the channel capacity. At rates higher than capacity, reliable communication is impossible [1].

[2]The shannon capacity with $W = 1$ (also named spectral efficiency), i.e., $C = \log_2\left(1+\frac{\tilde{P}}{N_0}\right)$ (bits/s/Hz), is usually utilized for performance analysis. It is also adopted in this thesis without loss of generality.

by combining the signals from independent transmission links (which experience independent channel fading). As described in [4], diversity-combining uses the fact that independent signal links have a low probability of experiencing deep fades simultaneously. The diversity can be realized in many ways, e.g., the bit interleaving at time domain, subcarrier interleaving in orthogonal frequency division multiplexing (OFDM) systems at frequency domain, and multi-antenna transmitting/receiving in spatial domain.

Multi-antenna transmitting/receiving, also known Multiple Input Multiple Output (MIMO), is an intuitive way to harvest the spatial diversity gain. If the antennas are separately enough, the maximum diversity order $M * N$ (i.e., $M * N$ independent transmission links) can be reached, where M and N are the numbers of transmit and receive antennas respectively. Both the academia [4–7] and industry [8–13] generally accept that the required separation distance between antennas to yield independent channel fading is the same order of the carrier wavelength (from half to several wavelengths). Since the requirement of the same order of the carrier wavelength is not difficult to be satisfied for many wireless devices, the multi-antenna diversity has been extensively adopted. One typical application is the base stations and smartphones[3] in cellular networks.

However, the number of configurable antennas on a specific device is still restricted. Especially, some kinds of wireless devices (e.g., sensor nodes) are required to be as small as possible. The setup of two diversity antennas is already infeasible for these size and resource limited devices. Recently, a novel form of spatial diversity technique named cooperative diversity attracts much research attention from the pioneering works of [15, 16]. The nodes in the cooperative networks act as relays and form a virtual multi-antenna system to assist the transmission between the source and the destination, which realizes the spatial diversity in a distributed manner. Due to the existence of the relaying phase, the cooperative diversity is also called cooperative relaying. It has been proved that cooperative relaying is effective to improve the transmission quality and enlarge the coverage area of the wireless networks. Till now, the researchers

[3]The popular smartphones, e.g., Apple Iphone, Samsung Galaxy and Nokia Lumia all adopt the spatial diversity antenna [14].

have studied the application of cooperative relaying in different kinds of wireless networks, such as 5G networks, wireless sensor networks, smart grids and even underwater acoustic systems [17–20].

1.2 Basic Theory of Cooperative Relaying

The direct transmission and cooperative relaying are shown respectively in Fig 1.2. For the convenience of analysis, the channel from node i to node j is modeled as Rayleigh block flat fading channel with the average channel gain $E(|h_{ij}|^2) = \sigma_{ij}^2$, where $h_{ij} \sim CN\left(0, \sigma_{ij}^2\right)$ is the channel fading coefficient. Given that all the devices operate in the half-duplex mode and time division multiple access is adopted to make orthogonal channel access, the cooperative relaying is generally divided into two phases. In phase I, the source sends the signals of its message, and both the destination and the cooperative relay listen to it. In phase II, the cooperative relay retransmits its received signals to the destination based on a selected cooperative relaying protocol. Then the destination combines the signals of both phases to obtain the spatial diversity gain.

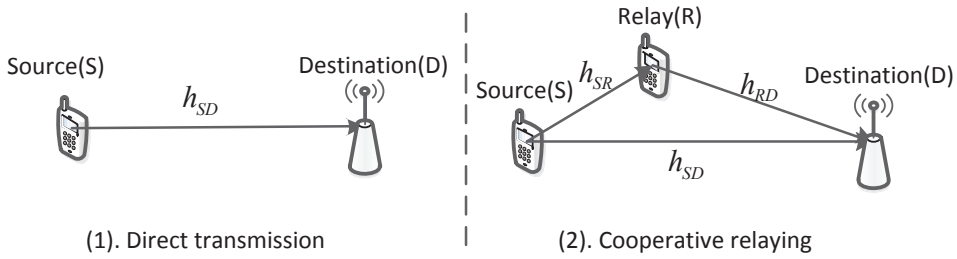

Figure 1.2: Direct transmission and cooperative relaying.

For the direct transmission, the received signals at the destination can be written as

$$y_D = \sqrt{P} h_{SD} x + n_{SD} \tag{1.1}$$

where, x is the transmitted signals and $n_{ij} \sim CN\left(0, N_0\right)$ represents the additive white Gaussian noise (AWGN) at the node j. The maximum achievable

transmission rate/channael capacity is derived as

$$C^d = \log_2\left(1+\rho|h_{SD}|^2\right) \tag{1.2}$$

where $\rho = P/N_0$ denotes the system signal to noise ratio (SNR). The transmission suffers from outage if the channel capacity is less than the target transmission rate R. An important performance metric to evaluate the quality of the wireless transmission is the outage probability $P_{out} = \Pr\{C < R\}$, from which the diversity order can be also derived by $d_o = -\lim_{\rho\to\infty} \frac{\log P_{out}}{\log \rho}$. d_o reflects the number of independent transmission links. As for the direct transmission, the outage probability is obtained as

$$P_{out}^d = \Pr\left\{C^d < R\right\} = 1 - e^{-\frac{1}{\sigma_{SD}^2}\frac{2^R-1}{\rho}} \overset{\rho\to\infty}{\approx} \frac{1}{\sigma_{SD}^2}\frac{2^R-1}{\rho} \tag{1.3}$$

It is easy to get that the diversity order of the direct transmission is 1, which is consistent with the intuitive observation.

For the cooperative relaying transmission, the decode-and-forward (DF) and amplify-and-forward (AF) are two fundamental cooperative relaying protocols [16]. The theory of them is described as follows.

A. DF protocol

The DF relay first decodes the signals received in Phase I, and then forwards the message after re-encoding. To realize the diversity order of 2, the selective DF relaying protocol is analyzed in this thesis. That is to say, the relay forwards the message only if the channel gain of the source-relay link is higher than a threshold. Considering that maximal ratio combining (MRC) is adopted at the destination, the channel capacity of DF protocol is

$$C^{DF} = \begin{cases} \frac{1}{2}\log_2\left(1+\rho|h_{SD}|^2\right), & |h_{SR}|^2 < \left(2^{2R}-1\right)/\rho \\ \frac{1}{2}\log_2\left(1+\rho|h_{SD}|^2+\rho|h_{RD}|^2\right), & |h_{SR}|^2 \geq \left(2^{2R}-1\right)/\rho \end{cases} \tag{1.4}$$

where $\frac{1}{2}$ is due to the rate degradation of cooperative relaying. The outage

probability is thus derived as [16]

$$P_{out}^{DF} = \Pr\left\{C^{DF} < R\right\} \overset{\rho\to\infty}{\approx} \frac{1}{2\sigma_{SD}^2}\frac{\sigma_{SR}^2 + 2\sigma_{RD}^2}{\sigma_{SR}^2\sigma_{RD}^2}\left(\frac{2^{2R}-1}{\rho}\right)^2 \tag{1.5}$$

The diversity order 2 can be confirmed for the DF cooperative relaying protocol. Intuitively speaking, there are two independent links: direct link and relaying link. The data transmission can be success if either of the two links does not undergo the deep fade.

B. AF protocol

Unlink the DF relay, the AF relay only amplifies its received signals by a factor and forwards the amplified signals directly. The factor is used to scale the transmit power to be P and is given as

$$\varphi = \frac{\sqrt{P}}{\sqrt{P|h_{sr}|^2 + N_0}} \tag{1.6}$$

Therefore, the received signal at the destination from the relay is

$$y_{RD} = \varphi h_{RD} y_{SR} + n_{RD} = \varphi h_{RD}\left(h_{SR}x + n_{SR}\right) + n_{RD} \tag{1.7}$$

The corresponding received SNR is calculated as $\gamma_{RD} = \frac{\rho|h_{SR}|^2\rho|h_{RD}|^2}{1+\rho|h_{SR}|^2+\rho|h_{RD}|^2}$. Thus, the channel capacity of AF protocol is

$$\begin{aligned} C^{AF} &= \frac{1}{2}\log_2\left(1+\rho|h_{SD}|^2+\gamma_{RD}\right) \\ &= \frac{1}{2}\log_2\left(1+\rho|h_{SD}|^2+\frac{\rho|h_{SR}|^2\rho|h_{RD}|^2}{1+\rho|h_{SR}|^2+\rho|h_{RD}|^2}\right) \end{aligned} \tag{1.8}$$

In the high ρ region, the outage probability is approximated to be [16]

$$P_{out}^{AF} = \Pr\left\{C^{AF} < R\right\} \overset{\rho\to\infty}{\approx} \frac{1}{2\sigma_{SD}^2}\frac{\sigma_{SR}^2 + \sigma_{RD}^2}{\sigma_{SR}^2\sigma_{RD}^2}\left(\frac{2^{2R}-1}{\rho}\right)^2 \tag{1.9}$$

It is observed that the AF cooperative relaying protocol also has diversity order 2. Although DF and AF protocols are extensively adopted, both of

them have their own merits and drawbacks. For example, DF relay does not need to storage the analog waveforms but has a higher complexity for the decoding and re-encoding, while AF relay has a lower complexity but needs the process of analog waveforms and amplifies the noise simultaneously. Therefore, other cooperative relaying protocols, e.g., compress-and-forward [21, 22] and demodulate-and-forward [23, 24], are also studied by the researchers. With its development in both theory and practice, the idea of cooperative relaying has been considered by different wireless standards such as Wimax [25] and 3GPP LTE-Advanced [26].

1.3 Physical Layer Security

In wireless networks, the openness of the transmission medium makes it vulnerable to the eavesdropping attacks. Generally, the receivers in the coverage area of a transmitter are all able to receive the transmitted signals. Therefore, besides the reliability and efficiency, the transmission security is also a crucial issue in the research of wireless networks. The cryptography is traditionally adopted at the upper layers of the network protocol stack to secure the data transmission. However, most of the encryption schemes rely heavily on the computational hardness assumptions and the premise of limited computing power at the eavesdropper, which is being threatened more by the emerging technologies, e.g., cloud computing and quantum computer. Besides that, key management is relatively complex for decentralized or dynamic wireless networks.

Compared to the cryptography which achieves the security mainly through transmitting the cipher text, the physical layer security (PLS) exploits the physical characteristics of the wireless channels (e.g., fading or noise) to *make that* the eavesdropper is unable to decode/receive the transmitted data (which may be the plain text) [27–30]. Therefore, it can realize the secure transmission without encryptions. The PLS is based on information theory to pursue perfect secrecy, and is being popularly studied in the research area of wireless security [31, 32]. The pioneer proposal of PLS is found in the work of Wyner [27]. It is concluded that it is possible to transmit the information in perfect secrecy

at a non-zero rate if the quality of the eavesdropping link is worse than that of the legitimate link. The PLS in wireless networks with fading channels is studied in [29], where the secrecy capacity (i.e., the maximum data rate at which the eavesdropper cannot decode any information) is given as the difference of the channel capacities between the legitimate link and the eavesdropping link. Fig 1.3 shows a typical wireless network under eavesdropping attack. Given the assumption of block-flat fading channels in the network, the instantaneous secrecy capacity is expressed as

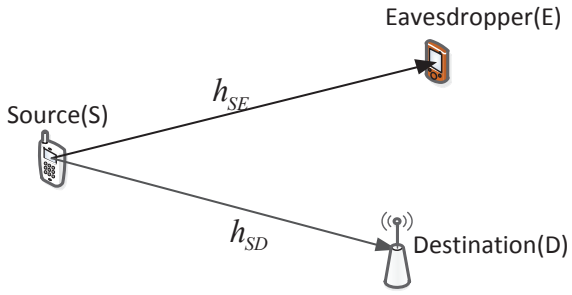

Figure 1.3: A wireless network under eavesdropping attack.

$$C_s = [C_D - C_E]^+ = \left[\log_2\left(1+\rho|h_{SD}|^2\right) - \log_2\left(1+\rho|h_{SE}|^2\right)\right]^+ \tag{1.10}$$

where, $[x]^+ = \max\{0, x\}$, C_D and C_E are the channel capacities at the destination and the eavesdropper respectively. The secrecy outage probability is also characterized in [29] as the probability that the instantaneous secrecy capacity is less than a target secrecy rate $R_s > 0$, i.e., $P_{out} = \Pr\{C_s < R_s\}$.

How to improve the secrecy capacity and/or reduce the secrecy outage probability is one of the main research directions of PLS. From their definitions, it is direct to consider the transmission strategies which can increase the channel capacity at the destination or decrease the channel capacity at the eavesdropper. Typical approaches include multi-antenna beamforming [33] and artificial noise [34]. The cooperative relaying has also been considered to enhance the PLS recently, which we denote as cooperative security. For example, cooperative relaying based beamforming and jamming for the PLS are studied in [35–40].

1.4 Motivation and Contributions

The cooperative relaying based beamforming and jamming generally have a higher complexity, which motivates us to design the cooperative security schemes based on the basic cooperative relaying transmission. The underlying idea is finding the diversity link which can provide the best secrecy performance to perform the data transmission. The finished works with their respective motivation and contributions are listed as follows.

1) For the two-user cooperation, we design an opportunistic user cooperation scheme (OUCS) to consistently achieve a better secrecy performance than the direct transmission, which cannot be ensured by the conventional cooperation scheme. With the conventional cooperation, it is easy to observe that *both* the destination and the eavesdropper can obtain the diversity gain, which may deteriorate the secrecy performance if the eavesdropper gets more. Therefore, we are motivated to design an OUCS based on the works of [41–43], such that the cooperative relaying link is activated only when it is regarded to be positive for the enhancement of PLS. The analysis of the OUCS for the two-user cooperation is conducted within the framework of game theory. We derive that the secrecy performance of the OUCS is always better that that of the direct transmission, which prompts the users to cooperate with each other.

2) The OUCS is extended to multi-user cooperation scenarios combining with the concept of optimal relay selection, which is proved to achieve the secrecy outage performance with full diversity. Although the optimal relay selection has been studied for cooperative security in [44–49], these schemes only deal with the question of with whom to cooperate. They do not fully exploit the diversity transmission links and cannot realize full secrecy diversity accordingly. However, by jointly solving the questions of whether to cooperate and with whom to cooperate under the eavesdropping attack, our proposed OUCS is proved to have full secrecy diversity performance.

3) The application of cooperative security in a kind of specific sensor networks - wireless body area networks (WBANs) is investigated. The physical channels of WBANs have their own characteristics: the path loss is severer com-

pared to other wireless networks due to the effect of human body. Therefore, relaying is usually considered in WBANs to improve the transmission reliability and energy efficiency [50–58]. By analyzing the secrecy outage performance of direct transmission and cooperative relaying, we prove that the cooperative relaying is also a feasible way to realize secrecy-enhanced data transmission in WBANs.

The cooperative security schemes studied above are to protect from external eavesdropping. For cooperative relay networks (CRNs), there is another form of eavesdropping attack: internal eavesdropping caused by the untrusted relays. These relays are willing to dedicate their resources to assist the transmission, while they simultaneously attempt to intercept the relayed data. The cooperative security does not work well for this issue and thus we introduce code assisted security. The achievements are described as follows.

1) We propose a fountain-code assisted security (FCAS) scheme for wireless secure transmission, which is proved to be also effective for protecting from the threat of internal eavesdropping in CRNs. Some researchers have made their efforts on the issue of untrusted relays in CRNs based on the conventional PLS, such as [59–66]. However, the perfect secrecy ensured by PLS is not always necessary under the *assumption* that a certain number of packets are required to recovery the original data. The fountain codes is a such kind of coding scheme that satisfies this assumption. Therefore, the security can be realized for fountain coded transmission if the destination receives fountain packets faster than the eavesdropper. We thus exploit the channel fading and transmit power control to ensure a higher packet reception rate at the destination. It is observed that FCAS reduces the intercept probability to zero (near-)exponentially as the number of source packets increases, and thus an arbitrarily small intercept probability can be achieved by simply increasing the number of source packets[4]. The validity of FCAS for protecting from internal eavesdropping is then confirmed in CRNs with an untrusted relay.

2) A fixed linear code assisted security (FLCAS) scheme is designed to

[4]The intercept probability instead of secrecy outage probability is adopted here since the code assisted security is not strict PLS.

further improve the secrecy performance of FCAS, and the application of it to resist multiple untrusted relays is then analyzed. The randomness characteristics of fountain codes still results in a small quantity of information leakage at the eavesdropper before it receives enough fountain packets correctly. Therefore, we use a fixed linear code to overcome this shortcoming of the fountain codes, through which the information encrypts itself more perfectly but with the same complexity as fountain codes. We exploit FLCAS to protect from internal eavesdropping in the CRNs with multiple untrusted relays. It is derived that the intercept probability is also decreased to zero exponentially with the number of source packets. However, the rate of decrease becomes significantly slow as the number of untrusted relays increases. We therefore further introduce the destination based jamming strategy to accelerate the rate of decrease and achieve an acceptable intercept probability for multiple untrusted relays. In addition, the comparisons of FLCAS with FCAS and experiment evaluations are conducted by using software defined radio platforms (NI USRP-2921).

1.5 Outline of the Thesis

The rest of the thesis consists of six chapters.

From Chapter 2 to Chapter 4, the cooperative security for protecting from the external eavesdropping attack is studied: In Chapter 2, the two-user cooperation under eavesdropping attack is analyzed within the framework of game theory. The designed opportunistic user cooperation scheme - OUCS which always achieves a better secrecy performance than the direct transmission is described. Then we explain how to motivate the users to cooperate with each other by combining the OUCS with Stackelberg game. In Chapter 3, the OUCS is extended to multi-user cooperation scenarios. Based on the OUCS, we give an integrated solution on the questions of whether to cooperation and with whom to cooperate under the eavesdropping attack, and prove that the secrecy outage performance with full diversity can be achieved. In Chapter 4, the application of cooperation security in WBANs is considered. We derive the secrecy outage probabilities for the direct transmission and cooperative multihop

relaying respectively according to the channel characteristics of WBANs, which confirms the feasibility of the cooperation security in WBANs.

From Chapter 5 to Chapter 6, the code assisted security for protecting from the internal eavesdropping attack is analyzed: In Chapter 5, the fountain-code assisted security - FCAS is studied. We first describe the theory of FCAS for the wireless secure transmission. After that, the FCAS is applied in CRNs with an untrusted relay to validate its effectiveness. In Chapter 6, the fixed linear code assisted security scheme - FLCAS is introduced and exploited to resist multiple untrusted relays. We give an explanation on the FLCAS and describe its secrecy performance and complexity at first. Then we exploit it in the CRNs with multiple untrusted relays for protecting from the internal eavesdropping. Finally we compare the FLCAS with FCAS and conduct experiment evaluations.

The thesis is concluded and the future research directions are discussed in Chapter 7.

Chapter 2

Two-User Cooperation Analysis under Eavesdropping Attack

Cooperative relaying is generally regarded as a win-win strategy for the participated users. The users dedicate their own resources to assist other users' data transmission, and in return they also get others' cooperation. To motivate the users to participate in the cooperative relaying, the following two conditions should be satisfied: 1) the cooperation from others should be beneficial for the considered performance metric; 2) the mechanism avoiding free-riders should be included. The analysis of these requirements in theory is suitable to adopt game theory, which is a powerful mathematical method for helping players (users) make optimal actions in a competitive environment.

In this chapter, the two-user cooperation behaviors under eavesdropping attack are analyzed through game theory. Considering the physical layer security (PLS), we prove that the conventional cooperation scheme actually deteriorates the secrecy performance compared to the direct transmission, given that the eavesdropper has a better channel condition to the users than the destination. In this case, the necessary condition of the cooperation that the users should obtain additional utilities from the cooperation is not satisfied, which makes the users have no incentive to participate in the cooperation game. In order to motivate users, an opportunistic user cooperation scheme (OUCS) is designed to improve the secrecy performance even if the eavesdropping channel

is superior to the legitimate channel, and it is also observed that the mutual cooperation is one of the Nash equilibriums. We further exploit the Stackelberg game with a punishment mechanism to avoid free-riders and make the mutual cooperation as the unique Nash equilibrium.

2.1 Introduction

Besides the theoretical studies, the real experiments have also shown the significant performance improvement via cooperative relaying in terms of bit error rate, network throughout and delay, packet error rate, etc [67–69]. Till now, however, the introduction of cooperative relaying in real wireless systems is still rare. Besides the hardware and protocol limitations, the selfishness of users in many wireless networks is one main obstacle. The selfish users first assess whether the cooperation from others is beneficial or not. They are willing to attend the cooperative relaying if the cooperation benefits themselves. However, they still only care about their own utilities and intend to be free-riders in cooperative communication systems. As a result, all of the users prefer not to cooperate because they cannot get equivalent cooperation from the others [70].

This cooperation behavior is especially suitable to be analyzed by the game theory. Researchers have employed different game models to motivate the users of wireless networks to cooperate with others. In [71], the repeated game is analyzed for decode-and-forward (DF) user cooperation, where the utilities achieved in future cooperation periods can make the users choose mutual cooperation currently. Nash bargaining solution is adopted to provide user incentive to cooperate for the bits-per-energy efficiency in [72]. Resource allocation is solved through Stackelberg game by [73] and [74]. Some studies, such as [75], utilize the auction game to analyze cooperative communication. In these papers [71–75], the cooperation from other users is generally assumed to be *beneficial* for the utilities the users care about. For example, the utility function is defined as a monotonically increasing function with the signal-to-noise ratio (SNR) in [71]. That is to say, acting as a free-rider can strictly

improve one's own utility. However, the assumption that the cooperation is beneficial is no longer reasonable under eavesdropping attack.

As described in Chapter 1, the perfect secrecy in PLS can be achieved if the secrecy rate is limited by the system secrecy capacity, which is defined as the difference between the channel capacity of the destination and that of the eavesdropper [29]. The secrecy outage occurs if a target secrecy rate is larger than the instantaneous secrecy capacity. Intuitively, the conventional cooperation with either DF or amplify-and-forward (AF) improves the channel capacity both at the destination and the eavesdropper. If the eavesdropper achieves more cooperation gain than the destination does, the secrecy performance is in fact deteriorated compared to the direct transmission. Therefore, it is necessary to reconsider the user cooperation behaviors with secrecy constraints. This chapter focuses on this issue and the contributions are threefold.

1) The conventional cooperation scheme is proved to be negative from the secrecy perspective if the eavesdropper has a better channel condition than the destination. Here, the secure transmission probability (*one minus the secrecy outage probability*) is treated as the users' utilities. Given the passive eavesdropping, the users cannot estimate the channel state information (CSI) of the eavesdropper and thus cannot decide whether the cooperation is positive or not. Therefore, the users have no incentive to participate in the game and accordingly the game theory analysis becomes meaningless.

2) To motivate users, an opportunistic user cooperation scheme (OUCS) is developed which can consistently achieve a higher secure transmission probability than the direct transmission even if the eavesdropper has a better channel condition. That is to say, the users are motivated to join in the game for a higher secrecy performance. After the game theory analysis, mutual cooperation is found to be one of the Nash equilibriums if one-shot static game is considered.

3) The Stackelberg game is then adopted with a simple punishment mechanism to avoid free-riders and stimulate the mutual cooperation, because the users generally transmit in a sequential fashion. The game is modified to reflect the symmetry of the users, in which the user who decides whether to cooperate or not in the current cooperation period acts as the leader and the other user

acts as the follower. In other words, they act as the leader by turns. The follower will refuse to cooperate if the leader behaves as a free rider, until this leader provides cooperation again. The mutual cooperation will be the unique Nash equilibrium if the users care about the subsequent utilities. This result is more valuable because the system converges to the mutual cooperation even in the distributed systems with selfish users.

2.2 System Model and Problem Formulation

2.2.1 System model

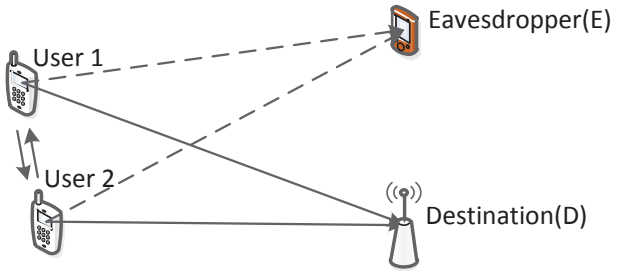

Figure 2.1: Two-user cooperation under eavesdropping attack.

The two-user cooperation under eavesdropping attack as shown in Fig 2.1 is considered. Two users intend to cooperate with each other to transmit their data to a common destination(D). An eavesdropper(E) overhears the data for illegal purpose through the *passive eavesdropping*, such that the CSI of the eavesdropper's links is unavailable. Both the destination and the eavesdropper employ the maximal ratio combining to achieve the diversity gain. The channel between two nodes i and j is modeled as Rayleigh block-flat fading with the average channel gain σ_{ij}^2, such that the channel fading coefficient $h_{ij} \sim CN\left(0, \sigma_{ij}^2\right)$. The potential cooperation partner is selected from neighboring users. Thus, the inter-user channels are assumed to be reliable (error-free) as is done in [71], and much better than the destination's and the eavesdropper's channels. To make it simple, we also assume that the channels between the users and the destination (and the eavesdropper) follow independent and identical distribution because the users are close to each other, and set $\sigma_{1D}^2 = \sigma_{2D}^2 = \sigma_{sd}^2$,

$\sigma_{1E}^2 = \sigma_{2E}^2 = \sigma_{se}^2$. Due to the passive eavesdropping, it is impossible to decide whether $\sigma_{sd}^2 > \sigma_{se}^2$ or not. The two users transmit their messages by turns based on the time division multiple access and a cycle forms one cooperation period. Both users are selfish and they choose whether to provide cooperation by themselves. Since the inter-user channel is assumed to be reliable, the DF cooperation is adopted to avoid the noise amplification. However, the simulation results of the AF cooperation will be also given for the comparison later. The transmit power of each node for every transmission period is restricted as P. If one user provides cooperation, it will offer $P/2$ to relay the other's signals. The power of additive white Gaussian noise at receivers is denoted by N_0.

2.2.2 Experimental evaluation on channel independence

The independence (/decorrelation) of channel gains among the antennas or cooperative users is the basis for the spatial diversity techniques. It has been introduced in Chapter 1 that both the academia [4–7] and industry [8–14] generally accept that the required separation distance between antennas to yield independent channel fading is the same order of carrier wavelengths (from half to several wavelengths). To confirm this conclusion again, we use the software defined radio platforms (NI USRP-2921) to evaluate the correlation coefficients for different separation distances between two antennas. The experiment setup is as shown in Fig 2.2. A transmitter continues to transmit the data packets, while two receivers estimate the received signal power related to every packet by using a probe that computes the average magnitude squared: analog.probe_avg_mag_sqrd_c().

The experiments are performed at 2.4GHz ISM band and both the line of sight (LOS) and non line of sight (NLOS) scenarios are considered. Each experiment transmits 2500 packets, and we perform three times to calculate the mean value of the correlation coefficients for different separation distances. Since there are some nonreceived packets, their received signal power is set to be -80dBm for computational convenience. The experiment results are shown in Table 2.1. As noted in [76], signals are often said to be "effectively" decorrelated if the correlation coefficient is below a certain threshold (typically 0.5

Figure 2.2: Experiment setup for evaluating channel correlations.

or 0.7), which is also the general case for the diversity applications [77–79]. It is observed from the Table 2.1 that in the experiments the correlation coefficient below 0.5 and 0.7 is hold for a distance larger than 100cm and 5cm respectively (the same order of the approximate carrier wavelength 12.5cm). This requirement is feasible and that's why many wireless devices nowadays exploit the multiple antennas to harvest the spatial diversity gain [10, 12, 14]. It is obviously applicable in cooperative relay networks, because the distance among distinct wireless devices is generally much longer than that within one device. Furthermore, researchers usually assume the independent channel gains pertaining to different transmission links for a simple theoretical analysis on their proposals, which is also adopted in our system model above.

Table 2.1: Correlation coefficients vs. separation distance between antennas

	1	5	10	20	50	100	150	200(cm)
LOS	0.76	0.70	0.56	0.52	0.69	0.61	0.42	0.24
NLOS	0.48	0.60	0.61	0.60	0.42	0.45	0.26	0.35

2.2.3 Problem formulation

The cooperation decision is made by both users through game theory to maximize their own utilities. Generally, a game is performed among N players. The strategies of these players comprise a strategy profile $\mathbf{s} = \{s_1, s_2, ...s_i, ...s_N\}$, where s_i is the selected strategy of user i. The possible strategies of user i is

defined as the strategy space of user i, $\mathbf{S}_i$ and $s_i \in \mathbf{S}_i$. The strategy profile of the opponents of user i is denoted by $\mathbf{s}_{-i} = \{s_1, s_2, ...s_{i-1}, s_{i+1}, ...s_N\}$. Under the strategy profile $\mathbf{s}$, the utility of user i is expressed as $U_i(\mathbf{s})$. Using these notations, we can easily give the definition of Nash equilibrium [71], which describes the specific strategy profiles that no user can improve its utility by merely changing its own strategy.

Definition: (Nash equilibrium) The strategy profile $\mathbf{s}^*$ is a Nash equilibrium if for each player i,

$$U_i(s_i^*, \mathbf{s}_{-i}^*) \geq U_i(s_i, \mathbf{s}_{-i}^*), \forall s_i \in \{\mathbf{S}_i - \{s_i^*\}\} \tag{2.1}$$

For the two-user cooperation game, both users have two strategies, namely cooperate (C) and not-cooperate (NC). Therefore, the game can be represented by a strategic form as shown in Table 2.2, where $\rho_i = \frac{P_i}{N_0} = \frac{P}{N_0}$ denotes the system SNR and $U_i(s_1, s_2) = u_i(x, y)$ is the utility function for different strategy profiles. The expression of $u_i(x, y)$ depends on which kind of performance the users care about. For example, the Shannon capacity $u_i(x, y) \approx \log_2(x|h_{1D}|^2 + y|h_{2D}|^2)$ and the transmission reliability for binary differential phase shift keying $u_i(x, y) = 1 - p_e = 1 - 0.5e^{-(x|h_{1D}|^2 + y|h_{2D}|^2)}$ are considered as the utilities in [71]. These utility functions monotonically increases with the received SNR. Each user can get better payoff if it chooses NC no matter what the other user chooses. The strategy profile {NC, NC} is the unique Nash equilibrium for this game because each user intends to be the free-rider. The authors of [71] also analyze the repeated game and find that {C, C} may be another Nash equilibrium if users consider future utilities.

Table 2.2: Strategy form for the two-user cooperative relaying game

User 1 \ User 2	Cooperate	Not-cooperate
Cooperate	$\left[u_1\left(\frac{\rho_1}{2}, \frac{\rho_2}{2}\right), u_2\left(\frac{\rho_1}{2}, \frac{\rho_2}{2}\right)\right]$	$\left[u_1\left(\frac{\rho_1}{2}, 0\right), u_2\left(\frac{\rho_1}{2}, \rho_2\right)\right]$
Not-cooperate	$\left[u_1\left(\rho_1, \frac{\rho_2}{2}\right), u_2\left(0, \frac{\rho_2}{2}\right)\right]$	$[u_1(\rho_1, 0), u_2(0, \rho_2)]$

Almost all the papers about the game theory analysis of cooperative relaying assume that cooperation from others is beneficial for the users [71–75].

However, the cooperation is not always positive for different considered utility functions. This paper analyzes the secure transmission probability in two-user cooperation scenario under eavesdropping attack and shows that the conventional cooperation in fact deteriorates this performance if $\sigma_{se}^2 > \sigma_{sd}^2$. As noted above and Chapter 1, the secrecy capacity is defined as the difference between the channel capacities of the destination and the eavesdropper [29],

$$C_s = [C_D - C_E]^+ \tag{2.2}$$

where, $[x]^+ = \max\{0, x\}$, C_D and C_E are the channel capacities of the destination and the eavesdropper respectively. The outage occurs if the instantaneous secrecy capacity of the system is less than a target secrecy rate R_s. For simplicity, we focus on the high system SNR scenario as [36, 71]. The secure transmission probability, $1 - \Pr\{outage\} = \Pr\{C_s \geq R_s\}$, is treated as the utility function,

$$\begin{aligned} u_i(x,y) &= \Pr\{C_s \geq R_s\} \\ &= \Pr\Big\{r\log_2\left(1 + x|h_{1D}|^2 + y|h_{2D}|^2\right) \\ &\quad -r\log_2\left(1 + x|h_{1E}|^2 + y|h_{2E}|^2\right) \geq R_s\Big\} \\ &\approx \Pr\left\{r\log_2\left(\frac{x|h_{1D}|^2 + y|h_{2D}|^2}{x|h_{1E}|^2 + y|h_{2E}|^2}\right) \geq R_s\right\} \end{aligned} \tag{2.3}$$

where, $r = \frac{1}{2}$ if user i gets the cooperation from the other user due to the rate degradation of the cooperative relaying and $r = 1$ for the direct transmission [16, 75].

Property 1: The conventional cooperation (DF) deteriorates the secure transmission probability if the eavesdropper has a better average channel gain than the destination.

Proof. We will compare the secure transmission probability for different strategy profiles. Without loss of generality, we derive the utilities of user 1 (Appendix

A.1).

$$u_1\left(\frac{\rho_1}{2},\frac{\rho_2}{2}\right)=\frac{3\xi+1}{(\xi+1)^3} \tag{2.4}$$

$$u_1\left(\rho_1,\frac{\rho_2}{2}\right)=\frac{7\xi+2}{(\xi+1)(\xi+2)(2\xi+1)} \tag{2.5}$$

$$u_1\left(\frac{\rho_1}{2},0\right)=u_1(\rho_1,0)=\frac{1}{\xi/\delta+1} \tag{2.6}$$

where $\xi=\frac{\sigma_{se}^2\delta^2}{\sigma_{sd}^2}$ and $\delta=2^{R_s}$. For any target secrecy rate $R_s>0$, we can get $\delta>1$ and further prove that

$$u_1(\rho_1,0)=u_1\left(\frac{\rho_1}{2},0\right)>\frac{1}{\xi+1}>u_1\left(\rho_1,\frac{\rho_2}{2}\right)>u_1\left(\frac{\rho_1}{2},\frac{\rho_2}{2}\right) \tag{2.7}$$

if $\xi>1$, which always holds when $\frac{\sigma_{se}^2}{\sigma_{sd}^2}>1$ (i.e., the eavesdropper has a better average channel gain than the destination). □

This result shows that the cooperation provided by other users in fact reduce the secure transmission probability if the eavesdropper has a better channel condition. Fig 2.3 illustrates the analytical curves and simulation results with $R_s=0.1$bits/s/Hz to reconfirm Property 1 (the simulation results of AF is also presented). The conventional cooperation with both DF and AF is negative compared to the direct transmission if $\frac{\sigma_{se}^2}{\sigma_{sd}^2}>1$. For the passive eavesdropping, the users cannot estimate the eavesdropper's CSI and thus cannot decide whether the cooperation from the other user is positive or not considering the secrecy. Therefore, they will have no incentive to participate in the game and the game theory analysis becomes meaningless. To describe this problem, we formulate the necessary condition of the cooperative relaying game first. Then we motivate the cooperation behavior through an opportunistic cooperation scheme which achieves a higher secure transmission probability than the direct transmission for any $\frac{\sigma_{se}^2}{\sigma_{sd}^2}$ values. The mutual cooperation is found to be one of the Nash equilibriums. After that, the Stackelberg game is modified with a punishment mechanism to make the mutual cooperation become the unique Nash equilibrium.

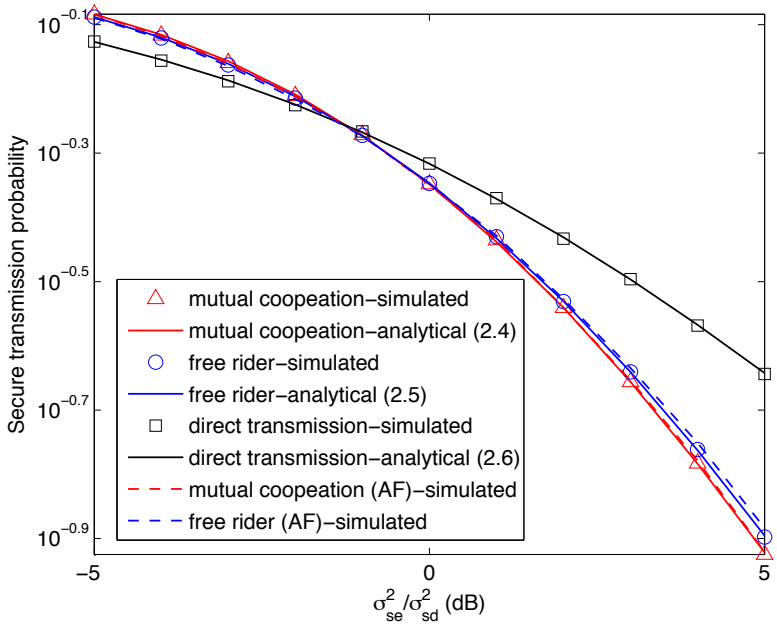

Figure 2.3: Secure transmission probability of user 1 for different strategy profiles with the conventional cooperation scheme.

2.3 User-Motivated Cooperation Scheme under Eavesdropping Attack

2.3.1 Necessary condition of the cooperation game

The users will prefer not to participate in the game if they cannot obtain benefits from the cooperation. Therefore, we formulate the necessary condition of the cooperation game to describe whether the users are interested in the game. Concentrating on the system model, we only consider the two-user cooperation for a simple representation, although it can be easily extended to the multi-user cooperation.

Necessary condition of the two-user cooperation game: For at least one strategy of user i, s_i, the cooperation from the other user should generate a higher utility compared to the NC status of the other user, i.e.,

$$U_i(s_i, \mathrm{C}) > U_i(s_i, \mathrm{NC}), \exists s_i \in \mathbf{S}_i \tag{2.8}$$

It can be understood as follows: A user who joins in the game intends to improve its own utility through mutual cooperation or as the free-rider. If the cooperation cannot realize any performance improvement no matter what strategy the user chooses, the decision not to attend the game is better. This formulated necessary condition can be used to validate whether the game theory analysis for the cooperation is necessary. In [71–75], it is all assumed that the cooperation can provide additional utilities to the users. For example, users can strictly improve their utilities if they act as the free-rider in [71], i.e., $U_i(s_i, \mathrm{C}) > U_i(s_i, \mathrm{NC})$ if s_i is NC. The source(s) should pay for the cooperation power to other users in [73] and [75], also because the cooperation from others is more beneficial than the direct transmission. However, according to Property 1, the necessary condition is not satisfied in terms of the secure transmission probability if an eavesdropper exists and has a better channel condition than the destination. Therefore, if we still adopt the conventional cooperation scheme under eavesdropping attack and cannot ensure that the destination will have a much better average channel gain, the users would prefer the direct transmission by themselves and have no interest in the cooperation game.

2.3.2 Motivate the user cooperation through an opportunistic user cooperation scheme (OUCS)

The analysis above shows that with the secrecy constraints none of the users is interested in the conventional cooperation mode. To satisfy the necessary condition of the cooperation game, the cooperation scheme must be revised to make it positive for any $\frac{\sigma_{se}^2}{\sigma_{sd}^2}$ values. The typical cooperation schemes for secrecy includes cooperative beamforming or jamming, as designed in [80–83]. The game theory analysis in these studies is reasonable, since the users can always achieve a better secrecy performance by the cooperation under certain assumptions (e.g., the CSI of the eavesdropping channel is available [80–83] or the jamming signal can be cancelled at the destination [83]). However, these assumptions are not valid in general cases, especially for the passive eavesdropping, and also the cooperative beamforming or jamming is relatively complicat-

ed. To relax the assumptions and reduce the complexity, we exploit the concept of the opportunistic cooperation to motivate the user cooperation.

The cooperation scheme is designed and presented as Fig 2.4. We consider the scenario wherein user 1 transmits its message and user 2 chooses the strategy C. Let's denote the average inter-user channel gain as $E(|h_{in}|^2) = \sigma_{in}^2$, where h_{in} is the inter-user channel coefficient. If user 1 finds out that $|h_{1D}|^2 \geq a \min\{|h_{in}|^2, |h_{2D}|^2\}$ (where a is the regulatory factor and $a = 1/\delta$ is found to be a rational choice), user 1 gives up the cooperation and transmits the message by itself. Otherwise, user 1 transmits the message to user 2 first and user 2 forwards the message using *different codebooks* [84][1]. Thus, receivers at both the destination and the eavesdropper cannot combine the signals of the direct and relay links. The destination uses the signal of the relay link, whereas the eavesdropper attempts to overhear the message in both phases.

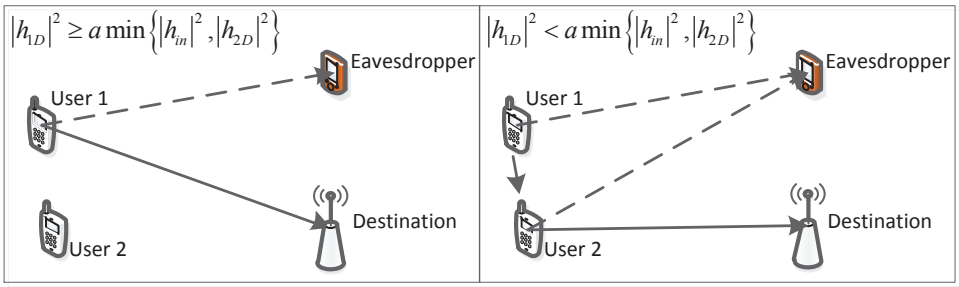

Figure 2.4: The OUCS for user 1 when user 2 provides cooperation.

Property 2: The OUCS achieves a higher secure transmission probability than the direct transmission for any $\frac{\sigma_{se}^2}{\sigma_{sd}^2}$ values if the inter-user channel is dominant and a is set to be $1/\delta$.

Proof. When user 2 provides cooperation to user 1 and OUCS is adopted, the secure transmission probability of user 1 is derived as (Appendix A.2)

$$u_1\left(\frac{\rho_1}{2}, \frac{\rho_2}{2}\right) = u_1\left(\rho_1, \frac{\rho_2}{2}\right) \overset{a=\frac{1}{\delta}}{=} \frac{1}{\xi/\delta + 1} + \Phi \tag{2.9}$$

where $\Phi = \frac{\xi^2+2\xi\delta+\xi\xi'\delta+\xi^2\delta(1-\xi')}{(\xi+1)(\xi'+1)(\xi+\xi\delta+\xi'\delta+\delta)(\xi+\xi\delta+\xi'\delta+2\delta)}$ and $\xi' = \frac{\sigma_{se}^2\delta^2}{\sigma_{in}^2}$. The utilities of user

[1]The decision on cooperation can be made in a centralized manner or a distributed manner as shown in [85] (by setting timers at user 1 and user 2 inversely proportional to $|h_{1D}|^2$ and $a \min\{|h_{in}|^2, |h_{2D}|^2\}$ respectively).

1 when user 2 chooses strategy NC are the same as the results in Sec 2.2.2, that is,

$$u_1\left(\frac{\rho_1}{2}, 0\right) = u_1\left(\rho_1, 0\right) = \frac{1}{\xi/\delta + 1} \tag{2.10}$$

The dominance of the inter-user channel in Property 2 means that the average channel gain of the inter-user channel is better than the product of the average eavesdropping channel gain and δ^2, i.e., $\sigma_{in}^2 > \sigma_{se}^2\delta^2$. Considering the small target secrecy rate, this requirement can be easily satisfied by selecting a neighboring user as the cooperation partner[2], which agrees with the system model. Therefore, we can obtain $\xi' < 1$ and thus $\Phi > 0$. Because $u_1\left(\frac{\rho_1}{2}, \frac{\rho_2}{2}\right) > u_1\left(\frac{\rho_1}{2}, 0\right)$ and $u_1\left(\rho_1, \frac{\rho_2}{2}\right) > u_1\left(\rho_1, 0\right)$ when $\Phi > 0$, Property 2 is proved. □

Fig 2.5 gives the simulation results of the OUCS with $R_s = 0.1$bits/s/Hz to confirm the property, assuming that $\sigma_{se}^2/\sigma_{in}^2 = -5, -10, -15$ dB. It is observed that the users can always obtain a higher secure transmission probability than the direct transmission. Thus, the users are motivated to participate in the cooperation game. Apparently, the performance improvement from the cooperation of one partner is limited. If multiple users are clustered together, the multi-user cooperation can be exploited to obtain more cooperation gain. The simulation results for five-user cooperation are also shown in Fig 2.5 to illustrate the performance improvement by the multi-user cooperation. The detailed analysis for multi-user cooperation will be considered in Chapter 3.

The strategy form with the OUCS is derived in Table 2.3. The necessary condition of the cooperation game is obviously satisfied. Both users intend to participate in the game because they can improve their secure transmission probabilities via the other's cooperation.

Table 2.3 shows that all of the four strategy profiles are Nash equilibriums. Neither of the users regrets its choice for any strategy profiles. It turns out that,

[2]For the neighboring users, the inter-user channel is always much better than the channels between them and other receivers due to the channel attenuation. In addition, a certain distance between the users and the eavesdropper can be also maintained through the geographic constraints or physical inspection. Therefore, $\sigma_{in}^2 > \sigma_{se}^2\delta^2$ is generally satisfied. Here, the effect of $\delta^2 = 2^{2R_s}$ is limited since the target secrecy rate is usually set to be very small to achieve an acceptable secrecy outage probability, e.g., $R_s = 0.1$bits/s/Hz in [29, 36].

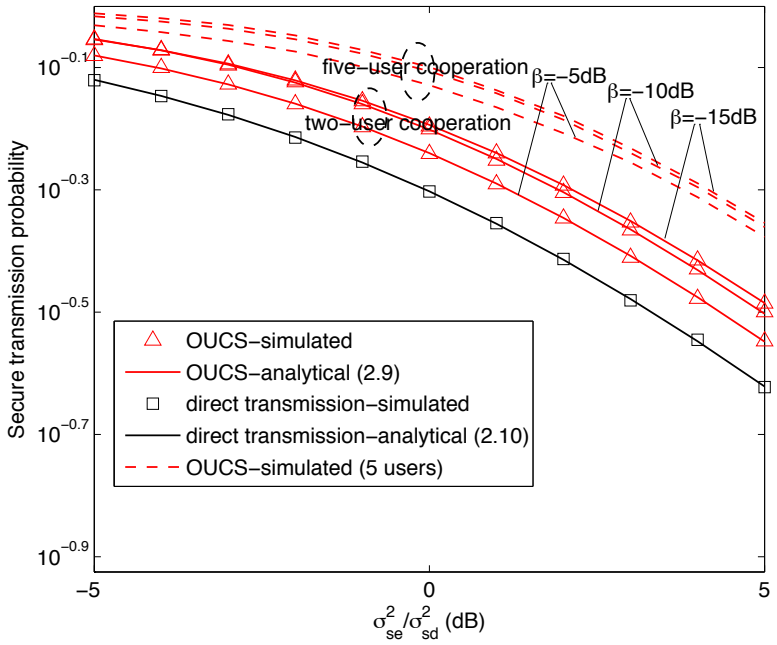

Figure 2.5: Secure transmission probability of user 1 for different strategy profiles with the OUCS ($\beta = \frac{\sigma^2_{se}}{\sigma^2_{in}}$).

if we treat this cooperation game as the one-shot static game [70], we cannot ensure that the users will select C as their strategies. Fortunately, the users always need a series of cooperation periods to transmit their data and also they transmit by turns. We can modify the Stackelberg game with a punishment mechanism to make the strategy profile {C, C} as the unique Nash equilibrium.

Table 2.3: Strategy form for the two-user cooperative relaying game with the OUCS (in terms of the secure transmission probability)

User 1 \ User 2	Cooperate	Not-cooperate
Cooperate	$\left[\frac{1}{\xi/\delta+1}+\Phi, \frac{1}{\xi/\delta+1}+\Phi\right]$	$\left[\frac{1}{\xi/\delta+1}, \frac{1}{\xi/\delta+1}+\Phi\right]$
Not-cooperate	$\left[\frac{1}{\xi/\delta+1}+\Phi, \frac{1}{\xi/\delta+1}\right]$	$\left[\frac{1}{\xi/\delta+1}, \frac{1}{\xi/\delta+1}\right]$

2.3.3 Motivate the mutual cooperation using Stackelberg game

The players in the Stackelberg game take actions in sequence. Focusing on our model, we also only give the mathematical formulation of the two-user Stackelberg game [86]. We denote that the user who takes action at the current time slot as the leader (L), and the other user as the follower (F). In the Stackelberg game, the leader is aware of the utility function of the follower. Thus, the leader can derive the optimal strategy of the follower s_F^* by assuming that it selects strategy s_L^0. Specifically, if the leader performs strategy s_L^0, the follower will choose strategy, $s_F^*(s_L^0) = \arg\max_{s_F \in \mathbf{S}_F} U_F(s_L^0, s_F)$. Therefore, the leader can decide its optimal strategy through $s_L^* = \arg\max_{s_L^0 \in \mathbf{S}_L} U_L(s_L^0, \arg\max_{s_F \in \mathbf{S}_F} U_F(s_L^0, s_F))$. Consequently, the optimal strategy of the follower is decided by $s_F^* = \arg\max_{s_F \in \mathbf{S}_F} U_F(s_L^*, s_F)$.

Because the users transmit their messages by turns, the cooperative relaying game is proper to be modeled by the Stackelberg game. However, the leader and the follower are always fixed for the general Stackelberg game [73,74,82,83]. In order to reflect the symmetrical structure of the cooperation period as shown in Fig 2.6, we modify the Stackelberg game as follows: the user who decides whether to provide cooperation or not in the current time slot is treated as the leader, and the follower is the user that is transmitting. That is to say, the two users take turns to be the leader, which is different from the general Stackelberg game.

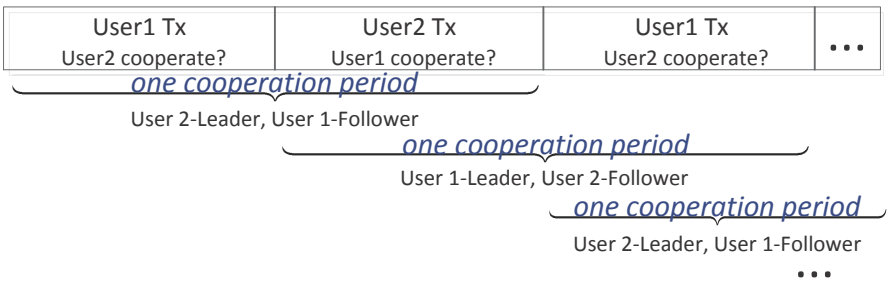

Figure 2.6: Stackelberg game for the two-user cooperation.

From the Table 2.3, we can obtain that

$$U_F(s_L^0, \mathrm{C}) = U_F(s_L^0, \mathrm{NC}), \forall s_L^0 \in \{\mathrm{C}, \mathrm{NC}\} \tag{2.11}$$

which means that the follower's selection does not affect its own secure transmission probability. To motivate the cooperation, we design a punishment mechanism that the follower user refuses to cooperate if the leader intends to be a free-rider. That is to say, if the leader selects strategy NC in one cooperation period, the follower in this cooperation period will choose NC accordingly in future periods until the leader chooses the strategy C again ($s_F^*(\mathrm{NC}) = \mathrm{NC}$). If the leader selects strategy C currently, it will get the cooperation from the follower as a reward ($s_F^*(\mathrm{C}) = \mathrm{C}$). Therefore, we can calculate the different utilities for the leader's strategies,

$$U_L(\mathrm{C}, s_F^*(\mathrm{C})) = U_L(\mathrm{C}, \mathrm{C}) = \frac{1}{\xi/\delta + 1} + \Phi \tag{2.12}$$

$$U_L(\mathrm{NC}, s_F^*(\mathrm{NC})) = U_L(\mathrm{NC}, \mathrm{NC}) = \frac{1}{\xi/\delta + 1} \tag{2.13}$$

We can further derive

$$s_L^* = \arg\max_{s_L^0 \in \mathbf{S}_L} U_L(s_L^0, s_F^*(s_L^0)) = \mathrm{C} \tag{2.14}$$

Both users prefer choosing C as their strategies if they care about the subsequent punishment from each other. The strategy profile {C, C} becomes the unique Nash equilibrium when we employ the Stackelberg game and the punishment mechanism.

2.4 Summary

The game theory is exploited to analyze the two-user cooperation behaviors under eavesdropping attack. It is proved that the conventional cooperation from others is in fact negative for the physical layer security if the eavesdropper has a

better average channel gain that the destination, and users will not participate in the cooperation game. Therefore, a simple but effective opportunistic user cooperation scheme (OUCS) is introduced to motivate users, which can always achieve a better secrecy performance than the direct transmission. The mutual cooperation is thus found to be a Nash equilibrium. To make the mutual cooperation as the unique Nash equilibrium, we further adopt the modified Stackelberg game with a punishment mechanism. Through the analysis of the Stackelberg game, both users will select cooperation as their optimal strategies based on the OUCS, which is also a global optimality for the users. Due to its superiority, the designed OUCS will be extended to the multi-user cooperation scenarios in next chapter.

Chapter 3

Multi-User OUCS with Full Secrecy Diversity for Cooperative Relay Networks (CRNs)

The opportunistic user cooperation scheme (OUCS) is exploited to motivate user cooperation under eavesdropping attack in Chapter 2. However, the OUCS therein only solves the problem of whether to cooperate. In this chapter we extend the results of Chapter 2, and analyze the multi-user cooperative relay networks by modifying the OUCS to further solve the problem of with whom to cooperate.

For mathematical convenience, we first define a secrecy performance index called secrecy-providing capability (SPC) for both the source and the cooperative users(/relays). By comparing the values of SPC of these nodes, the OUCS jointly decides whether to cooperate and with whom to cooperate from the perspective of physical layer security. The secrecy outage performance of the OUCS is then derived. From the results we prove that full secrecy diversity can be achieved (i.e., the diversity order is $N+1$ for one source with N cooperative users), which outperforms existing alternatives in the literature. Numerical results are then provided to validate the theoretical analysis.

Moreover, the full secrecy diversity performance of the OUCS is also confirmed in another typical multi-user cooperative relay scenario that multiple sources share a dedicated cooperative relay.

3.1 Introduction

In cooperative relay networks, the cooperation scheme itself is an important fact to motivate users' cooperation. It is proved in Chapter 2 that the opportunistic user cooperation scheme (OUCS), which decides whether to cooperate or not according to the channel conditions, is feasible to realize secrecy-enhanced data transmission under the external eavesdropping attack. On the other hand, if there are multiple cooperative users(/relays), which relay(s) is selected to assist the transmission also affects the performance a lot. To apply the cooperative relaying more effectively, the optimal relay selection strategy is introduced by considerable works [41, 85, 87–89].

From the perspective of physical layer security (PLS), the application of optimal relay selection has also been researched by [44–49]. The authors in [44–46] realize enhanced PLS through the ordinary user cooperation with relay selection, but they just analyze a special scenario in which the direct links (the link between the source and the eavesdropper as well as that between the source and the destination) are blocked. Although the direct links are considered in [47, 48], the channel capacities of the source-relay links are not taken into account in the relay selection process and the cooperation is also performed blindly without considering whether it is beneficial to the secrecy performance. Furthermore, in [49] only the eavesdropper exploits the direct link from the source to it. Due to these limitations, the schemes in [44–49] cannot achieve the full secrecy diversity performance, which motivates us to modify the OUCS proposed in Chapter 2 to realize full secrecy diversity.

In the OUCS of Chapter 2, however, the decision on the cooperation is only based on the channel state information (CSI) of the legitimate links, and does not consider the CSI of the eavesdropping links. This CSI should be helpful to further improve the secrecy performance if it's available. In addition, only

one cooperative relay is assumed in that work. Given multiple cooperative relays, the relay selection issue should also be taken into consideration. In this chapter, we analyze the multi-user cooperative relay networks and revise the OUCS with the concept of optimal relay selection to achieve full diversity from the perspective of PLS. The main contributions can be outlined as follows: 1) A secrecy performance index called secrecy-providing capability (SPC) is defined for all the transmitter nodes, including the source and the cooperative relays, under different CSI assumptions of the eavesdropping links. Based on the values of SPC, the OUCS jointly decides whether to cooperate and with whom to cooperate to enhance the transmission security. 2) The secrecy outage probability of the OUCS is derived accordingly. By analyzing the diversity order it is found that the full diversity performance (i.e., diversity order $N + 1$ for N cooperative relays) is achieved, which outperforms existing alternatives in [44–49] (in which at most diversity order N can be achieved). 3) Another typical multi-user scenario of the cooperative relay networks is also considered, in which a dedicated cooperative relay is shared by multiple sources. It is observed that with minor changes the OUCS can still achieve the full secrecy diversity performance.

3.2 System Model

The cooperative network considered in this paper is shown in Fig 3.1, which consists of one source (S), one destination (D), N cooperative relays (R_1, R_2, ..., R_N) and one eavesdropper (E). S intends to transmit confidential information to D securely under the eavesdropping attack of E. The cooperative relays dedicate their resources to assist the transmission not only for the reliability but also for the security. All of the nodes are assumed to operate in the half-duplex mode. Due to the low complexity and favorable diversity performance, optimal relay selection strategy is adopted in which only the "best" relay is selected to assist the transmission. As usual, cooperative relaying is divided into two phases for one transmission. In Phase I, the source broadcasts its message and other nodes listen to it. Then in Phase II, the selected cooperative relay R_{n*} forwards this

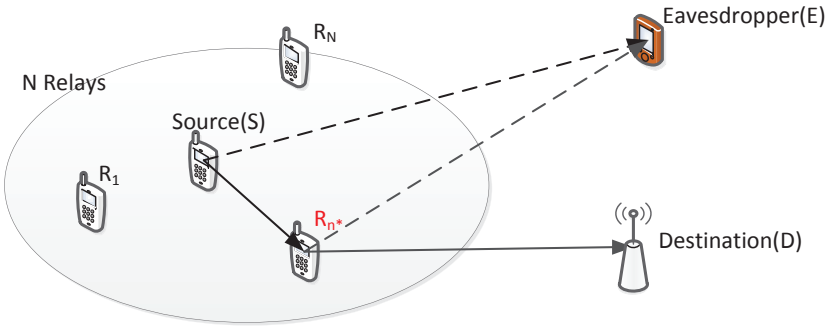

Figure 3.1: Multi-user cooperative networks under eavesdropping attack.

message. The receivers (both D and E) combine the signals of the two phases to harvest the spatial diversity gain through maximal ratio combining.

Similar to Chapter 2, the transmission links are modelled as Rayleigh block-flat fading channels. Specifically, the channel coefficient h_{ij} between nodes i and j is a circularly symmetric complex Gaussian random variable with mean zero and variance σ_{ij}^2, and it changes independently from one transmission to another. The instantaneous CSI between legitimate nodes is supposed to be known through channel estimation. As for the CSI between legitimate nodes and the eavesdropper, three cases are considered for different real-world systems: (A)the CSI cannot be estimated; (B)statistical CSI can be estimated; (C)instantaneous CSI can be estimated[1] [44]. The noise at each receiver is assumed as additive white Gaussian noise with variance N_0. The source and relays transmit signals with power P, and $\rho = P/N_0$ represents the average signal-to-noise ratio (SNR) of the system.

3.3 Scheme Descriptions

In this section, a more precise secrecy performance of the conventional user cooperation is introduced first. Then we give the definition of SPC, based on which the proposed multi-user OUCS is decided.

[1]There are examples of real-world systems corresponding to the three cases: (A)the eavesdropper performs strict passive eavesdropping; (B)the location of the eavesdropper can be determined to analyze its average channel conditions; (C)the eavesdropper is also a legitimate node which transmits its own signals but is prohibited from obtaining the confidential messages [90].

As described in the system model, the source broadcasts a message first and then the selected cooperative relay forwards it. We assume that the set of cooperative relays is formed to be much closer to the source and the relays can decode the source message correctly. It is reasonable for the relays to adopt the decode-and-forward (DF) protocol, in which the selected relay re-encodes and forwards its decoded message to the destination. Both the destination and the eavesdropper can combine the signals from the source and the relay. Therefore, their channel capacities $C_{D(E)} = \frac{1}{2}\log_2(1 + \gamma_{SD(E)} + \gamma_{n^*D(E)})$, where n^* represents the selected relay R_{n^*} and $\gamma_{ij} = \rho|h_{ij}|^2$ denotes the received SNR at the receiver j for the link from node i to node j.

In [47,48] and Chapter 2, the secrecy capacity using DF protocol is derived directly by the definition $C_s = [C_D - C_E]^+$. However, considering the select relay is also a legitimate receiver besides the destination, the channel capacity of the source-relay link should be taken into account when calculating the secrecy capacity, i.e., $C_s = [\min\{C_{n^*}, C_D\} - C_E]^+$ as that in [91,92]. Therefore, a more precise secrecy capacity of the conventional cooperation is calculated by

$$\begin{aligned} C_s &= \left[\min\left\{\frac{1}{2}\log_2(1+\gamma_{Sn^*}), \frac{1}{2}\log_2(1+\gamma_{SD}+\gamma_{n^*D})\right\}\right. \\ &\qquad \left. -\frac{1}{2}\log_2(1+\gamma_{SE}+\gamma_{n^*E})\right]^+ \\ &= \left[\frac{1}{2}\log_2\left(\frac{1+\min\left\{\gamma_{Sn^*}, \gamma_{SD}+\gamma_{n^*D}\right\}}{1+\gamma_{SE}+\gamma_{n^*E}}\right)\right]^+ \\ &\overset{high\,\rho}{\approx} \left[\frac{1}{2}\log_2\left(\frac{\min\left\{\gamma_{Sn^*}, \gamma_{SD}+\gamma_{n^*D}\right\}}{\gamma_{SE}+\gamma_{n^*E}}\right)\right]^+ \end{aligned} \tag{3.1}$$

The secrecy outage event occurs if the instantaneous secrecy capacity is less than a target secrecy rate R_s, and the secrecy outage probability is $\Pr\{C_s < R_s\}$.

Similar to Chapter 2, it can be observed from Eqn (3.1) that the conventional cooperation provides diversity gain at both the destination and the eavesdropper, thereby affecting anti-eavesdropping capabilities. Meanwhile, the channel capacity of the link between the source and the selected relay may become the bottleneck in some cases, which should be also considered in the OUCS.

The SPC is defined for the source and the cooperative relays first to facilitate the implementation of the OUCS. To restrict the diversity gain achieved by the eavesdropper, the randomize-and-forward (RF) cooperation scheme proposed in [84] is exploited as Chapter 2 and [90]. The source and the cooperative relays use different codebooks to transmit the confidential message, and the transmission is secured as long as the broadcast and the relaying phases are secured separately. Furthermore, the channel capacity of the source-relay link is included in the definition of SPC for the relays. The detailed definition of SPC is given in Table 3.1.

Table 3.1: Definition of SPC

	Case A	Case B	Case C
Source	γ_{SD}	$\frac{\gamma_{SD}}{\sigma_{SE}^2}$	$\frac{\gamma_{SD}}{\gamma_{SE}}$
Relay(R_n)	$\min\{\gamma_{Sn}, \gamma_{nD}\}$	$\min\left\{\frac{\gamma_{Sn}}{\sigma_{SE}^2}, \frac{\gamma_{nD}}{\sigma_{nE}^2}\right\}$	$\min\left\{\frac{\gamma_{Sn}}{\gamma_{SE}}, \frac{\gamma_{nD}}{\gamma_{nE}}\right\}$

The proposed OUCS is designed based on the SPC, including whether to cooperate and with whom to cooperate. Specifically, the optimal cooperative relay is firstly selected by $n^* = \underset{n\in\{1,2,\ldots,N\}}{\arg\max}\{\mathrm{SPC}_n\}$. Then if $\mathrm{SPC}_S \geq \mathrm{SPC}_{n^*}$, the source transmits its message to the destination directly in Phase I and the relays keep silent in Phase II[2]; otherwise, the cooperation mode is performed that the source transmits its message to the selected relay in Phase I and the relay forwards it by RF protocol in Phase II. The eavesdropper attempts to intercept the information in both phases.

The instantaneous secrecy capacity of the OUCS can be expressed as follows,

$$C_s = \mathrm{I}(\mathrm{SPC}_S \geq \mathrm{SPC}_{n^*})C_{s-direct} + \mathrm{I}(\mathrm{SPC}_S < \mathrm{SPC}_{n^*})C_{s-RF} \tag{3.2}$$

where $\mathrm{I}(X)$ is the indicator function (i.e., $\mathrm{I}(X) = 1/0$ if event X is true/false),

[2]The secrecy capacity can be further increased if the source continues to transmit in Phase II. For a simple comparison between the OUCS and alternatives, this manner is not considered here.

and

$$\begin{aligned} C_{s-direct} &= \left[\frac{1}{2}\log_2\left(1+\gamma_{SD}\right)-\frac{1}{2}\log_2\left(1+\gamma_{SE}\right)\right]^+ \\ &\overset{high\rho}{\approx} \left[\frac{1}{2}\log_2(\frac{\gamma_{SD}}{\gamma_{SE}})\right]^+ \end{aligned} \tag{3.3}$$

$$\begin{aligned} C_{s-RF} &= \left[\frac{1}{2}\log_2(\min\left\{\frac{1+\gamma_{Sn^*}}{1+\gamma_{SE}},\frac{1+\gamma_{n^*D}}{1+\gamma_{n^*E}}\right\})\right]^+ \\ &\overset{high\,\rho}{\approx} \left[\frac{1}{2}\log_2(\min\left\{\frac{\gamma_{Sn^*}}{\gamma_{SE}},\frac{\gamma_{n^*D}}{\gamma_{n^*E}}\right\})\right]^+ \end{aligned} \tag{3.4}$$

From Eqn (3.2), the secrecy outage performance and diversity order can be analyzed as shown in the next section.

The implementation of the multi-user OUCS can be also made in a distributed [85] or centralized manner. For the distributed manner, a timer which is inversely proportional to the SPC is set at each node and the timers of the nodes exhaust in sequence according to their SPC. If the timer of the source exhausts first, it broadcasts a flag message to relay nodes and the direct transmission will be performed. Otherwise, cooperation occurs if the timer of a cooperative relay exhausts first. For the centralized manner, a control node maintains a SPC table for all the nodes. The implementation is made by looking up this table.

3.4 Performance Analysis

The approximate closed-form expressions for the secrecy outage probability of the proposed OUCS are derived in this section. Based on the results, the diversity order is then analyzed.

3.4.1 Secrecy outage probability

The Case A is considered first in which no CSI of the eavesdropping links is available. According to the definition, the secrecy outage probability can be

written as

$$P_{out}^{A} = \Pr\left(\frac{1}{2}\log_2(\frac{\gamma_{SD}}{\gamma_{SE}}) < R_s, \gamma_{SD} \geq \min\{\gamma_{Sn^*}, \gamma_{n^*D}\}\right) \Pr\left(\frac{1}{2}\log_2(\min\left\{\frac{\gamma_{Sn^*}}{\gamma_{SE(n^*)}}, \frac{\gamma_{n^*D}}{\gamma_{n^*E}}\right\}) < R_s, \gamma_{SD} < \min(\gamma_{Sn^*}, \gamma_{n^*D})\right) \quad (3.5)$$

Here, we consider that orthogonal frequency resources (e.g., different subchannels in OFDM systems) are assigned to the direct link and the relaying links in the OUCS, such that γ_{SE} and $\gamma_{SE(n)}, n \in \{1, 2, ..., N\}$, are independent from each other[3]. By denoting $\lambda_{ij} = 1/\sigma_{ij}^2$ we can get

$$\begin{aligned}
P_{out}^{A} &= \int_0^\infty \prod_{n=1}^{N} \left[1 - e^{-(\lambda_{Sn}+\lambda_{nD})x}\right] \lambda_{SD} e^{-\lambda_{SD}x} e^{-\lambda_{SE}\frac{x}{2^{2R_s}}} dx \\
&\quad + \sum_{n=1}^{N} \int_0^\infty (1 - e^{-\lambda_{SD}x}) \prod_{\substack{m=1 \\ m\neq n}}^{N} \left[1 - e^{-(\lambda_{Sm}+\lambda_{mD})x}\right] \\
&\quad \left\{\lambda_{Sn} e^{-\lambda_{Sn}x} \int_x^\infty \lambda_{nD} e^{-\lambda_{nD}y} dy - \left[\lambda_{Sn} e^{-\lambda_{Sn}x}(1 - e^{-\lambda_{SE}\frac{x}{2^{2R_s}}}) \right.\right. \\
&\quad \left. \int_x^\infty \lambda_{nD} e^{-\lambda_{nD}y}(1 - e^{-\lambda_{nE}\frac{y}{2^{2R_s}}}) dy\right] \\
&\quad + \lambda_{nD} e^{-\lambda_{nD}x} \int_x^\infty \lambda_{Sn} e^{-\lambda_{Sn}y} dy - \left[\lambda_{nD} e^{-\lambda_{nD}x}(1 - e^{-\lambda_{nE}\frac{x}{2^{2R_s}}}) \right. \\
&\quad \left.\left. \int_x^\infty \lambda_{Sn} e^{-\lambda_{Sn}y}(1 - e^{-\lambda_{SE}\frac{y}{2^{2R_s}}}) dy\right]\right\} dx \\
&= \sum_{i=0}^{N} (-1)^i \sum_{\substack{J\subseteq\{1,2,...,N\} \\ |J|=i}} \frac{\lambda_{SD}}{\lambda_{SD} + \sum_{j\in J} \lambda_{SDj} + \frac{\lambda_{SE}}{2^{2R_s}}} \\
&\quad + \sum_{n=1}^{N} \left[\sum_{i=0}^{N} (-1)^i \sum_{\substack{J\subseteq\{1,2,...N,N+1\}-\{n\} \\ |J|=i}} \left[\frac{\lambda_{Sn}}{\sum_{j\in J} \lambda_{SDj} + \lambda_{Sn} + \frac{\lambda_{SE}}{2^{2R_s}} + \lambda_{nD}}\right.\right. \\
&\quad \left.\left. + \frac{\lambda_{Sn}\lambda_{nD}}{\left(\lambda_{nD} + \frac{\lambda_{nE}}{2^{2R_s}}\right)\left(\sum_{j\in J} \lambda_{SDj} + \lambda_{Sn} + \lambda_{nD} + \frac{\lambda_{nE}}{2^{2R_s}}\right)}\right]\right.
\end{aligned}$$

[3]The results with a shared frequency resource (i.e., an identical γ_{SE}) are also simulated in the next section, which show a similar outage performance and a same diversity order as the orthogonal scenario.

$$
\begin{aligned}
&-\frac{\lambda_{Sn}\lambda_{nD}}{\left(\lambda_{nD}+\frac{\lambda_{nE}}{2^{2R_s}}\right)\left(\sum\limits_{j\in J}\lambda_{SDj}+\lambda_{Sn}+\frac{\lambda_{SE}}{2^{2R_s}}+\lambda_{nD}+\frac{\lambda_{nE}}{2^{2R_s}}\right)}\\
&+\frac{\lambda_{nD}}{\sum\limits_{j\in J}\lambda_{SDj}+\lambda_{Sn}+\lambda_{nD}+\frac{\lambda_{nE}}{2^{2R_s}}}\\
&+\frac{\lambda_{Sn}\lambda_{nD}}{\left(\lambda_{Sn}+\frac{\lambda_{SE}}{2^{2R_s}}\right)\left(\sum\limits_{j\in J}\lambda_{SDj}+\lambda_{Sn}+\frac{\lambda_{SE}}{2^{2R_s}}+\lambda_{nD}\right)}\\
&\left.-\frac{\lambda_{Sn}\lambda_{nD}}{\left(\lambda_{Sn}+\frac{\lambda_{SE}}{2^{2R_s}}\right)\left(\sum\limits_{j\in J}\lambda_{SDj}+\lambda_{Sn}+\frac{\lambda_{SE}}{2^{2R_s}}+\lambda_{nD}+\frac{\lambda_{nE}}{2^{2R_s}}\right)}\right]
\end{aligned}
\tag{3.6}
$$

where $\lambda_{SDj}=\lambda_{Sj}+\lambda_{jD},\forall j\in\{1,...,N\}$ and $\lambda_{SD(N+1)}=\lambda_{SD}$.

Similar to Case A, the exact CSI of the eavesdropping links is unavailable for Case B, but the statistical CSI regarding these links can be obtained, e.g., based on the location of the eavesdropper. The derived outage probability for Case B is similar to Eqn (3.6), in which we only need to replace λ_{ij} with $\sigma_{iE}^2\lambda_{ij}$. For Case C in which the instantaneous CSI can be estimated, the secrecy outage probability is derived as follows,

$$
\begin{aligned}
P_{out}^{C} &= \Pr\left(\frac{1}{2}\log_2(\frac{\gamma_{SD}}{\gamma_{SE}})<R_s,\frac{\gamma_{SD}}{\gamma_{SE}}\geq\min\left\{\frac{\gamma_{Sn^*}}{\gamma_{SE(n^*)}},\frac{\gamma_{n^*D}}{\gamma_{n^*E}}\right\}\right)\\
&\quad\Pr\left(\frac{1}{2}\log_2(\min\left\{\frac{\gamma_{Sn^*}}{\gamma_{SE(n^*)}},\frac{\gamma_{n^*D}}{\gamma_{n^*E}}\right\})<R_s,\ \frac{\gamma_{SD}}{\gamma_{SE}}<\min\left\{\frac{\gamma_{Sn^*}}{\gamma_{SE(n^*)}},\frac{\gamma_{n^*D}}{\gamma_{n^*E}}\right\}\right)\\
&= \Pr\left(\frac{1}{2}\log_2(\frac{\gamma_{SD}}{\gamma_{SE}})<R_s\right)\prod_{n=1}^{N}\Pr\left(\frac{1}{2}\log_2(\min\left\{\frac{\gamma_{Sn}}{\gamma_{SE(n)}},\frac{\gamma_{nD}}{\gamma_{nE}}\right\})<R_s\right)\\
&= \int_0^\infty\lambda_{SD}e^{-\lambda_{SD}x}e^{-\lambda_{SE}\frac{x}{2^{2R_s}}}dx\prod_{n=1}^{N}\left[1-\int_0^\infty\lambda_{Sn}e^{-\lambda_{Sn}x}\right.\\
&\quad\left.(1-e^{-\lambda_{SE}\frac{x}{2^{2R_s}}})dx\int_0^\infty\lambda_{nD}e^{-\lambda_{nD}y}(1-e^{-\lambda_{nE}\frac{y}{2^{2R_s}}})dy\right]\\
&= \frac{\lambda_{SD}}{\lambda_{SD}+\frac{\lambda_{SE}}{2^{2R_s}}}\prod_{n=1}^{N}\left[1-\frac{\frac{\lambda_{SE}}{2^{2R_s}}\frac{\lambda_{nE}}{2^{2R_s}}}{\left(\lambda_{Sn}+\frac{\lambda_{SE}}{2^{2R_s}}\right)\left(\lambda_{nD}+\frac{\lambda_{nE}}{2^{2R_s}}\right)}\right]
\end{aligned}
\tag{3.7}
$$

3.4.2 Diversity order analysis

It can be observed from Eqn (3.6) and Eqn (3.7) that the secrecy outage probability is independent of ρ in high SNR regime. The traditional definition of diversity order is not applicable. Therefore, a generalized definition of diversity order proposed in [45, 93] for wireless PLS is adopted:

$$d_{secrecy} = -\lim_{\delta_{de}\to\infty} \frac{\log(P_{out})}{\log(\delta_{de})} \tag{3.8}$$

where $\delta_{de} = \frac{\sigma_{SD}^2}{\sigma_{SE}^2}$ is the ratio of the average channel gain of the source-destination link to that of the source-eavesdropper link (which is also referred to be the main-to-eavesdropper ratio (MER) in [45]). This diversity order definition reflects the reduction rate of the secrecy outage probability as δ_{de} increases. We adopt $\sigma_{Sn}^2 = c_{Sn}\sigma_{SD}^2$, $\sigma_{nD}^2 = c_{nD}\sigma_{SD}^2$ and $\sigma_{nE}^2 = c_{nE}\sigma_{SE}^2$ to denote the average channel gains of the relaying links in the cooperative networks, where c_{Sn}, c_{nD} and c_{nE} are constant values.

Based on the fact that $e^x \geq 1+x$, the upper bound of P_{out}^A can be obtained as follows,

$$\begin{aligned}
P_{out}^{A-up} \;=\; & \int_0^\infty \prod_{n=1}^{N} \left[(\lambda_{Sn}+\lambda_{nD})x\right] \lambda_{SD} e^{-\lambda_{SD}x} e^{-\lambda_{SE}\frac{x}{2^{2R_s}}}\, dx \\
& + \sum_{n=1}^{N} \int_0^\infty \lambda_{SD} x \prod_{\substack{m=1 \\ m\neq n}}^{N} \left[(\lambda_{Sm}+\lambda_{mD})x\right] \\
& \Big[\Big(\lambda_{Sn} e^{-\lambda_{Sn}x} e^{-\lambda_{SE}\frac{x}{2^{2R_s}}} e^{-\lambda_{nD}x} \\
& + \lambda_{Sn} e^{-\lambda_{Sn}x} \int_x^\infty \lambda_{nD} e^{-\lambda_{nD}y} e^{-\lambda_{nE}\frac{y}{2^{2R_s}}}\, dy \\
& - \lambda_{Sn} e^{-\lambda_{Sn}x} e^{-\lambda_{SE}\frac{x}{2^{2R_s}}} \int_x^\infty \lambda_{nD} e^{-\lambda_{nD}y} e^{-\lambda_{nE}\frac{y}{2^{2R_s}}}\, dy\Big) \\
& + \Big(\lambda_{nD} e^{-\lambda_{nD}x} e^{-\lambda_{nE}\frac{x}{2^{2R_s}}} e^{-\lambda_{Sn}x} \\
& + \lambda_{nD} e^{-\lambda_{nD}x} \int_x^\infty \lambda_{Sn} e^{-\lambda_{Sn}y} e^{-\lambda_{SE}\frac{y}{2^{2R_s}}}\, dy \\
& - \lambda_{nD} e^{-\lambda_{nD}x} e^{-\lambda_{nE}\frac{x}{2^{2R_s}}}
\end{aligned}$$

$$\int_x^\infty \lambda_{Sn} e^{-\lambda_{Sn} y} e^{-\lambda_{SE} \frac{y}{2^{2R_s}}} dy \Bigg) \Bigg] dx \tag{3.9}$$

By using Eqn (3.326.2) of [94],

$$\int_0^\infty x^p \exp\left(-\beta x^q\right) dx = \frac{\Gamma(\psi)}{q\beta^\psi}, \psi = \frac{p+1}{q} \tag{3.10}$$

where Re$\beta > 0$, Re$p > 0$ and Re$q > 0$, we can derive $d_{secrery}^{A-up} = N+1$ (please see Appendix B.1 for details). Since there are only $N+1$ independent transmission links for one source and N cooperative relays, $d_{secrery}^{A-up} \leq d_{secrery}^{A} \leq N+1$. Therefore, $d_{secrery}^{A} = N+1$, which indicates that in Case A the full diversity is achieved. Similar to the derivation for Case A, it can be proved that Case B has the same diversity order $N+1$.

For Case C, the secrecy outage probability can be rewritten as

$$\begin{aligned}
P_{out}^{C} &= \frac{\lambda_{SD}}{\lambda_{SD} + a\lambda_{SE}} \prod_{n=1}^{N} \left[1 - \frac{a^2 \lambda_{SE} \lambda_{nE}}{\left(\lambda_{Sn} + a\lambda_{SE}\right)\left(\lambda_{nD} + a\lambda_{nE}\right)} \right] \\
&= \frac{\frac{1}{\sigma_{SD}^2}}{\frac{1}{\sigma_{SD}^2} + \frac{a}{\sigma_{SE}^2}} \prod_{n=1}^{N} \left[\frac{\frac{1}{c_{Sn} c_{nD} \sigma_{SD}^4} + \left(\frac{1}{c_{nD}} + \frac{1}{c_{Sn} c_{nE}}\right) \frac{a}{\sigma_{SD}^2 \sigma_{SE}^2}}{\left(\frac{1}{c_{Sn}\sigma_{SD}^2} + \frac{a}{\sigma_{SE}^2}\right)\left(\frac{1}{c_{nD}\sigma_{SD}^2} + \frac{a}{c_{nE}\sigma_{SE}^2}\right)} \right] \\
&= \frac{1}{\delta_{de}} \frac{1}{\delta_{de}^{-1} + a} \prod_{n=1}^{N} \left[\frac{1}{\delta_{de}} \frac{\frac{\delta_{de}^{-1}}{c_{Sn} c_{nD}} + a\left(\frac{1}{c_{nD}} + \frac{1}{c_{Sn} c_{nE}}\right)}{\left(\frac{\delta_{de}^{-1}}{c_{Sn}} + a\right)\left(\frac{\delta_{de}^{-1}}{c_{nD}} + \frac{a}{c_{nE}}\right)} \right] \\
&= \left(\frac{1}{\delta_{de}}\right)^{N+1} \frac{1}{\delta_{de}^{-1} + a} \prod_{n=1}^{N} \left[\frac{\frac{\delta_{de}^{-1}}{c_{Sn} c_{nD}} + a\left(\frac{1}{c_{nD}} + \frac{1}{c_{Sn} c_{nE}}\right)}{\left(\frac{\delta_{de}^{-1}}{c_{Sn}} + a\right)\left(\frac{\delta_{de}^{-1}}{c_{nD}} + \frac{a}{c_{nE}}\right)} \right]
\end{aligned} \tag{3.11}$$

where, $a = \frac{1}{2^{2R_s}}$. It is easy to obtain that $d_{secrery}^{C} = -\lim_{\delta_{de} \to \infty} \frac{\log(P_{out}^{C})}{\log(\delta_{de})} = N+1$. The full diversity is also achieved in the Case C.

3.5 Numerical Results and Discussions

Numerical results are presented in this section to validate the secrecy performance of the proposed OUCS. It is shown that the OUCS achieves a better performance than the existing alternatives in terms of secrecy outage proba-

bility, and the full diversity is also confirmed. Without loss of generality, the parameter c_{Sn} for the simulation is generated randomly from [10,100], while c_{nD} and c_{nE} are generated randomly from [5,25]. The target secrecy rate is set to be $R_s = 0.5$bits/s/Hz.

In Fig 3.2, the secrecy outage probabilities of the direct transmission, conventional cooperation and OUCS are illustrated, given that only one cooperative user is specified to provide the cooperation. It is observed that the OUCS always performs better than the conventional cooperation, especially when the CSI of the eavesdropping links can be obtained (Case C). That is because the OUCS utilizes the cooperation opportunistically according to the time-varing channel qualities. Furthermore, the diversity order of the OUCS is shown to be 2, while the direct transmission and the conventional cooperation only have diversity order 1. Although the OUCS may be slightly worsen than the direct transmission in low MER (δ_{de}) region, it does much better as MER increases.

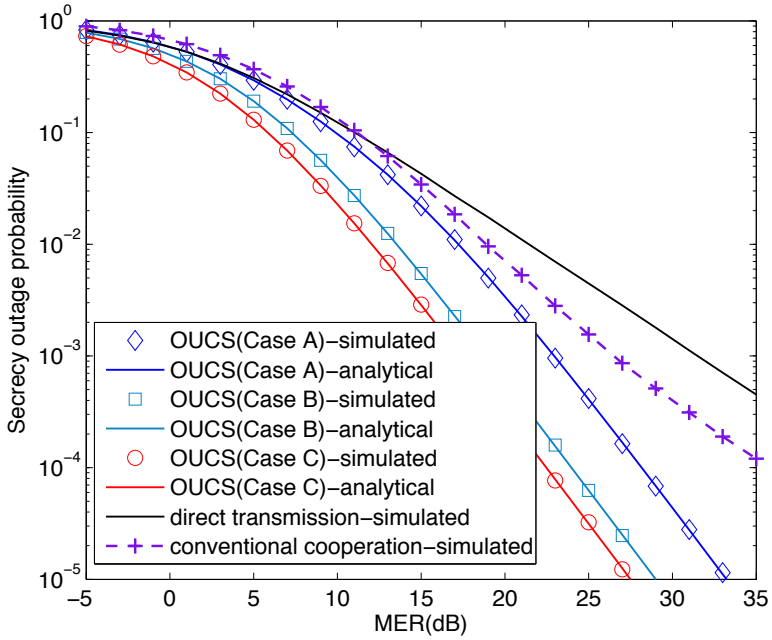

Figure 3.2: Secrecy outage probability vs. MER for the direct transmission, conventional cooperation and OUCS with one cooperative relay.

Fig 3.3 shows the comparison of secrecy outage performance between the proposed OUSC and alternatives in [45] and [47, 48] (with N=2 cooperative

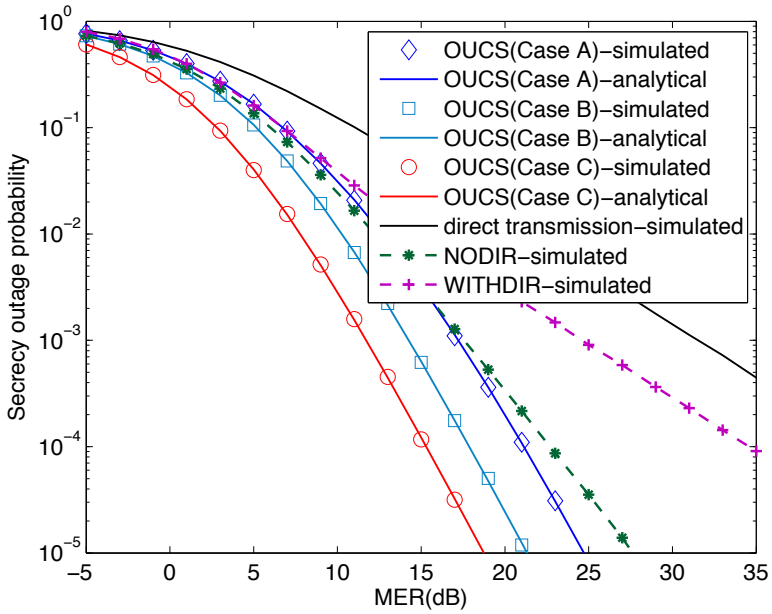

Figure 3.3: Secrecy outage probability vs. MER for the OUCS and alternative cooperation schemes with optimal relay selection.

users). All of the schemes select the "best" relay to assist the secure transmission. In our OUCS, the relay selection is based on $n^* = \underset{n\in\{1,2,\ldots,N\}}{\arg\max}\ \{\mathrm{SPC}_n\}$ and the cooperation occurs opportunistically by comparing SPC_{n^*} and SPC_S. In [45], the direct links are not considered such that the optimal relay selection scheme ("NODIR") is $n^* = \underset{n\in\{1,2,\ldots,N\}}{\arg\max}\left\{\frac{1+\min\{\gamma_{Sn},\gamma_{nD}\}}{1+\gamma_{nE}}\right\}$. Since the NODIR simply neglects the direct links even if they exist, its diversity order cannot exceed the number of the cooperative relays, i.e., N (The same problem is found in [44, 46, 49][4], where the diversity order is also N). The direct links are taken into account in [47, 48], and their relay selection scheme can be written as $n^* = \underset{n\in\{1,2,\ldots,N\}}{\arg\max}\left\{\frac{1+\gamma_{SD}+\gamma_{nD}}{1+\gamma_{SE}+\gamma_{nE}}\right\}$ (denoted by "WITHDIR"). However, the conventional cooperation is performed blindly therein and the source-relay links are not involved in this relay selection scheme. Both the NODIR and WITHDIR assume that the instantaneous CSI of the eavesdropping links are available, which is same as the Case C in this chapter.

It is shown from Fig 3.3 that the diversity order of NODIR is N (i.e., 2)

[4]In [49], only the eavesdropper exploits the direct link.

as concluded in [45]. The diversity order of WITHDIR is still 1, because this scheme does not take into account the channel capacities of the source-relay links. However, the OUCS in this paper can achieve the full diversity (diversity order $N+1$). Moreover, It is found from Fig 3.2 and Fig 3.3 that the simulated results are consistent with the analytical curves.

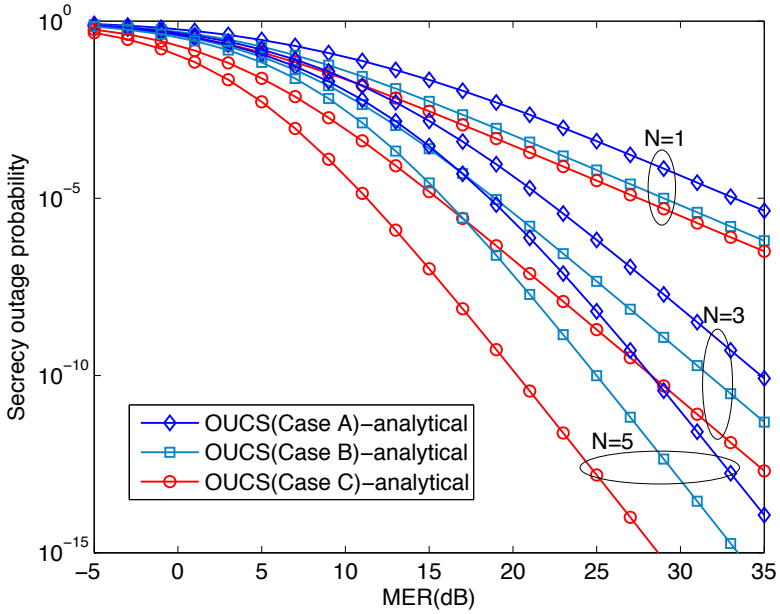

Figure 3.4: Secrecy outage probability vs. MER for the OUCS with different numbers of cooperative relays.

Fig 3.4 plots the secrecy outage probabilities of the OUCS for N=1,3,5 cooperative relays. Exploiting more cooperative relays can achieve a much lower secrecy outage probability. Meanwhile, as N increases the secrecy outage probability reduces to zero much faster for MER$\rightarrow\infty$. The diversity order of the OUCS is also observed to be N+1. In Fig 3.5, the OUCS with a shared frequency resource in the cooperative network is simulated. The simulation results are approximate to the analytical values derived in this paper for orthogonal frequency resource allocation, and more importantly the full diversity performance is still ensured. That's to say, the conclusions obtained above are also applicable to this scenario.

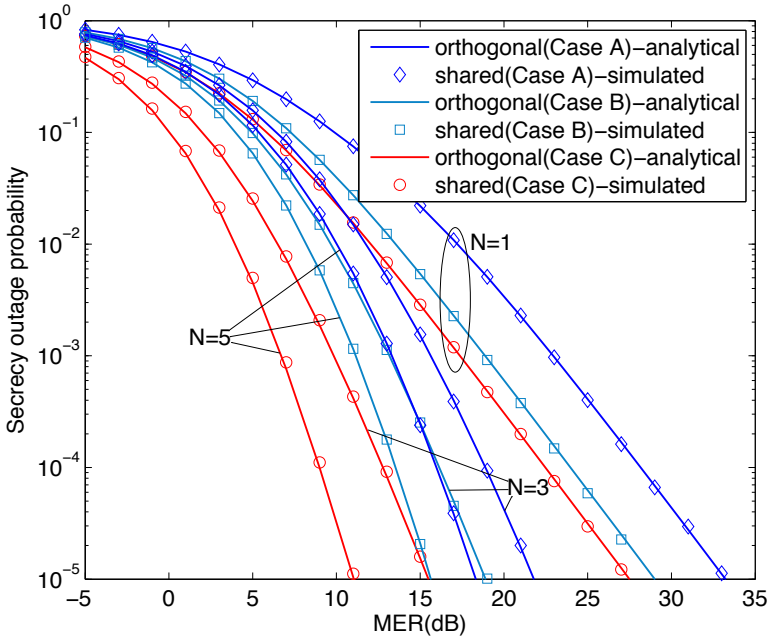

Figure 3.5: Secrecy outage probability vs. MER for the OUCS with orthogonal or shared frequency resource allocation.

3.6 Another Form of Multi-User OUCS

There is another typical multi-user cooperative relay networks: multiple sources share a dedicated cooperative relay to communicate with the destination. In this case, the multiuser diversity (MUD) instead of optimal relay selection should be adopted (in fact, the principle of them is almost the same). For every time slot the source with best channel condition is scheduled to access the channel and transmit its data, which is named as MUD. There have been some literatures studying the application of MUD in cooperative relay networks, such as [95–98]. Due to the similar principle between the MUD and optimal relay selection, our proposed OUCS can be also modified with MUD to enhance the PLS.

The system model considered here is as shown in Fig 3.6, where system parameters are assumed to be the same as those in Fig 3.1. We modify the OUCS as follows: the optimal source is first selected by $k^* = \underset{k\in\{1,2,\ldots,K\}}{\arg\max}\ \{\mathrm{SPC}_k\}$. Then similar to Sect 3.3 if $\mathrm{SPC}_{k^*} \geq \mathrm{SPC}_R$, the selected source transmits its

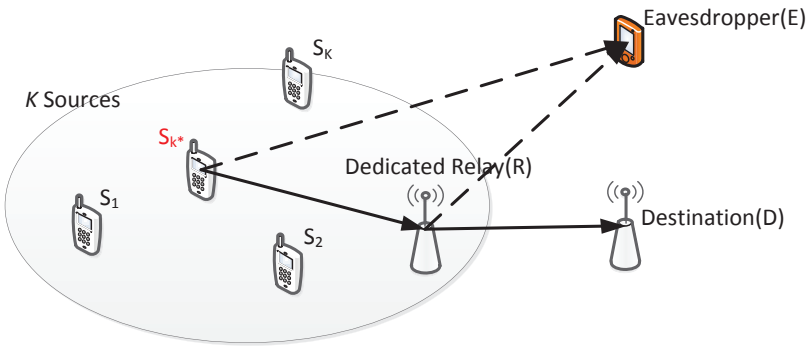

Figure 3.6: Multi-source cooperative networks under eavesdropping attack.

message directly to the destination in Phase I and the relay keeps silent in Phase II; otherwise, the cooperation mode is conducted that the selected source transmits its message to the relay in Phase I and the relay forwards it by RF protocol in Phase II. The eavesdropper also attempts to obtain the information in both phases.

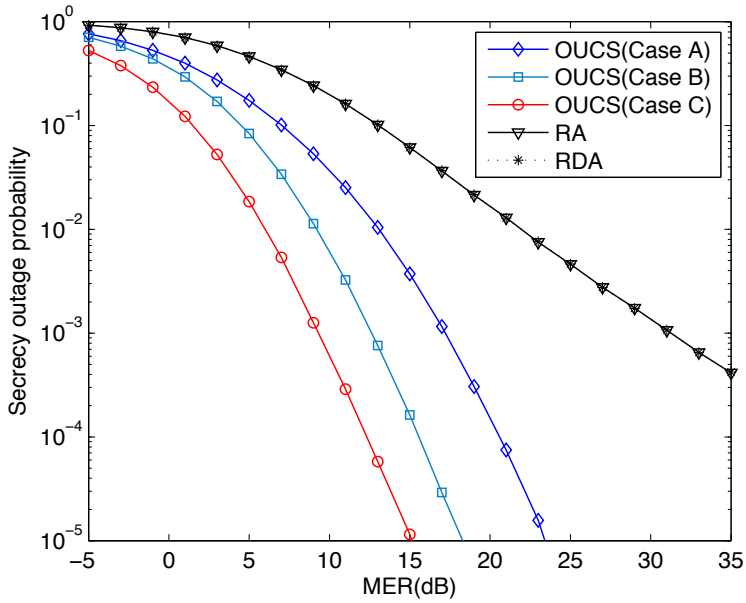

Figure 3.7: Secrecy outage probability vs. MER for the OUCS and the conventional cooperation with RA and RDA.

Fig 3.7 shows the secrecy outage performance of the OUCS and the conventional cooperation (K=3). For the conventional cooperation, the random access (RA) and round-robin access (RDA) are presented. It can be observed

that the OUCS surpasses the conventional cooperation with both RA and RDA significantly. That is because every time it is the source with the "best" secrecy-providing transmission link that accesses the channel and accordingly optimal secrecy performance is provided, while the conventional cooperation cannot get any benefits from the multiuser diversity gain. Moveover, it is shown that the OUCS realizes full diversity performance (diversity order $K + 1 = 4$) while the conventional cooperation only have diversity order 1.

3.7 Summary

In this chapter, the opportunistic user cooperation scheme (OUCS) is extended to multi-user cooperative relay networks for achieving full secrecy diversity performance. Considering the eavesdropping attack, a performance index called secrecy-providing capability (SPC) is first introduced for both the source and the cooperative relays. The OUCS jointly solves the problems of whether and with whom to cooperate based on the values of SPC. Then, the closed form expressions for the secrecy outage probability of the OUCS are derived, from which the full diversity performance is confirmed. The numerical results are also given to verify the theoretical analysis and validate the superiority of the OUCS over the existing alternatives. In addition, another typical form of multi-user cooperative relay networks, where a dedicated relay services multiple sources, is also analyzed to confirm the effectiveness of the OUCS in enhancing the physical layer security.

Chapter 4

Secure Transmission through Cooperative Relaying in Wireless Body Area Networks

We make our effort in this chapter on the application of cooperative security to a kind of specific sensor networks - wireless body area networks (WBANs). The channel attenuation (/path loss) is proved to be severe in WBANs by the literature, which makes relaying become a general strategy to improve the data transmission reliability and energy efficiency of WBANs. Unlike these works, the relaying on the enhancement of physical layer security for WBANs is studied by us. Specifically, the secrecy outage performance for direct transmission and cooperative multihop relaying is derived based on the channel characteristics of WBANs. The results illustrate that cooperative multihop relaying performs much better than direct transmission in terms of secrecy outage probability.

4.1 Introduction

The wireless body area networks (WBANs) generally mean the wireless networks of wearable sensor devices for monitoring the physiological data of human bodies [51], which have been considered for a variety of application scenarios, e.g., consumer electronics, healthcare and athletic training. The

monitoring data generated by sensor nodes in WBANs are transmitted to the gateway node via a wireless link. Compared with its wired counterparts, WBANs are more flexible and comfortable for practical use.

However, the on-body channels in WBANs are affected a lot by the human body. The received power is reduced quickly as the link distance increases. Based on the experiment measurements of [50], the path loss can be still modeled by Friis formula [99] but with a larger path loss coefficient than that in free space. Therefore, it is preferable to adopt short-distance multihop relaying in WBANs [51], since the sever path loss makes that the channel gain for each short-distance hop is much higher than that for the direct/single-hop transmission. The research works [50–58] have illustrated the effectiveness of relaying (/cooperative relaying) to reduce the energy consumption or improve the reliability of WBANs.

Similar to other wireless networks, the openness of the wireless medium makes the monitoring data to be overheard easily. Besides the cryptography, the physical layer security (PLS) may be an alternative secure data transmission method for the resource and size limited nodes in WBANs. The PLS simply exploits the wireless channel fading to achieve perfect secrecy [29]. As described in the above chapters, the secrecy capacity, defined as the difference between the channel capacities of the legitimate (main) link and the eavesdropping link, indicates the maximum data rate at which the eavesdropper cannot decode any information. Considering that the channel fading is random, the probability of secrecy outage (the instantaneous secrecy capacity is lower than a target secrecy rate) is usually adopted to evaluate the secrecy performance. Because the cooperative multihop relaying can improve the channel gain (i.e., channel capacity) of the legitimate links in WBANs, we thus think it should be also positive for the improvement of the secrecy performance.

Although the PLS has been studied extensively, to the best of our knowledge, we are the first to study the secrecy performance improvement for WBANs from the PLS perspective. The contribution of this chapter is: The application of cooperative security in WBANs is analyzed. Specifically, we derive and compare the secrecy outage performance for both the single-hop and coopera-

tive multihop transmission based on the channel characteristics of WBANs. It is observed from the results that the multihop relaying is not only beneficial for the reliability and energy efficiency as shown in the literature, but also an effective strategy to enhance the PLS of WBANs given the severe path loss of radio signals through the human body [50, 51].

4.2 System Model

The considered system model is shown in Fig 4.1, where a WBAN is implemented on a human body and an eavesdropper attempts to intercept the monitoring data. The sensor nodes transmit their data to the gateway node by using the time division multiple access to realize orthogonal channel sharing. The main channel between the sensor and the gateway nodes is regarded as the on-body channel, whereas the wiretap channel is the off-body channel. Based on the existing research, the on-body channel can be modeled as a log-normal fading channel [50, 51]. Therefore, the received signal to noise ratio (SNR) γ_M for the main channel follows log-normal distribution, and its probability density function is

$$f(\gamma_M) = \frac{1}{\sqrt{2\pi}\sigma_M\gamma_M} \exp\left(-\frac{\left(10\log_{10}\gamma_M - \mu_M\right)^2}{2\sigma_M^2}\right) \tag{4.1}$$

with μ_M [dB] and σ_M [dB] denoting the mean value and standard deviation of the received SNR respectively. The off-body channel can be regarded as the Rayleigh fading [100], and thus the received SNR γ_W for the wiretap channel follows the exponential distribution of parameter λ_W,

$$f(\gamma_W) = \lambda_W \exp\left(-\lambda_W\gamma_W\right) \tag{4.2}$$

The path loss is assumed to follow friis formula [50,51]. Thus we can obtain that

$$\mathrm{E}[\gamma_-^{dB}](d) = \mathrm{E}[\gamma_-^{dB}](d_0) - 10n\log_{10}\frac{d}{d_0} \tag{4.3}$$

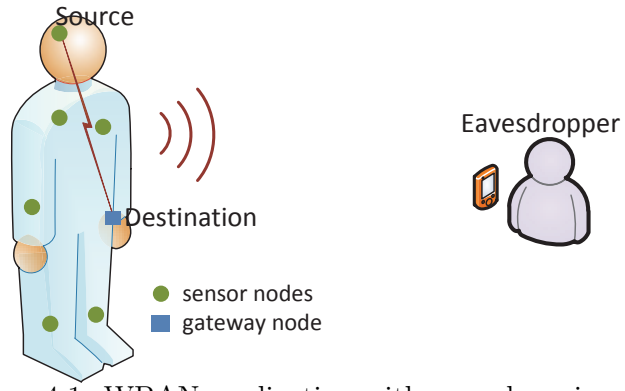

Figure 4.1: WBAN application with eavesdropping attack.

where $\mathrm{E}[\gamma_{-}^{dB}](d)$ denotes the mean value [dB] of the received SNR at a distance d and n is the path loss exponent. For the on-body channel, the path loss exponent is generally larger than 2 due to the severe shadowing in WBANs (In [50], it is assumed that $n = 3.11$ for the line of sight channel and $n = 5.9$ for the non-line of sight channel). It has been proved that the cooperative relaying is effective in resisting channel fading and improving energy efficiency in [50–58]. Here, we will further show the superiority of cooperative relaying from the PLS perspective in WBANs.

4.3 Secrecy Outage Analysis for Direct and Relaying Transmission

The secrecy capacity of the system is described as follows according to its definition,

$$\begin{aligned} C_S &= [C_M - C_W]^+ \\ &= [\log_2(1+\gamma_M) - \log_2(1+\gamma_W)]^+ \end{aligned} \tag{4.4}$$

and for a target secrecy rate R_S the outage probability is calculated by $P_{out} = \Pr\{C_S < R_S\}$. Since the cumulative distribution function of the log-normal distribution is $F(x;\mu,\sigma) = Q\left(\frac{\mu - 10\log_{10}x}{\sigma}\right)$ by using Q-function, the secrecy

outage probability for the direct/single-hop transmission is

$$\begin{aligned} P_{out}^{S-hop} &= \Pr\left\{[\log_2(1+\gamma_M) - \log_2(1+\gamma_W)]^+ < R_s\right\} \\ &= \int_0^\infty Q\left(\frac{\mu_M - 10\log_{10}(\gamma_W 2^{Rs} + th)}{\sigma_M}\right)\lambda_W e^{-\lambda_W \gamma_W} d\gamma_W \end{aligned} \quad (4.5)$$

with $th = 2^{Rs} - 1$[1]. For cooperative multihop relaying, we still adopt the relaying protocol of the opportunistic user cooperation scheme (i.e., OUCS) in the Chapter 2 and 3, but neglect the direct link here due to the severe path loss. That is, the relays adopt different codebooks to avoid the diversity combining at the eavesdropper [84]. Thus, the secrecy outage occurs no matter which hop suffers from outage. We can then obtain the secrecy outage probability for M-hop cooperative relaying,

$$\begin{aligned} P_{out}^{M-hop} &= 1 - \prod_{i=1}^{M}(1 - P_{out,i}^{S-hop}) \\ &= 1 - \prod_{i=1}^{M}\left[1 - \int_0^\infty Q\left(\frac{\mu_{M,i} - 10\log_{10}(\gamma_{W,i} 2^{Rs} + th)}{\sigma_{M,i}}\right)\right. \\ &\qquad \left.\lambda_{W,i} e^{-\lambda_{W,i}\gamma_{W,i}} d\gamma_{W,i}\right] \end{aligned} \quad (4.6)$$

where i indicates the ith hop. Based on the Eqn (4.3), the mean received SNR $\mu_{M,i}$ becomes much larger than μ_M with the hop distance decreasing. If the distance for the ith hop is $1/p$ $(p \geq 1)$ of the distance for the single-hop, $\mu_{M,i} = \mu_M + 10n\log_{10}p$. Therefore, the secrecy outage probability for each hop in multihop will be significantly smaller than that of the single-hop transmission, given that these hop distances are much shorter[2]. Accordingly, P_{out}^{M-hop} becomes much lower than P_{out}^{S-hop}, as confirmed by simulations in the next section.

[1]The approximate result of (4.5) can be obtained numerically by $e^{-\lambda_W \alpha} + \int_0^\alpha Q\left(\frac{\mu_M - 10\log_{10}(\gamma_W 2^{Rs} + th)}{\sigma_M}\right)\lambda_W e^{-\lambda_W \gamma_W} d\gamma_W$.

[2]Wiretap channels for each hop are assumed to follow identical distribution because of the relatively long distance between the WBAN and the eavesdropper, i.e., $\lambda_{W,i} = \lambda_W, \forall i$.

4.4 Numerical Results and Discussions

The secrecy outage probability is compared between the direct/single-hop transmission and cooperative multihop relaying under different parameter settings. The transmit power at the nodes is fixed to make the single-hop transmission achieve a reliability of 99% for an received SNR threshold of 0dB, $\sigma_{M(,i)} = 5$dB and the target secrecy rate is set to $R_S = 0.5$bits/s/Hz. The cooperative relays are initially positioned to divide the distance between the sensor node and the gateway node equally.

In Fig 4.2, the secrecy outage probability for the single-hop, two-hop and three-hop transmission is presented for different MER= $\mathrm{E}[\gamma_M]/\mathrm{E}[\gamma_W]$ values (In practical systems, MER is usually much larger than 0dB since the WBAN is a short range wireless network and the eavesdropper may not be able to come very close to the target WBAN). The simulated results are consistent with the analytical curves, and it is also observed that the multihop achieves a much better secrecy outage performance than the single-hop. As the number of the hop and the path loss exponent increase, the multihop becomes more effective.

Fig 4.3 shows the effect of the cooperative relay's location for the two-hop transmission (MER= 10dB) by assuming that it is difficult to set more relays. The midpoint turns out to be optimal as expected. Furthermore, we consider more freedom of the cooperative relay's location and illustrate the secrecy performance in Fig 4.4 for n=3.11, which confirms again that a better secrecy performance is achieved as the cooperative relay approaches the midpoint. This result provides a reference for how to decide an optimal cooperative relay, and also benefits the practical relay positioning if the dedicated relay is employed.

4.5 Summary

The application of cooperative security in wireless body area networks is analyzed in this chapter. Due to the severe path loss caused by the human body, reducing the transmission distance can improve the channel capacity sig-

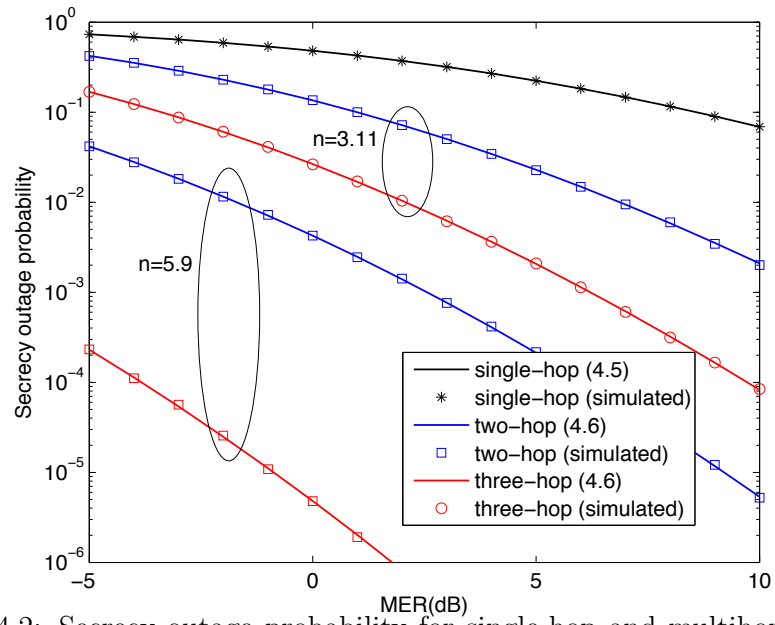

Figure 4.2: Secrecy outage probability for single-hop and multihop transmission.

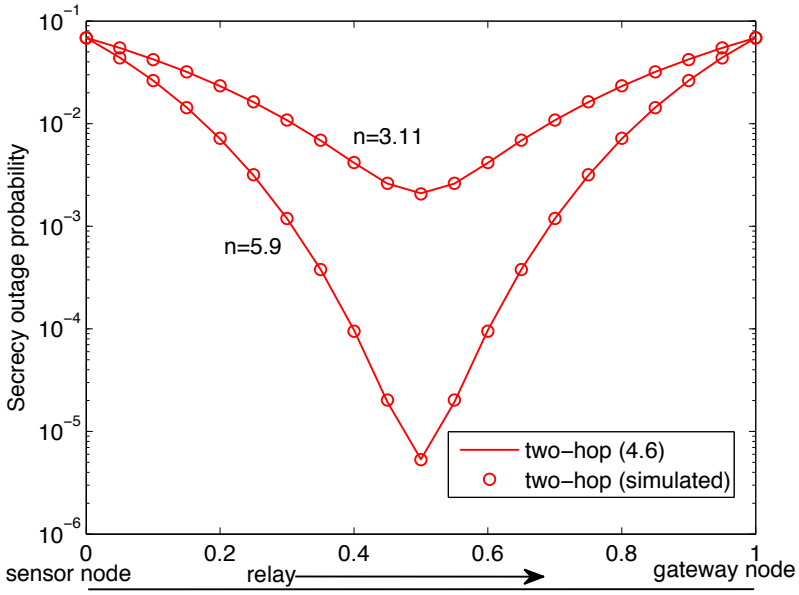

Figure 4.3: The effect of the relay's location for the two-hop transmission.

nificantly. This characteristic motivates us to introduce the cooperative multihop relaying to improve the channel capacities of the legitimate links and thus enhance the physical layer security. Through the theoretical analysis and nu-

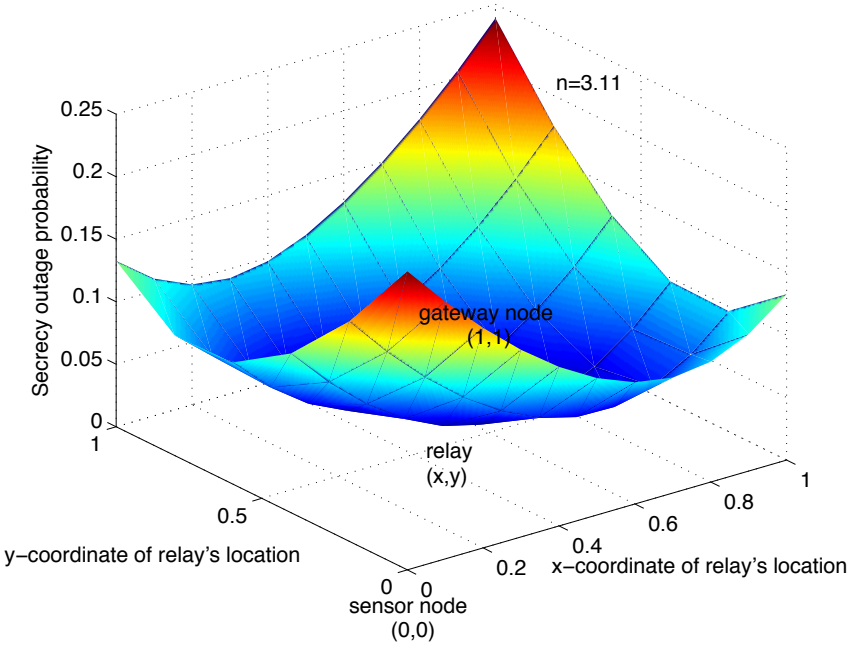

Figure 4.4: The effect of the relay's location (with more freedom) for the two-hop transmission.

merical results, the cooperative security is proved to be a feasible strategy to enhance the transmission security in WBANs.

Chapter 5

Fountain Code Assisted Security for Internal Eavesdropping in CRNs with an Untrusted Relay

The external eavesdropping attack is considered in the above chapters. However, the cooperative relay networks may also suffer from internal eavesdropping if the cooperative relays are untrusted. In this chapter, a secure transmission scheme named *fountain code assisted security (FCAS)* is designed and then utilized to protect from the internal eavesdropping.

FCAS is based on the characteristics that, in fountain coded transmission systems, the receivers need a sufficient number of fountain packets to recover the original data. Secure transmission can be achieved if the legitimate user receives enough fountain packets before the eavesdropper. For this purpose, we utilize the independent channel fading of different users to ensure a higher packet reception rate at the destination. The channel fading is competent if the destination is known to have a better average channel condition than that of the eavesdropper; otherwise, transmit power control (TPC) relative to the destination channel is employed. Numerical results show that the intercept probability is reduced to zero (near-)exponentially as the number of source packets increases. Moreover, due to the ordinary fountain coded transmission, the achievable data rate of the delivery depends only on the source-destination

channel capacity rather than the system secrecy capacity.

When we treat the untrusted cooperative relays as the eavesdroppers, the secure transmission is realized if the destination receives fountain packets faster than these relays. The adoption of FCAS with & without TPC is analyzed for both the decode-and-forward and amplify-and-forward relaying with an untrusted relay. It is observed that FCAS is also powerful to protect from the internal eavesdropping, and its superiority is confirmed again that the intercept probability can be reduced to zero (near-)exponentially by increasing the number of source packets.

5.1 Introduction

The secrecy capacity in physical layer security (PLS) dictates the maximum data rate at which perfect secrecy of the transmitted messages can be ensured (the eavesdropper cannot decode any information correctly) [29]. In practice, such protection mechanism is not always necessary, if we *assume* that the transmitted packets of the confidential data are related and a certain number of packets are required for data recovery.

Fountain codes are introduced by us to satisfy this *assumption*. These fountain codes, such as LT (Luby Transform) codes and Raptor codes, are first proposed to deliver files in a reliable and efficient manner without retransmission. Using a fountain encoder, an infinite number of packet streams can be generated, and each encoded fountain packet is the bitwise sum of distinct source packets chosen randomly [101]. As described in [101], the original data file can be recovered from any set of N encoded fountain packets by assuming that the source file comprises K packets and N is slightly larger than K. This underlying characteristic provides a novel insight into secure delivery: the security is achieved if the intended user can receive enough fountain packets before the eavesdropper does. In this chapter, the independence of channel fading across different users is utilized to ensure that the packet reception rate at the destination is higher than that at the eavesdropper. Specifically, if the average channel quality of the source-destination link is known to be better than that of

the source-eavesdropper link, we prove that channel fading itself is competent and security can be achieved without any additional operations. Otherwise, a transmit power control (TPC) strategy is adopted. In this manner, the destination can maintain the received signal-to-noise ratio (SNR) above the desired level for correct channel decoding, whereas the eavesdropper suffers from outage with a certain probability because of independent channel fading.

If the eavesdropper also obtains a sufficient number of fountain packets when the destination can perform the fountain decoding, the confidential data are intercepted. The results show that the intercept probability of the proposed scheme decreases (near-)exponentially with increasing value of K. This study does not need to address the perfect secrecy of data streams in physical layer. Confidential data are delivered through ordinary fountain coded transmission, and correct decoding of some fountain packets at the eavesdropper is allowed as long as the intended user finishes the fountain decoding first. Therefore, the achievable data rate of the delivery is only bounded by the channel capacity of the source-destination link.

The designed fountain code assisted security (FCAS) presents a new security perspective on the research area of PLS. In this chapter, we further extend FCAS to cooperative networks for resisting an untrusted relay. Till now, the cooperative networks with an untrusted relay have been studied widely from the perspective of PLS [59–63], but all aim at improving the secrecy capacity or reducing the secrecy outage probability. Based on the concept of FCAS, however, the secure transmission can be realized if the destination can receive fountain packets faster than the untrusted relay. The utilization of FCAS with & without TPC to resist the untrusted relay is studied for both the decode-and-forward (DF) and amplify-and-forward (AF) relaying protocols. The theoretical results of the intercept probability are derived, which are further validated by the numerical simulations. The advantages of FCAS are observed to be inherited, especially that the intercept probability is reduced (near-)exponentially as the value of K increases.

5.2 Fountain Code Assisted Security (FCAS)

5.2.1 System model

Fig 5.1 presents a three-node wireless system that consists of one source (S), one destination (D), and one eavesdropper (E). The source wants to deliver a confidential data file to the destination and the eavesdropper tries to overhear the message. The file is relatively large and is divided into long message packets (K packets). These packets are delivered by the source using fountain codes at the application layer. Both the destination and the eavesdropper will attempt to obtain a sufficient number of fountain packets to recover the original file, and it is assumed that no usable information is leaked prior to the completion of fountain decoding. When enough fountain packets have been correctly decoded, the destination sends a feedback to the source to terminate the transmission. Secure delivery is achieved if the eavesdropper has not received enough fountain packets at this time.

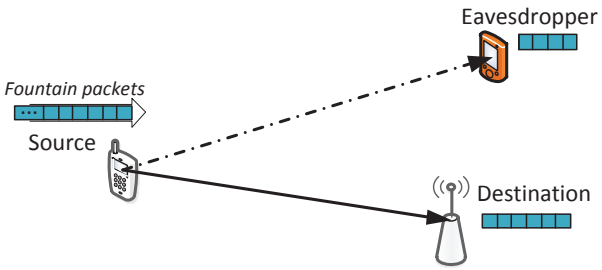

Figure 5.1: Secure wireless transmission by using fountain codes.

The wireless channels are modeled as the Rayleigh block flat fading, i.e., channel coefficients are constant during the time slot of one packet and change independently across different time slots. The channel coefficient h_{ij} between nodes i and j is a circularly symmetric complex Gaussian random variable with zero mean and variance $\sigma_{ij}^2 = d_{ij}^{-\beta}$, where d_{ij} is the distance between nodes i and j, and β is the path loss exponent. Additive white Gaussian noise w is assumed at the receiver with variance N_0. If the source sends the packets with power P, the received SNR at receiver j can be represented as $\gamma_{Sj} = \rho|h_{Sj}|^2$, where $\rho = P/N_0$ denotes system SNR.

The source continually sends the encoded fountain packets ($f[1], f[2], f[3]$, ...) generated by the K original packets ($p[1], p[2], ..., p[K]$) until the destination can decode the file correctly. After the cyclic redundancy check (CRC) encoding at the data link layer and the channel encoding at the physical layer are performed, the encoded fountain packets become ($x[1], x[2], x[3], ...$), which are sent over the wireless channel. In time slot n, the received signal at node j can be written as $y_j[n] = x[n]h_{Sj}[n] + w_j[n]$, $j \in \{D, E\}$. The target transmission rate is R bits/s/Hz, and capacity-achieving channel code is adopted for theoretical analysis. If $\log(1+\gamma_{Sj}[n]) \geq R$, the received packet can be decoded reliably and kept for fountain decoding; otherwise, this packet is discarded [102, 103]. If any $N = \lceil (1+\delta)K \rceil$ encoded fountain packets are received correctly, Bob can recover the original file, and so can Eve. Here δ represents the decoding overhead of fountain codes [101] and $\lceil \cdot \rceil$ denotes the ceiling function.

5.2.2 Scheme descriptions and performance analysis

This section introduces the physical layer strategies based on the independent channel fading of different users to ensure a higher packet reception rate at the destination. Two different scenarios are considered, and some application issues are presented.

A. The destination has a better average channel condition than the eavesdropper (*S1*)

S1 corresponds to the scenario where the distance between the source and the eavesdropper is larger than that between the source and the destination, due to the geographical restraints or physical inspection. For example, the source wants to deliver the files to the destination in one room, whereas the eavesdropper is not allowed to enter. For this scenario, the destination has a better expected value of the received SNR. The channel fading is competent to secure the transmission, which is denoted as CF strategy for future reference.

Based on the system model, the receiver is considered to obtain the fountain packet reliably in time slot n if $\log(1+\gamma_{Sj}[n]) \geq R$. The outage probabil-

ities at Bob and Eve are expressed respectively by

$$\varepsilon_{SD} = \Pr\left\{\log_2(1+\gamma_{SD}[n]) < R\right\} = 1 - e^{-\lambda_{SD}\zeta/\rho} \tag{5.1}$$

$$\varepsilon_{SE} = \Pr\left\{\log_2(1+\gamma_{SE}[n]) < R\right\} = 1 - e^{-\lambda_{SE}\zeta/\rho} \tag{5.2}$$

where $\lambda_{ij} = \left(\sigma_{ij}^2\right)^{-1}$ and $\zeta = 2^R - 1$. The required number of time slots for the destination to recover the file, L_{SD}, meets the negative binomial distribution $\mathcal{NB}(N, 1-\varepsilon_{SD})$. Its probability mass function (PMF) and cumulative distribution function (CDF) can be respectively given by

$$\begin{aligned} f_{L_{SD}}(l) &= \Pr\left\{L_{SD} = l\right\} \\ &= \begin{pmatrix} l-1 \\ N-1 \end{pmatrix} (1-\varepsilon_{SD})^N {\varepsilon_{SD}}^{l-N}, l \geq N \end{aligned} \tag{5.3}$$

$$\begin{aligned} F_{L_{SD}}(l) = &\Pr\left\{L_{SD} \leq l\right\} \\ = &\sum\nolimits_{x=N}^{l} \begin{pmatrix} x-1 \\ N-1 \end{pmatrix} (1-\varepsilon_{SD})^N {\varepsilon_{SD}}^{x-N}, l \geq N \end{aligned} \tag{5.4}$$

The PMF and the CDF of L_{SE} (i.e., the required number of time slots for the eavesdropper) have the same forms as Eqn (5.3) and (5.4), with ε_{SD} replaced by ε_{SE}. According to the mean value of the negative binomial distribution, the expected values of the recovery time at the destination and the eavesdropper are given as follows,

$$E(L_{SD}) = N + \frac{N\varepsilon_{SD}}{1-\varepsilon_{SD}} = \frac{N}{1-\varepsilon_{SD}} \tag{5.5}$$

$$E(L_{SE}) = N + \frac{N\varepsilon_{SE}}{1-\varepsilon_{SE}} = \frac{N}{1-\varepsilon_{SE}} \tag{5.6}$$

Because $d_{SE} > d_{SD}$, it turns out that $\varepsilon_{SE} > \varepsilon_{SD}$, and hence, $E(L_{SD}) < E(L_{SE})$. The expected time slots for the destination to obtain enough fountain

packets is less than that for the eavesdropper. However, the interception is inevitable due to the randomness of the channel fading. The eavesdropper intercepts the original file if it decodes N fountain packets first or simultaneously. The exact intercept probability can be derived as

$$\varepsilon^{CF} = \sum\nolimits_{l=N}^{\infty} f_{L_{SD}}(l) F_{L_{SE}}(l) \tag{5.7}$$

As shown by the simulation results in Section 5.2.3, the intercept probability decreases near-exponentially as K increases. If K is sufficiently large, the delivery can be conducted with a negligible probability of information leakage.
B. The CSI pertaining to the source-eavesdropper link is unavailable or the eavesdropper has a better average channel condition (*S2*)

Channel fading is unable to guarantee security for *S2*, and an additional physical layer strategy is required. We introduce the TPC technique to ensure the higher packet reception rate at the destination. Specifically, transmit power is adjusted based on the channel estimation of the source-destination link. If the channel gain of the source-destination link is lower than a threshold, the transmission is postponed at this time slot. Otherwise, the transmission is performed with a constant received SNR at the destination (i.e., with a constant data rate) through the power control[1]. This strategy is also regarded as truncated channel inversion [4]. According to [4], if P denotes the average transmit power, the control strategy is expressed as

$$P'(\gamma_{SD}) = \begin{cases} P\frac{\gamma^c}{\gamma_{SD}}, & \gamma_{SD} \geq \gamma_0, \\ 0, & \gamma_{SD} < \gamma_0, \end{cases} \tag{5.8}$$

where $P'(\gamma_{SD})$, γ^c and γ_0 represent the transmit power for different γ_{SD}, the constant received SNR and the cutoff fade depth respectively. It is derived from

[1]Channel estimation errors may occur in practical systems. Thus redundant transmit power is needed, which deteriorates the secrecy performance to a certain degree but does not affect the performance improvement with increasing K values. In this chapter, we consider the perfect CSI estimation for a simplified theoretical analysis.

the average power constraint that

$$\gamma^c = \frac{1}{\mathrm{E}_{\gamma_0}\left[1/\gamma_{SD}\right]} = \frac{1}{\int_{\gamma_0}^{\infty} f(\gamma_{SD})/\gamma_{SD} d\gamma_{SD}} \tag{5.9}$$

with $f(\cdot)$ denoting the probability density function for the continuous random variable. The optimal value of the cutoff fade depth, γ_0^*, is selected to maximize the capacity,

$$\gamma_0^* = \arg\max_{\gamma_0} \log_2\left(1 + \frac{1}{\mathrm{E}_{\gamma_0}\left[1/\gamma_{SD}\right]}\right) \Pr(\gamma_{SD} \geq \gamma_0) \tag{5.10}$$

For all of the transmission time slots (i.e., the time slots when $\gamma_{SD} \geq \gamma_0$), the outage probability at the destination is zero. However, the eavesdropper encounters outage in the transmission time slot n if

$$\begin{aligned} &\log_2(1 + \frac{P(\gamma_{SD})[n]}{N_0}|h_{SE}[n]|^2) < \log_2(1+\gamma^c) \triangleq R \\ \Rightarrow \quad &|h_{SE}[n]|^2 < |h_{SD}[n]|^2 \end{aligned} \tag{5.11}$$

The delivery of the original file is finished in N transmission time slots because of the zero-outage at the destination, and then the transmission is terminated. The eavesdropper intercepts the file only when it can also have zero-outage performance during these N time slots. In other words, the channel gain of the eavesdropper should be greater than or equal to that of the destination in these time slots. Thus the intercept probability is calculated as

$$\begin{aligned} \varepsilon^{TPC} &= \prod_{i=1}^{N} \Pr\left\{ |h_{SE}[i]|^2 \geq |h_{SD}[i]|^2 \middle| \gamma_{SD}[i] \geq \gamma_0 \right\} \\ &= \left\{ \frac{\lambda_{SD} e^{-(\lambda_{SD}+\lambda_{SE})th}}{(\lambda_{SD}+\lambda_{SE})\, e^{-\lambda_{SD} th}} \right\}^N \end{aligned} \tag{5.12}$$

where $th = \gamma_0/\rho$. The intercept probability also decreases exponentially with K. Obviously, this power control strategy is also suitable for *S1*.

C. Application issues of the proposed scheme

The intercept probability of the proposed scheme decreases as the value of

K increases. This characteristic can be utilized to satisfy the required secrecy constraint. If we assume a maximum possible average channel gain of the eavesdropper, the minimum values of K can be derived by

$$K^{CF} = \arg\min_{K>0} \left\{ \varepsilon^{CF}(N) < \varepsilon_{th} \right\} \tag{5.13}$$

$$K^{TPC} = \arg\min_{K>0} \left\{ \varepsilon^{TPC}(N) < \varepsilon_{th} \right\} \tag{5.14}$$

where ε_{th} is the intercept probability requirement. For the delivery of large files or streaming media, the value of K can be selected flexibly as described in [104]. Therefore, it is feasible to realize a desired intercept probability by adjusting the value of K. When dealing with small files, the confidential data can be distributed into more packets by introducing redundancy or merging multiple files.

The other observation is that in the proposed scheme, the source delivers the confidential data through ordinary fountain coded transmission. The achievable data rates for CF and TPC strategies in the physical layer depend on the outage capacity and the capacity of the truncated channel inversion respectively [4]. It is not necessary to deliver the fountain packets according to the system secrecy capacity, which focuses on the perfect secrecy of every transmitted packet. The eavesdropper is allowed to correctly decode some transmitted fountain packets. However, before enough fountain packets are obtained for fountain decoding, the eavesdropper cannot recover the original data file or even any original packets at the application layer due to the fountain encoding and optional preprocessing.

Besides the power control strategy, other adaptive strategies can be also adopted for *S2*, such as adaptive modulation and coding as well as channel pre-compensation. The eavesdropper suffers from outage if its channel gain is lower than that of the destination because the related control parameters are adjusted according to the source-destination link. The control parameters at the source can be derived from the pilot signal or CSI feedback sent by the

destination[2]. System complexity is not increased much because many existing wireless protocols have introduced these techniques. The additional complexity of the proposed scheme is caused by the introduction of fountain codes, which has been analyzed in detail in [101] and references therein.

5.2.3 Numerical results and discussions

The results of computer simulations are provided to evaluate the proposed scheme. The simulation environment is established in a 2D rectangular coordinate system, where the source and the destination are located at (0, 0) and (1, 0) respectively. Path loss exponent β is set to 3, $\rho = 10dB$ and $\delta = 0.05$.

Fig 5.2 shows the effect of K on the secrecy performance of the proposed scheme[3][4]. The simulation results are consistent with those of the theoretical analysis. Moreover, the intercept probability is reduced to zero near-exponentially with increasing K values for the CF strategy in *S1*, and is reduced to zero exponentially for the TPC strategy. Therefore, an arbitrarily small intercept probability can be realized by increasing the value of K.

The intercept probability for the different locations of Eve is presented in Fig 5.3. The intercept probability is slightly higher than 0.5 for the CF strategy when Eve is also located at (1, 0) and has the same average channel condition as Bob. This result is due to that the interception occurs when the eavesdropper obtains N fountain packets first or simultaneously. The intercept probability for the CF strategy also decreases (increases) as the value of K increases given that the destination has a better (worse) average channel condition than the eavesdropper. Therefore, the CF strategy is only applicable to *S1*. On the other hand, the TPC strategy applies to both scenarios and exhibits better secrecy performance but at the cost of system complexity. The secrecy performance of the two strategies deteriorates as the eavesdropper comes closer to the source. However, increasing the value of K is an effective approach to reduce

[2]The proposed scheme does not rely on the secrecy of CSI.

[3]Simulation for large K values is difficult because of the extremely small intercept probability.

[4]For ε^{CF} of (5.7), we find that the items $l > (N+500)$ almost cannot affect the sum value when $K \leq 300$. Thus, the first 500 items are adopted to obtain approximate results.

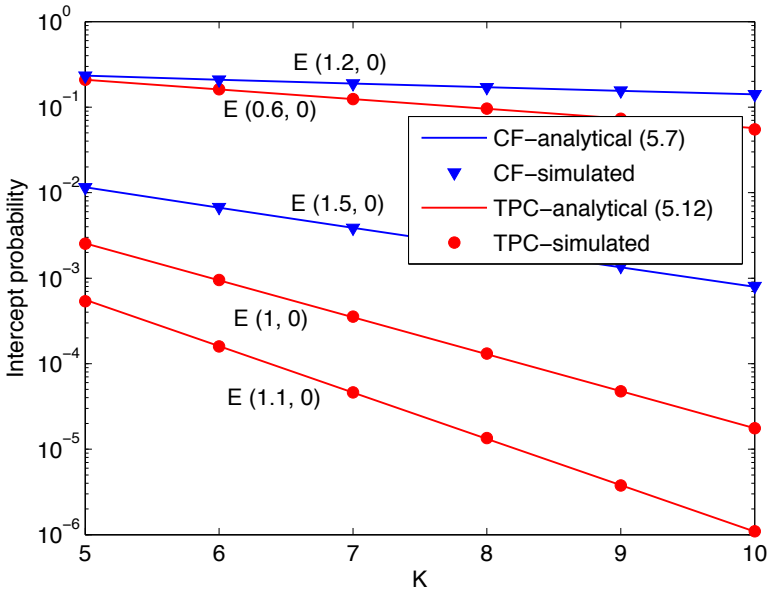

Figure 5.2: Intercept probability with different values of K.

the intercept probability.

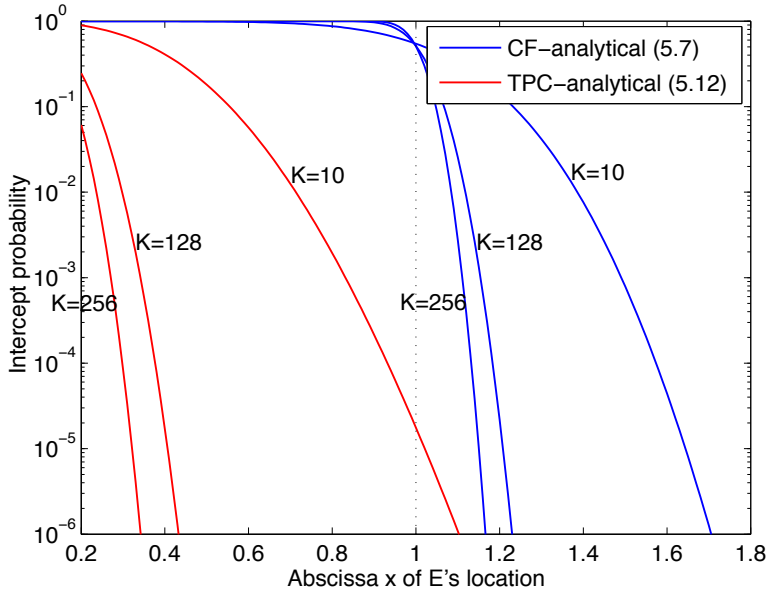

Figure 5.3: Intercept probability for the different locations of the eavesdropper (E is located at (x, 0)).

Table 5.1 provides some results of the minimum values of K for different application scenarios, which are derived from Eqn (5.13) and (5.14) numerically.

The results prove again that the desired intercept probability can be satisfied by selecting an appropriate value of K. In 3GPP MBMS [105], $K \geq 1024$ is recommended; this condition is sufficient to realize secure delivery for a wide range of application scenarios.

Table 5.1: The minimum values of K for different application scenarios

	CF		TPC		
E / ε_{th}	$(1.5, 0)$	$(1.2, 0)$	$(1.1, 0)$	$(1, 0)$	$(0.6, 0)$
10^{-3}	10	74	5	6	23
10^{-5}	19	120	10	11	42
10^{-10}	41	275	18	22	84

5.3 FCAS for Internal Eavesdropping in CRNs

5.3.1 System model

The cooperative networks with an untrusted relay is as shown in Fig 5.4, where the relay helps to forward the source packets but also attempts to decode the information. The channel model is the same as that in Fig 5.1, and FCAS is adopted to protect from the internal eavesdropping. That is to say, the secure transmission is realized if the destination receives fountain packets faster than the untrusted relay.

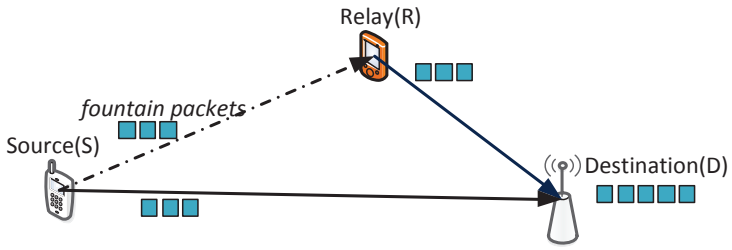

Figure 5.4: The cooperative network with an untrusted relay.

5.3.2 FCAS without transmit power control

First, we consider the cooperation scenario by only using fountain codes for DF and AF protocols respectively. For simplicity, the selection combining is adopted at the destination.

A. DF protocol

For DF protocol, the relay decodes the transmitted fountain packets and then forwards the correctly decoded packets to the destination. According to the channel model, the packet loss probability at the relay is similar to the result in Section 5.2, i.e.,

$$\begin{aligned} \varepsilon_{R-DF} &= \Pr\{\log_2(1+\rho|h_{SR}|^2) < R\} \\ &= 1 - e^{-\lambda_{SR}\zeta/\rho} \end{aligned} \tag{5.15}$$

Due to the cooperative relaying, a packet is lost at the destination only when both the direct link and the relay link have a bad channel quality. The packet loss probability at the destination is

$$\begin{aligned} \varepsilon_{D-DF} &= \Pr\{\log(1+\rho|h_{SD}|^2) < R\} \\ &\quad \Pr\{\log(1+\rho\min\{|h_{SR}|^2, |h_{RD}|^2\}) < R\} \\ &= (1 - e^{-\lambda_{SD}\zeta/\rho})(1 - e^{-(\lambda_{SR}+\lambda_{RD})\zeta/\rho}) \end{aligned} \tag{5.16}$$

As described in Section 5.2, the required time slots L_j for the receiver j to receive N fountain packets correctly follow the negative binomial distribution $\mathcal{NB}(N, 1-\varepsilon_j)$. That is to say, the probability mass function and cumulative distribution function of L_j are

$$\begin{aligned} f_{L_{j-DF}}(l) &= \Pr\{L_{j-DF} = l\} \\ &= \begin{pmatrix} l-1 \\ N-1 \end{pmatrix} (1-\varepsilon_{j-DF})^N {\varepsilon_{j-DF}}^{l-N}, l \geq N \end{aligned} \tag{5.17}$$

$$F_{L_{j-DF}}(l) = \Pr\{L_{j-DF} \leq l\}$$

$$= \sum_{x=N}^{l} \begin{pmatrix} x-1 \\ N-1 \end{pmatrix} (1-\varepsilon_{j-DF})^{N} {\varepsilon_{j-DF}}^{x-N}, l \geq N \quad (5.18)$$

The expected values of L_j is $N/(1-\varepsilon_j)$. Therefore, if we know that $\varepsilon_{D-DF} < \varepsilon_{R-DF}$, the destination is expected to receive fountain packets faster than the relay does. Since the channel fading is random, there is still a certain probability that the relay decodes enough fountain packets first. This intercept probability is derived as

$$\mathrm{P}_{\mathrm{intercept-DF}} = \sum_{l=N}^{\infty} f_{L_{D-DF}}(l) F_{L_{R-DF}}(l) \quad (5.19)$$

If $\varepsilon_{D-DF} < \varepsilon_{R-DF}$, $\mathrm{P}_{\mathrm{intercept-DF}}$ reduceds to zero near-exponentially as N (i.e., K) increases. When K is large enough, the probability of interception becomes too small to be ignored.

B. AF protocol

For AF protocol, the untrusted relay simply forwards the received signal after amplification. Simultaneously, the relay tries to decode the transmitted packets for itself. The packet loss probability of the relay for AF protocol is the same as that for DF protocol, and thus $\varepsilon_{R-AF} = \varepsilon_{R-DF}$. The packet loss probability at destination is changed to

$$\begin{aligned} \varepsilon_{D-AF} &= \Pr\{\log(1+\rho|h_{SD}|^2) < R\} \\ &\quad \Pr\{\log(1+\frac{\rho|h_{SR}|^2\rho|h_{RD}|^2}{1+\rho|h_{SR}|^2+\rho|h_{RD}|^2}) < R\} \\ &= \left(1-e^{-\lambda_{SD}\zeta/\rho}\right)\left(1-2e^{-(\lambda_{SR}+\lambda_{RD})\zeta/\rho}\right. \\ &\quad \left.\sqrt{\lambda_{SR}\lambda_{RD}\frac{\zeta}{\rho}\left(\frac{\zeta}{\rho}+1\right)}\, K_1\left(2\sqrt{\lambda_{SR}\lambda_{RD}\frac{\zeta}{\rho}\left(\frac{\zeta}{\rho}+1\right)}\right)\right) \quad (5.20) \end{aligned}$$

where $K_1()$ is the first order modified Bessel function of the second kind [94, 106]. The following analysis is similar to that for the DF protocol, by changing DF to AF in the equations. The security can be enhanced by increasing K value, if $\varepsilon_{D-AF} < \varepsilon_{R-AF}$.

5.3.3 FCAS with transmit power control

Because the secure cooperation scheme only using fountain codes does not work when $\varepsilon_{D-D(A)F} \geq \varepsilon_{R-D(A)F}$, we still propose to use transmit power control to solve this problem[5].

A. DF protocol

The transmit power control designed for DF protocol is shown as follows,

$$\begin{cases} P_{S-DF} = \frac{\zeta N_r}{\max\left\{|h_{SD}|^2, |h_{SR}|^2\right\}}, if\ C_{RD} \geq R \\ P_{S-DF} = \frac{\zeta N_r}{|h_{SD}|^2}, if\ C_{RD} < R \end{cases} \tag{5.21}$$

In this case, the destination can always decode the transmitted packets, while the relay loses the packet when $|h_{SR}|^2 < |h_{SD}|^2$. Therefore, in order to intercept the information, $|h_{SR}|^2$ should be larger than or equal to $|h_{SD}|^2$ in all the N transmission time slots. That means the intercept probability is

$$\mathrm{P}^{\mathrm{TPC}}_{\mathrm{intercept-DF}} = \prod_{n=1}^{N} \Pr\left(|h_{SR}|^2 \geq |h_{SD}|^2\right) = \left(\frac{\lambda_{SD}}{\lambda_{SD} + \lambda_{SR}}\right)^N \tag{5.22}$$

It is observed that we can reduce the intercept probability to zero by simply increasing the value of N (K).

B. AF protocol

The transmit power control scheme for AF protocol is designed as,

$$\begin{cases} P_{S-AF} = \frac{(1+\rho|h_{RD}|^2)\zeta N_0}{\left(\rho|h_{SR}|^2|h_{RD}|^2 - |h_{SR}|^2\zeta\right)}, if |h_{SR}|^2 \geq |h_{SD}|^2 \\ P_{S-AF} = \frac{\zeta N_0}{|h_{SD}|^2}, if\ |h_{SR}|^2 < |h_{SD}|^2 \end{cases} \tag{5.23}$$

For AF protocol with transmit power control, the intercept probability is the same as that for DF protocol, such that $\mathrm{P}^{\mathrm{TPC}}_{\mathrm{intercept-AF}} = \mathrm{P}^{\mathrm{TPC}}_{\mathrm{intercept-DF}}$.

[5]Without loss of generality, γ_0 of Eqn (5.8) is set to be zero in this section. However, it is simple to revise the derived results for other values of γ_0.

5.3.4 Numerical results and discussions

In this section, the numerical results are given to validate our proposed scheme. Similar to Section 5.2, the source and destination are located at (0,0) and (1,0) respectively in a two-dimensional coordinate simulation environment, while the relay (eavesdropper) moves on X axis from (0,0) to (1,0). The decoding overhead of fountain codes $\delta = 0.05$. In addition, the path loss exponent β and ρ are set to be 3 and 20dB for simulation convenience.

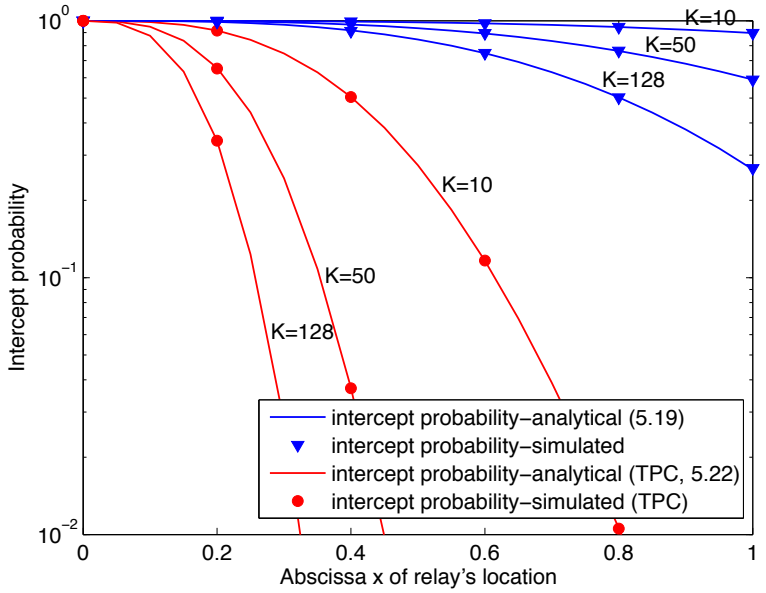

Figure 5.5: The intercept probability of the FCAS without & with TPC for a DF untrusted relay.

Fig 5.5 shows both the analytical and the simulated results of the FCAS without/with TPC for a DF untrusted relay. First, it can be observed that the simulation results accord with the theoretical analysis. In addition, the secure cooperation without TPC does not work when the relay is near to the source (to be more exact, when $\varepsilon_{D-DF} \geq \varepsilon_{R-DF}$), since we cannot reduce the intercept probability by increasing the value of K. However, the secure cooperation scheme with TPC works even when the relay is close to the source. Through increasing the value of K, the intercept probability decreases to zero rapidly. The results for an AF untrusted relay are similar to those for the

DF untrusted relay, and thus we omit the performance figure here due to the similarity.

5.4 Summary

In this chapter a novel secure wireless transmission scheme using fountain codes (fountain-code assisted security: FCAS) is first proposed. To realize the secrecy of data transmission, physical layer strategies are introduced to make the destination receive fountain packets faster than the eavesdropper. Analytical and simulated results demonstrate that the proposed scheme can almost always realize secure transmission if the number of source packets is sufficiently large. In addition, the proposed scheme delivers confidential data through ordinary fountain codes, which are transmitted according to the channel capacity of the source-destination link instead of the system secrecy capacity.

Then, the proposed FCAS scheme is applied in cooperative networks to resist an untrusted relay. Similarly, the security can be realized if we can make the destination obtain fountain packets more quickly than the relay. The theoretical analysis and numerical simulations are also conducted, from which the effectiveness of the FCAS for protecting from the internal eavesdropping is confirmed.

Chapter 6

Fixed Linear Code Assisted Security for Resisting Multiple Untrusted Relays

The fountain code assisted security (FCAS) is proposed in last chapter to realize secure wireless transmission, and then used to protect from the internal eavesdropping caused by an untrusted relay. Due to the randomness characteristics of fountain codes, however, the eavesdropper can still decode a small number of original packets before enough fountain packets are obtained. Therefore, we adopt a fixed linear code in this chapter, which overcomes this shortcoming of fountain codes ("fixed" used here is corresponding to the randomness characteristics of fountain codes). Furthermore, the more complicated scenario of the internal eavesdropping by multiple untrusted relays is analyzed. It is derived that the superiority of FCAS is still held, that the intercept probability is decreased to zero exponentially with the number of source packets. To accelerate the rate of decrease for multiple untrusted relays, the introduction of destination based jamming strategy is also considered. At last, the comparisons of the fixed linear code assisted security with FCAS and experiment evaluations are conducted.

6.1 Introduction

We exploit the fountain codes to achieve the secure data transmission for wireless networks (fountain code assisted security, FCAS) in Chapter 5. The scheme is based on an important fact that, for fountain coded transmissions, any receiver must obtain a sufficient number of fountain packets to recover the original data. If the destination can accumulate the packets more quickly than the eavesdropper, the security will be guaranteed. However, the fountain packets do not conceal the original data ideally. Since each encoded fountain packet is the bitwise sum of distinct source packets chosen randomly [101], there are always some fountain packets which are the original packets. If fountain decoding is performed greedily, the receiver can still decode a small number of original packets even though not enough fountain packets are received (as shown in Fig. 8 of [101] and the experimental decodings performed by us in Fig 6.1, where the parameter settings for the degree distribution are the same as those in Fig. 8 of [101]). For the strict application that no original packets can be decoded by the eavesdropper, we introduce a fixed linear code by which the information can encrypt itself more perfectly than the fountain codes.

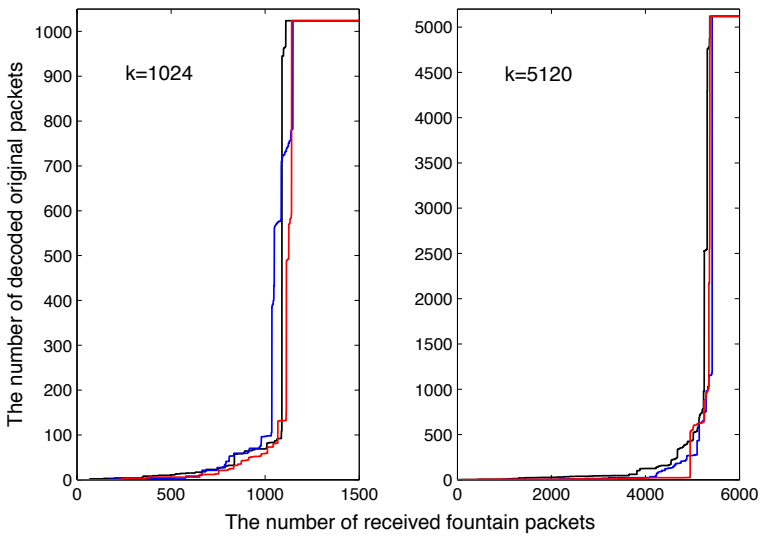

Figure 6.1: Three experimental decodings for LT fountain codes.

On the other hand, the internal eavesdropping attack considered in Chapter 5 is only caused by one untrusted relay. For a more general application, the cooperative networks with multiple untrusted relays should be studied. Till now, few literatures [64–66, 107] research on the issue of multiple untrusted relays, among which [64–66] focus on the perfect secrecy through the original physical layer security (PLS) and [107] considers the security from a different perspective of bit error rate. In this chapter, we contribute to this issue and adopt the fixed linear code assisted security (FLCAS) to resist untrusted relays. Specifically, Our contributions are listed as follows,

1) A fixed linear code assisted security scheme -FLCAS with linear complexity is designed, which avoids the information leakage caused by the fountain codes before enough coded packets are received correctly. Similar to FCAS, the FLCAS also relaxes the strict requirements of PLS, and thus the transmission can be performed according to the ordinary channel capacity instead of the secrecy capacity.

2) The security performance (intercept probability) is derived when applying the FLCAS to resist multiple untrusted relays. The intercept probability is proved to be also reduced to zero exponentially as the number of the original packets increases. To accelerate the rate of decrease of the intercept probability, the destination based jamming (DBJ) strategy is further introduced. In addition, it is observed that adopting cooperation achieves a better secrecy performance than treating the untrusted relays as pure eavesdroppers.

3) The comparisons of FLCAS with FCAS are made by analyzing their similarities and differences. Then, the experiment evaluations using NI USRP-2921 platforms are conducted to confirm their secrecy performance.

6.2 System Model

The considered cooperative networks with multiple untrusted relays are as shown in Fig 6.2, which consists of one source (S), one destination (D) and K untrusted relays (denoted by a relay set $\mathbf{R}=\{\mathrm{R}_1, \mathrm{R}_2, ..., \mathrm{R}_\mathrm{K}\}$). All of the nodes are operated in a half-duplex mode with a single antenna. S intends to deliver

a confidential data to D through packet-based wireless transmission with the potential cooperation of the relays. However, the relays are only service level trust but not data level trust [107], i.e., they attempts to intercept (decode) the data simultaneously when they cooperate. For the worst case, the relays are also supposed to be collusive with each other.

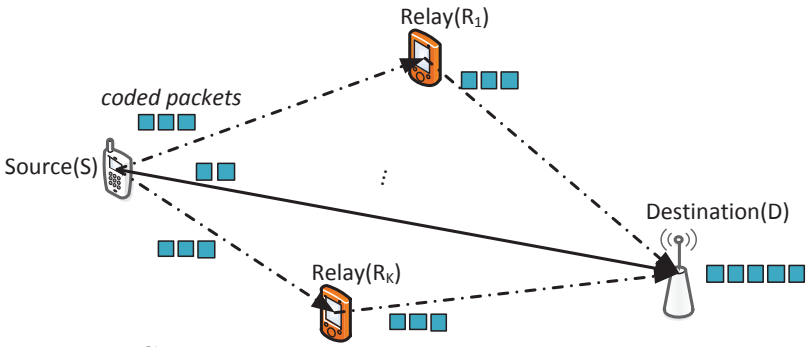

Figure 6.2: Cooperative networks with multiple untrusted relays

The transmission links are modelled as the Rayleigh block flat fading channels as usual. That is to say, the channel coefficient h_{uv} between node u and node v is a complex circularly symmetric Gaussian variable with mean zero and variance σ_{uv}^2. Meanwhile, h_{uv} remains constant during the transmission of one packet and varies independently among different packets. S and the relays (if cooperation is selected) transmit the packets with power P and a target rate R bits/s/Hz. The noise at each receiver is represented by the additive white Gaussian noise with variance N_0. Therefore, the received signal-to-noise ratio (SNR) for the link between node u and node v is written as $\gamma_{uv} = \rho|h_{uv}|^2$, where $\rho = P/N_0$. The γ_{uv} follows an exponential distribution with parameter $\lambda_{uv} = (\rho\sigma_{uv}^2)^{-1}$.

The original packets of the confidential data are denoted by $(\mathrm{I}_1, \mathrm{I}_2, \ ..., \mathrm{I}_N)$. For the direct transmission (DT), the instantaneous achievable rate at D can be expressed as

$$C_D = \log_2(1 + \gamma_{SD}) \tag{6.1}$$

Considering that the capacity-achieving code is adopted at the physical layer, D receives I_n correctly if $C_D \geq R$. The system uses basic automatic repeat-

request (ARQ) mechanism to ensure D obtains all of the packets, in which the receivers simply discard the erroneous packets. When the relays are treated pure eavesdroppers, the achievable rate of the relay $\mathrm{R_k}$ is

$$C_k = \log_2 (1 + \gamma_{Sk}) \tag{6.2}$$

Since the relays are collusive, they can share their obtained information. For simplicity, we assume that one original packet is intercepted if any relay decodes it correctly and the mutual information accumulation among the relays is not considered. Therefore, the packet I_n is intercepted if $\max\limits_{\mathrm{R_k} \in \mathbf{R}} \{C_k\} \geq R$.

If the cooperation mode is decided, the relays assist the transmission of S but also act as the eavesdroppers at the same time. As a low complexity scheme to benefit from the multi-relay cooperation, relay selection strategy is adopted in which only the best relay is selected to cooperate for every transmission. The transmission is divided into two phases. In phase I S broadcasts its packet, and in phase II the selected relay forwards its received signals by either DF or AF protocol. The achievable rate at D by using the DF protocol is given by

$$C_D^{DF} = 0.5 \log_2 \left(1 + \gamma_{SD} + \max_{\mathrm{R_k} \in \mathbf{R}'} \{\gamma_{kD}\} \right) \tag{6.3}$$

where $\mathbf{R}'$ is the decoding set which includes the relays that succeed in decoding the transmitted packet. As for the AF protocol, the achievable rate at D is

$$C_D^{AF} = 0.5 \log_2 \left(1 + \gamma_{SD} + \max_{\mathrm{R_k} \in \mathbf{R}} \left\{ \frac{\gamma_{Sk} \gamma_{kD}}{1 + \gamma_{Sk} + \gamma_{kD}} \right\} \right) \tag{6.4}$$

The achievable rate at relay $\mathrm{R_k}$ in the cooperation mode is $C'_k = 0.5 C_k$. Therefore, it requires $\max\limits_{\mathrm{R_k} \in \mathbf{R}} \{C'_k\} \geq R$ to intercept one packet.

6.3 Fixed Linear Code Assisted Security (FLCAS)

It can be observed that the relays can easily intercept some confidential data if the original packets are transmitted directly. Therefore, a fixed linear code assisted security scheme is designed to resist untrusted relays while employing them to cooperate.

6.3.1 Scheme descriptions

Intuitively, the original packets can be pre-processed such that a certain number of the processed packets are necessary to recover the original data. And thus the transmission is secured if the destination receives enough processed packets faster than the eavesdroppers. In our previous work of last chapter, the fountain codes are adopted to realize this kind of secure transmission. Due to the randomness characteristics of fountain codes, however, the eavesdropper(s) can still decode a small number of original packets before enough fountain packets are obtained. Therefore, a fixed linear coding scheme is adopted in this chapter which achieves a much better information self-encrypted performance. Specifically, for the N original packets $(\mathrm{I}_1, \mathrm{I}_2, ..., \mathrm{I}_N)$, the following $N \times N$ generator matrix is used,

$$T = \begin{bmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 0 & 1 \\ 1 & 1 & 1 & \cdots & 1 & 0 \end{bmatrix} \tag{6.5}$$

Assuming each original packet has B bits, i.e., $\mathrm{I}_n = [i_{1n}, i_{2n}, ..., i_{Bn}]^{tr}$, the coding scheme is written as

$$[\mathrm{P}_1, \mathrm{P}_2, ..., \mathrm{P}_N] = [\mathrm{I}_1, \mathrm{I}_2, ..., \mathrm{I}_N] * T(\mathrm{mod}2) \tag{6.6}$$

where, the processed packet $\mathrm{P}_n = [p_{1n}, p_{2n}, ..., p_{Bn}]^{tr}$ also has B bits. The scheme can be represented as the following equation by the bit-wise modulo two operation among the original packets,

$$\mathrm{P}_n = \mathrm{I}_1 \oplus ... \oplus \mathrm{I}_{n-1} \oplus \mathrm{I}_{n+1} \oplus ... \oplus \mathrm{I}_N = \sum_{l=1}^{N} \mathrm{I}_l \oplus \mathrm{I}_n \tag{6.7}$$

If N is an even number, the generator matrix T has an inverse matrix $T^{-1} = T$. That is to say, the original packets can be recovered through the same process as the encoding scheme,

$$\mathrm{I}_n = \mathrm{P}_1 \oplus ... \oplus \mathrm{P}_{n-1} \oplus \mathrm{P}_{n+1} \oplus ... \oplus \mathrm{P}_N = \sum_{l=1}^{N} \mathrm{P}_l \oplus \mathrm{P}_n \tag{6.8}$$

If the number of the original packets is odd in practical application, we can simply add a redundant packet. The FLCAS combines this fixed linear code and the concept of PLS to realize the secure data transmission: First the data packets are transmitted after this fixed linear code, and then channel fading is exploited to make that only the destination receives all of the coded packets through ARQ. As far as we know, we are the first to jointly use this fixed linear code and physical characteristics of the wireless channels to pursue the secure data transmission.

6.3.2 Secrecy performance and complexity

A. Secrecy performance

According to the scheme descriptions, we can get the following conclusion: if less than $N-1$, $N-1$ and N coded packets are obtained correctly, 0, only 1 and all of the N original packets can be recovered respectively. As for

the recovery of one specified original packet I_n, it needs $N-1$ coded packets $\{\mathrm{P}_1, ..., \mathrm{P}_{n-1}, \mathrm{P}_{n+1}, ..., \mathrm{P}_N\}$. The secrecy of I_n is achieved if less than these $N-1$ coded packets are received. Therefore, all of the original packets cannot be recovered before $N-1$ coded packets are received.

In case we neglect the data leakage caused by one original packet (only one original packet can be recovered when $N-1$ coded packets are received), it is regarded that the confidential data is intercepted only if the untrusted relays obtain all of the N coded packets when the transmission from S to D is finished. By exploiting the random channel fading at the physical layer, an arbitrarily small intercept probability can be realized as N increases. This characteristic is utilized in this chapter to resist these untrusted relays and satisfy any predetermined secrecy constraints, which will be analyzed in detail in next section.

B. Linear complexity

The encoding process can be designed directly based on Eqn (6.7) that $\mathrm{P}_n = \sum_{l=1}^{N} \mathrm{I}_l \oplus \mathrm{I}_n$, in which the $\sum_{l=1}^{N} \mathrm{I}_l$ is calculated first and then each P_n is derived by the modulo two operation with I_n. Therefore, the complexity of the proposed scheme is $2N$ (i.e., linear complexity $\mathcal{O}(N)$). The complexity of the decoding process has the same result.

6.4 Intercept Probability Analysis

In this section, the intercept probability of FLCAS for protecting from the internal eavesdropping is analyzed.

6.4.1 Intercept probabilities for direct transmission and cooperative relaying with untrusted relays

A. Direct transmission

In this case, the untrusted relays are not employed and simply treated as the eavesdroppers. The probability that one received packet is not decoded

correctly at the destination is

$$\varepsilon_D = \Pr\left\{C_D = \log_2\left(1+\gamma_{SD}\right) < R\right\} = 1 - e^{-\lambda_{SD}\tau} = F\left(\lambda_{SD}\tau\right) \tag{6.9}$$

where, $F\left(\chi\right) = 1 - \exp\left(-\chi\right)$ and $\tau = 2^R - 1$. On the other hand, the relays have the packet error probability

$$\begin{aligned} \varepsilon_R &= \Pr\left\{\max_{\mathrm{R_k}\in\mathbf{R}}\left\{C_k\right\} = \log_2\left(1+\max_{\mathrm{R_k}\in\mathbf{R}}\left\{\gamma_{Sk}\right\}\right) < R\right\} \\ &= \prod_{k=1}^{K}\left(1-e^{-\lambda_{Sk}\tau}\right) = \prod_{k=1}^{K} F\left(\lambda_{Sk}\tau\right) \end{aligned} \tag{6.10}$$

The required time slots T_D and T_R for the destination and the relays to recover one packet meets the geometric distribution with parameter $1-\varepsilon_D$ and $1-\varepsilon_R$ respectively, i.e., their probability mass function (PMF) and cumulative distribution function (CDF) are given by

$$f_v\left(T_v\right) = \varepsilon_v^{T_v-1}\left(1-\varepsilon_v\right) \tag{6.11}$$

$$F_v\left(T_v\right) = \sum_{t_v=1}^{T_v}\varepsilon_v^{t_v-1}\left(1-\varepsilon_v\right) = 1-\varepsilon_v^{T_v} \tag{6.12}$$

To obtain one coded packet, the relays should decode the packet correctly not after it is correctly received by the destination through ARQ. Thus, the intercept probability for one coded packet is calculated as

$$\begin{aligned} P_{I-1} &= \sum_{T_D=1}^{\infty} f_D\left(T_D\right) F_R\left(T_D\right) \\ &= \sum_{T_D=1}^{\infty}\varepsilon_D^{T_D-1}(1-\varepsilon_D)(1-\varepsilon_R^{T_D}) = \frac{1-\varepsilon_R}{1-\varepsilon_D\varepsilon_R} \end{aligned} \tag{6.13}$$

In order to intercept the confidential data, the eavesdropper should receives all of the $\{\mathrm{P}_1, \mathrm{P}_2, ..., \mathrm{P}_N\}$ correctly. The intercept probability is thus derived as

$$P_I = \left(P_{I-1}\right)^N \tag{6.14}$$

It is observed that the intercept probability decreases to zero *exponentially* as N increases, which means that any arbitrary small intercept probability can be satisfied by simply increasing the value of N.

B. DF protocol

For the DF cooperation, there should be some coded packets that D receives directly without the cooperation of any relays (i.e., the decoding set R′ should be null set). In this case, the packet error probability of D is

$$\begin{aligned} \varepsilon_D^{DF} &= \Pr\left\{C_D^{DF} = 0.5\log_2\left(1+\gamma_{SD}+\max_{\mathrm{R_k}\in\emptyset}\{\gamma_{kD}\}\right) < R\right\} \\ &= 1-e^{-\lambda_{SD}\tau'} = F\left(\lambda_{SD}\tau'\right) \end{aligned} \tag{6.15}$$

where, $\tau' = 2^{2R}-1$. Simultaneously, $\varepsilon_R^{DF} = \prod_{k=1}^{K} F\left(\lambda_{Sk}\tau'\right)$. The secure transmission of one packet is thus obtained as

$$\begin{aligned} P_{S-1}^{DF} &= \sum_{T_D=1}^{\infty} f_D\left(T_D\right)\left(1-F_R\left(T_D\right)\right) \\ &= \sum_{T_D=1}^{\infty} \left(\varepsilon_D^{DF}\right)^{T_D-1}\left(1-\varepsilon_D^{DF}\right)\left(\varepsilon_R^{DF}\right)^{T_D} \\ &= \frac{\varepsilon_R^{DF}-\varepsilon_D^{DF}\varepsilon_R^{DF}}{1-\varepsilon_D^{DF}\varepsilon_R^{DF}} \end{aligned} \tag{6.16}$$

Therefore, the intercept probability of one packet is

$$P_{I-1}^{DF} = 1-P_{S-1}^{DF} = \frac{1-\varepsilon_R^{DF}}{1-\varepsilon_D^{DF}\varepsilon_R^{DF}} \tag{6.17}$$

The intercept probability of the confidential data is also

$$P_I^{DF} = \left(P_{I-1}^{DF}\right)^N \tag{6.18}$$

For mathematical convenience and fair comparison among different numbers of relays, it is assumed that for all of the λ_{Sk} and λ_{kD} are identical in this

chapter, and denoted that $\lambda_{Sk} = \lambda_{SR}$ and $\lambda_{kD} = \lambda_{RD}$. We can easily derive

$$P_{I-1}^{DF}(K_1) > P_{I-1}^{DF}(K_2), \quad \text{for } K_1 > K_2 \tag{6.19}$$

from the fact that $\varepsilon_R(K_1) < \varepsilon_R(K_2)$. Therefore, more untrusted relays *deteriorates* the secrecy performance, although more diversity gain can be achieved. Furthermore, whether to select the cooperation or not can be also decided by comparing Eqn (6.13) and Eqn (6.17). However, we can still reduce the intercept probability *exponentially* by simply increasing the value of N.

C. AF protocol

It is intractable to obtain the exact intercept probability of the AF protocol. Therefore, we consider its upper and lower bounds by using the following inequalities,

$$\frac{\gamma_{Sk}\gamma_{kD}}{1+\gamma_{Sk}+\gamma_{kD}} \geq \frac{\gamma_{Sk}\gamma_{kD}}{\gamma_{Sk}+\gamma_{kD}} - \frac{1}{4} \geq \frac{1}{2}\min\left\{\gamma_{Sk}, \gamma_{kD}\right\} - \frac{1}{4} \triangleq \gamma_{AF}^{-} \tag{6.20}$$

and,

$$\frac{\gamma_{Sk}\gamma_{kD}}{1+\gamma_{Sk}+\gamma_{kD}} \leq \frac{\gamma_{Sk}\gamma_{kD}}{\gamma_{Sk}+\gamma_{kD}} \leq \min\left\{\gamma_{Sk}, \gamma_{kD}\right\} \triangleq \gamma_{AF}^{+} \tag{6.21}$$

where the first equality comes from the result derived in [108].

First the upper bound of the intercept probability is analyzed. We can derive the probability that both D and the untrusted relays cannot receive a packet correctly as follows,

$$\begin{aligned}
\varepsilon_{R,D}^{AF+} &= \Pr\left\{\max_{k\in \mathrm{R}}\left\{\gamma_{Sk}\right\} < R, \gamma_{SD} + \max_{k\in \mathrm{R}}\left\{\gamma_{AF}^{-}\right\} < R\right\} \\
&= G\left(F\left(\lambda_{SR}\tau'\right), \frac{\lambda_{SR}}{I_1}F\left(I_1\tau'\right) - A_1 \right. \\
&\quad \left. + \frac{\lambda_{RD}}{I_1 - \lambda_{SR}}\left[F\left(\lambda_{SR}\tau'\right) - \frac{\lambda_{SR}}{I_1}F\left(I_1\tau'\right)\right] - A_2\right)
\end{aligned} \tag{6.22}$$

where,

$$G(\alpha,\beta) = K\sum_{k_1=0}^{K-1}\sum_{k_2=0}^{K-1-k_1}\left[\begin{pmatrix} K-1 \\ k_1 \end{pmatrix} \begin{pmatrix} K-1-k_1 \\ k_2 \end{pmatrix} \alpha^{k_1}(-1)^{k_2}(1-\alpha)^{K-1-k_1-k_2}\beta\right]$$

$I_1 = (\lambda_{SR}+\lambda_{RD})(k_2+1)+\lambda_{RD}(K-1-k_1-k_2)$, $I_2 = I_1 - 0.5\lambda_{SD}$, $\tau_1 = 2^{2R}-0.75$ and,

$$A_1 = \begin{cases} \lambda_{SR}[1-F(\lambda_{SD}\tau_1)]\tau', I_2 = 0 \\ \frac{\lambda_{SR}[1-F(\lambda_{SD}\tau_1)]}{I_2} F(I_2\tau'), else \end{cases}$$

$$A_2 = \begin{cases} \frac{\lambda_{RD}[1-F(\lambda_{SD}\tau_1)]}{\lambda_{SR}} [F(\lambda_{SR}\tau') \\ \quad -\lambda_{SR}\tau'\exp(-\lambda_{SR}\tau')], I_2-\lambda_{SR}=0 \\ \frac{\lambda_{RD}[1-F(\lambda_{SD}\tau_1)]}{I_2-\lambda_{SR}} [F(\lambda_{SR}\tau') - \lambda_{SR}\tau'], I_2 = 0 \\ \frac{\lambda_{RD}[1-F(\lambda_{SD}\tau_1)]}{I_2-\lambda_{SR}} \left[F(\lambda_{SR}\tau') - \frac{\lambda_{SR}}{I_2}F(I_2\tau')\right], else \end{cases}$$

(See Appendix C.1).

Then the probability that only D decodes a packet correctly is similarly calculated as,

$$\begin{aligned} \varepsilon_{R,\mathcal{D}}^{AF+} &= \Pr\left\{\max_{k\in\mathrm{R}}\{\gamma_{Sk}\} < R, \gamma_{SD} + \max_{k\in\mathrm{R}}\{\gamma_{AF}^{-}\} \geq R\right\} \\ &= G(F(\lambda_{SR}\tau'), A_1 + A_2) \end{aligned} \tag{6.23}$$

Therefore, the intercept probability of one coded packet can be derived as

$$P_{I-1}^{AF+} = 1 - \sum_{T_D=1}^{\infty}\left(\varepsilon_{R,D}^{AF+}\right)^{T_D-1}\varepsilon_{R,\mathcal{D}}^{AF+} = 1 - \frac{\varepsilon_{R,\mathcal{D}}^{AF+}}{1-\varepsilon_{R,D}^{AF+}} \tag{6.24}$$

And we can obtain the upper bound of the intercept probability of the confidential data by

$$P_I^{AF+} = \left(P_{I-1}^{AF+}\right)^N \tag{6.25}$$

On the other hand, the expression of the lower band P_I^{AF-} is similar to P_I^{AF+}, and we only need to replace τ_1 with τ' and set $I_2 = I_1 - \lambda_{SD}$. Therefore, the intercept probability of the confidential data is also reduced *exponentially* as the value of N increases. The upper bound of the intercept probability can be used to decide a suitable value of N to satisfy any required security level. It is not intuitive to compare the intercept probabilities for different numbers of relays, and we will observe the tendency through the numerical results.

6.4.2 Intercept probabilities for destination based jamming

In some practical networks, the direct link between S and D is blocked such that the transmission is realized only through the help of relays. It is impossible to realize the secure transmission by DF protocol since the relays should decode the packets correctly to forward them. For the ordinary AF protocol, it is also unusable because for any relay $\mathrm{R_k}$ we have $\gamma_{Sk} \geq \frac{\gamma_{Sk}\gamma_{kD}}{1+\gamma_{Sk}+\gamma_{kD}}$. The relays can always decode the packets correctly if D does. Therefore, a scheme called destination based jamming (DBJ) [59, 64] is exploited in the literature. In this chapter, we attempt to combine the DBJ with FLCAS to realize the secure transmission regardless of the existence of the direct link. In DBJ, the transmit power P in Phase I is allocated between S and D with parameter $\alpha \in [1, 0]$. S transmits its packet with power αP and D transmits artificial noise with power $(1-\alpha)P$ simultaneously. Then the relay forwards the received superposition signal still with power P. D can subtract the artificial noise from the received signal since it is generated by itself, while the relays are confused by it. Therefore, the achievable rates at the relays and D are derived respectively as [64],

$$C_k^{DBJ} = 0.5 \log_2 \left(1 + \frac{\alpha\gamma_{Sk}}{1 + (1-\alpha)\gamma_{kD}}\right) \tag{6.26}$$

$$C_D^{DBJ} = 0.5 \log_2 \left(1 + \max_{\mathrm{R_k} \in \mathbf{R}} \left\{ \frac{\alpha\gamma_{Sk}\gamma_{kD}}{1 + \alpha\gamma_{Sk} + (2-\alpha)\gamma_{kD}} \right\}\right) \tag{6.27}$$

First, we calculate the upper bound of the intercept probability based on the following equations

$$\frac{\alpha\gamma_{Sk}\gamma_{kD}}{1+\alpha\gamma_{Sk}+(2-\alpha)\gamma_{kD}} \geq \frac{1}{(2-\alpha)}\left(\frac{1}{2}\min\left\{\alpha\gamma_{Sk},(2-\alpha)\gamma_{kD}\right\}-\frac{1}{4}\right) \quad (6.28)$$

$$\frac{\alpha\gamma_{Sk}}{1+(1-\alpha)\gamma_{kD}} < \frac{\alpha\gamma_{Sk}}{(1-\alpha)\gamma_{kD}} \quad (6.29)$$

Let's denote $X_1 = \alpha\gamma_{Sk}$ and $X_2 = (2-\alpha)\gamma_{kD}$. If $\tau_2 = \left(2^{2R}-1\right)\frac{1-\alpha}{2-\alpha} \geq 1$, we can derive that

$$\begin{aligned}\varepsilon_{R,D}^{DBJ+} &= \Pr\left\{\max_{\mathrm{R_k}\in\mathbf{R}}\left\{\frac{X_1}{X_2}\right\}<\tau_2, \max_{\mathrm{R_k}\in\mathbf{R}}\left\{\min\left\{X_1,X_2\right\}\right\}<\tau_3\right\} \\ &= G\left(\frac{\lambda_{X_2}}{\lambda_{X_2}+\lambda_{X_1}\tau_2}, \frac{\lambda_{X_1}}{I_3}F\left(I_3\tau_3\right)\right. \\ &\quad \left.+\frac{\lambda_{X_2}}{I_3}F\left(I_3\tau_3\right)-\frac{\lambda_{X_2}}{I_4}F\left(I_4\tau_3\right)\right) \end{aligned} \quad (6.30)$$

and

$$\begin{aligned}\varepsilon_{R,\text{Đ}}^{DBJ+} &= \Pr\left\{\max_{\mathrm{R_k}\in\mathbf{R}}\left\{\frac{X_1}{X_2}\right\}<\tau_2, \max_{\mathrm{R_k}\in\mathbf{R}}\left\{\min\left\{X_1,X_2\right\}\right\}\geq\tau_3\right\} \\ &= G\left(\frac{\lambda_{X_2}}{\lambda_{X_2}+\lambda_{X_1}\tau_2}, \frac{\lambda_{X_1}}{I_3}\left[1-F\left(I_3\tau_3\right)\right]\right. \\ &\quad \left.+\frac{\lambda_{X_2}}{I_3}\left[1-F\left(I_3\tau_3\right)\right]-\frac{\lambda_{X_2}}{I_4}\left[1-F\left(I_4\tau_3\right)\right]\right) \end{aligned} \quad (6.31)$$

where $\tau_3 = 2\left[\left(2^{2R}-1\right)(2-\alpha)+0.25\right]$, $\lambda_{X_1} = \lambda_{SR}\alpha^{-1}$, $\lambda_{X_2} = \lambda_{RD}(2-\alpha)^{-1}$, $I_3 = \left(\lambda_{X_1}+\lambda_{X_2}\right)(k_2+1)+\left(\lambda_{X_2}+\lambda_{X_1}\tau_2\right)(K-1-k_1-k_2)$ and $I_4 = \lambda_{X_1}\tau_2+\lambda_{X_2}+\left(\lambda_{X_1}+\lambda_{X_2}\right)k_2+\left(\lambda_{X_2}+\lambda_{X_1}\tau_2\right)(K-1-k_1-k_2)$.

On the other hand, if $\tau_2 < 1$,

$$\varepsilon_{R,D}^{DBJ+} = G'\left(1,1,\left(\frac{\lambda_{X_1}}{\lambda_{X_1}+\lambda_{X_2}/\tau_2}\right)^{K-1}\frac{\lambda_{X_1}}{I_5}\,F\left(I_5\tau_3\right)\right) \quad (6.32)$$

and

$$\varepsilon_{R,\text{Đ}}^{DBJ+} = G'\left(1, 1, \left(\frac{\lambda_{X_1}}{\lambda_{X_1}+\lambda_{X_2}/\tau_2}\right)^{K-1} \frac{\lambda_{X_1}}{I_5}\left[1 - F\left(I_5\tau_3\right)\right]\right) \tag{6.33}$$

where, $G'\left(\varsigma, \beta, \varphi\right) = K\sum_{k_1=0}^{K-1}\left[\binom{K-1}{k_1}\left(-\varsigma\right)^{k_1}\beta^{K-1-k_2}\varphi\right]$, and $I_5 = \left(\lambda_{X_1}+\lambda_{X_2}/\tau_2\right)\left(k_1+1\right)$.

Therefore, the upper bound of the intercept probability of the confidential data is

$$P_I = \left(P_{I-1}^{DBJ+}\right)^N = \left(1 - \frac{\varepsilon_{R,\text{Đ}}^{DBJ+}}{1-\varepsilon_{R,D}^{DBJ+}}\right)^N \tag{6.34}$$

To derive the lower bound of the intercept probability, the following inequality is utilized

$$\begin{aligned}\frac{\alpha\gamma_{Sk}\gamma_{kD}}{1+\alpha\gamma_{Sk}+\left(2-\alpha\right)\gamma_{kD}} &\leq \frac{1}{\left(2-\alpha\right)}\min\left\{\alpha\gamma_{Sk}, \left(2-\alpha\right)\gamma_{kD}\right\} \\ &\leq \begin{cases}\gamma_{kD}, \text{①} \text{ if } \alpha\sigma_{Sk}^2 \geq \left(2-\alpha\right)\sigma_{kD}^2 \\ \frac{\alpha\gamma_{Sk}}{\left(2-\alpha\right)}, \text{②} \text{ if } \alpha\sigma_{Sk}^2 < \left(2-\alpha\right)\sigma_{kD}^2\end{cases}\end{aligned} \tag{6.35}$$

For case ①, we can derived that

$$\begin{aligned}\varepsilon_{R,D}^{DBJ-} &= \Pr\left\{\max_{\mathrm{R_k}\in\mathbf{R}}\left\{\frac{\alpha\gamma_{Sk}}{1+\left(1-\alpha\right)\gamma_{kD}}\right\} < \tau', \max_{\mathrm{R_k}\in\mathbf{R}}\left\{\gamma_{kD}\right\} < \tau'\right\} \\ &= G\left(1 - \frac{\lambda_{RD}e^{-\lambda_{SR}\tau'/\alpha}}{I_6}, \frac{\lambda_{RD}}{I_7}F\left(I_7\tau'\right)\right. \\ &\quad \left. -\frac{\lambda_{RD}e^{-\lambda_{SR}\tau'/\alpha}}{I_8}F\left(I_8\tau'\right)\right)\end{aligned} \tag{6.36}$$

and,

$$\begin{aligned}\varepsilon_{R,\text{Đ}}^{DBJ-} &= \Pr\left\{\max_{k\in\mathrm{R}}\left\{\frac{\alpha\gamma_{Sk}}{1+\left(1-\alpha\right)\gamma_{kD}}\right\} < \tau', \max_{k\in\mathrm{R}}\left\{\gamma_{kD}\right\} \geq \tau'\right\} \\ &= G\left(1 - \frac{\lambda_{RD}e^{-\lambda_{SR}\tau'/\alpha}}{I_6}, \frac{\lambda_{RD}}{I_7}\left[1 - F\left(I_7\tau'\right)\right]\right.\end{aligned}$$

$$-\frac{\lambda_{RD}e^{-\lambda_{SR}\tau'/\alpha}}{I_8}\left[1-F\left(I_8\tau'\right)\right]\Bigg) \tag{6.37}$$

where, $I_6 = \lambda_{RD} + \lambda_{SR}\left(1-\alpha\right)\tau'/\alpha$, $I_7 = \lambda_{RD}\left(k_2+1\right) + I_6\left(K-1-k_1-k_2\right)$ and $I_8 = I_7 + \lambda_{SR}\left(1-\alpha\right)\tau'/\alpha$.

Now the attentions turn to the case ②, we can derive that

$$\begin{aligned}
\varepsilon_{R,D}^{DBJ-} &= \Pr\left\{\max_{k\in\mathrm{R}}\left\{\frac{\alpha\gamma_{Sk}}{1+\left(1-\alpha\right)\gamma_{kD}}\right\} < \tau', \max_{k\in\mathrm{R}}\left\{\frac{\alpha\gamma_{Sk}}{\left(2-\alpha\right)}\right\} < \tau'\right\} \\
&= G'\left(1,1,\frac{1}{\left(k_1+1\right)}F\left(\frac{\left(k_1+1\right)\lambda_{SR}\tau'}{\alpha}\right)\right) + \\
&\quad G'\left(I_{10},I_{11},\frac{\lambda_{SR}e^{\frac{\lambda_{SD}}{(1-\alpha)}}}{I_9\left(k_1+1\right)}\left[F\left(\frac{I_9\left(k_1+1\right)\left(2-\alpha\right)\tau'}{\alpha}\right)\right.\right. \\
&\quad \left.\left.-F\left(\frac{I_9\left(k_1+1\right)\tau'}{\alpha}\right)\right]\right)
\end{aligned} \tag{6.38}$$

and

$$\begin{aligned}
\varepsilon_{R,\not D}^{DBJ-} &= \Pr\left\{\max_{k\in\mathrm{R}}\left\{\frac{\alpha\gamma_{Sk}}{1+\left(1-\alpha\right)\gamma_{kD}}\right\} < \tau', \max_{k\in\mathrm{R}}\left\{\frac{\alpha\gamma_{Sk}}{\left(2-\alpha\right)}\right\} \geq \tau'\right\} \\
&= G'\left(I_{10},I_{11},\frac{\lambda_{SR}e^{\frac{\lambda_{SD}}{(1-\alpha)}}}{I_9\left(k_1+1\right)}\right. \\
&\quad \left.\left[1-F\left(\frac{I_9\left(k_1+1\right)\left(2-\alpha\right)\tau'}{\alpha}\right)\right]\right)
\end{aligned} \tag{6.39}$$

where, $I_9 = \lambda_{SR} + \frac{\lambda_{RD}\alpha}{(1-\alpha)\tau'}$, $I_{10} = \frac{\lambda_{SR}e^{\frac{\lambda_{RD}}{(1-\alpha)}}}{I_9}$ and
$I_{11} = F\left(\frac{\lambda_{SR}\tau'}{\alpha}\right) + I_{10}\left(1-F\left(\frac{I_9\tau'}{\alpha}\right)\right)$.

The lower bound of the intercept probability for both cases ① and ② is

$$P_I^{DBJ-} = \left(P_{I-1}^{DBJ-}\right)^N = \left(1-\frac{\varepsilon_{R,\not D}^{DBJ-}}{1-\varepsilon_{R,D}^{DBJ-}}\right)^N \tag{6.40}$$

For the combination of DBJ with FLCAS, any required security level can be also satisfied by increasing the value of N.

6.5 Numerical Results and Discussions

In this section, the numerical results are provided to validate the theoretical analysis, and some remarkable conclusions are discussed. The simulation environment is established in a rectangular coordinate system, where the source and the destination are located at (0,0) and (0,1) respectively. The position of the relays is generated between the source and the destination. Without loss of generality, path loss coefficient and ρ is set to be 3 and 20dB respectively, and $R = 1$bit/s/Hz.

The intercept probability vs. N for the DT, DF and AF relaying is shown in Fig 6.3 for $K = 1, 2$ and 3, where the locations of the relays are assumed to be the midpoint between the source and the destination, i.e., (0.5,0). It can be observed that exploiting the relays to assist the transmission achieves a better secrecy performance compared to treating them as the pure eavesdroppers. More importantly, the intercept probability reduces to zero exponentially with the values of N based on FLCAS, which can be used to realize the required security level and is the main superiority compared to the alternative schemes. However, in accordance with the research works of [64, 65], the secrecy performance is deteriorated significantly with more relays (eavesdroppers). For $K \geq 2$ it is almost impossible to make a secure transmission due to the diversity gain at the relays, which makes us expect the results of DBJ.

Fig 6.4 illustrates the results of intercept probability for the DBJ strategy[1]. Although the secrecy performance is still deteriorated with the number of the relays (eavesdroppers), adopting DBJ results in interference-limited effect on the relays and thus improves the secrecy performance dramatically. Even for a large number of relays, the intercept probability is acceptable by combining DBJ with FLCAS given large N values. The intercept probability with different locations of relays ($K = 2$ and $N = 1000$) is shown in Fig 6.5. It is observed that the intercept probability is increased as the relays approach to the source, which is also an inherent weakness of the physical layer security. However, DBJ

[1]Because of the simulation time, only the results with small N values are given. For the results with large N values, the intercept probability can be obtained based on the exponential decline principle.

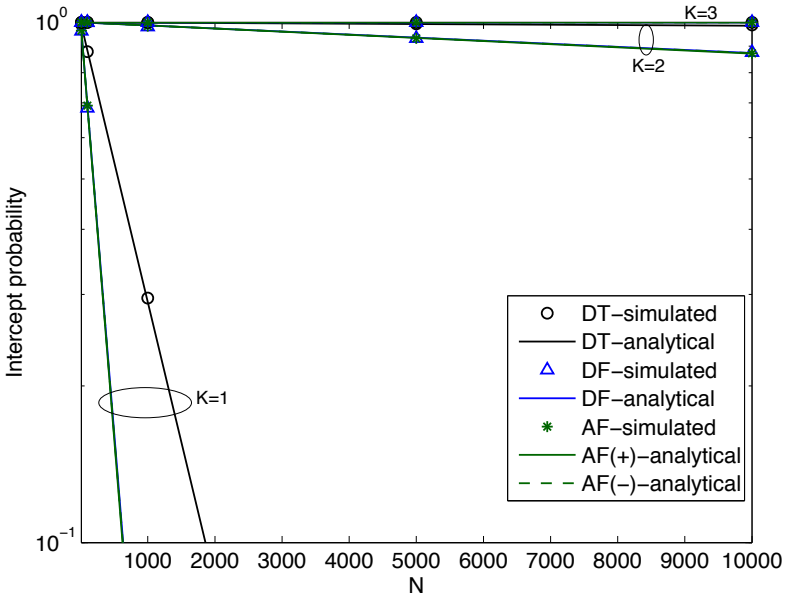

Figure 6.3: Intercept probability vs. N for the DT, DF and AF relaying

always performs much better than both the DF and AF cooperation, and also achieves an acceptable secrecy performance.

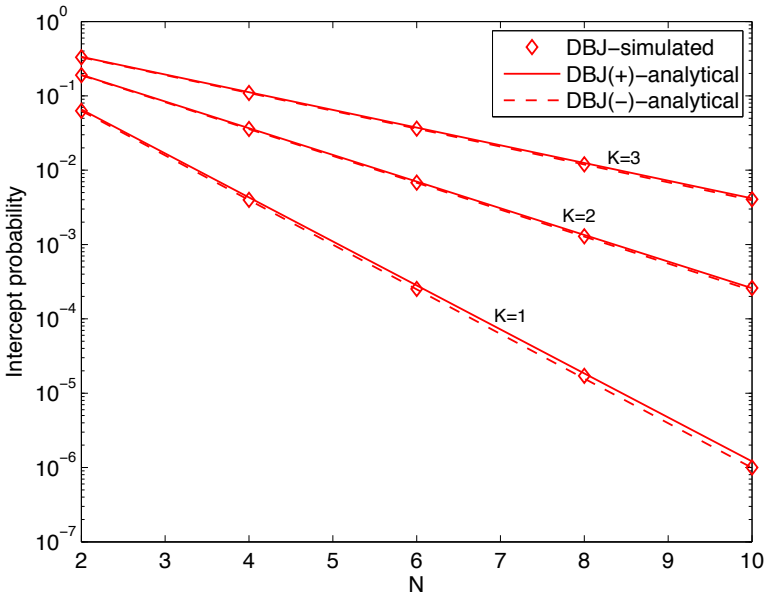

Figure 6.4: Intercept probability vs. N for the DBJ strategy

Due to its significant advantage, the DBJ is considered in the following

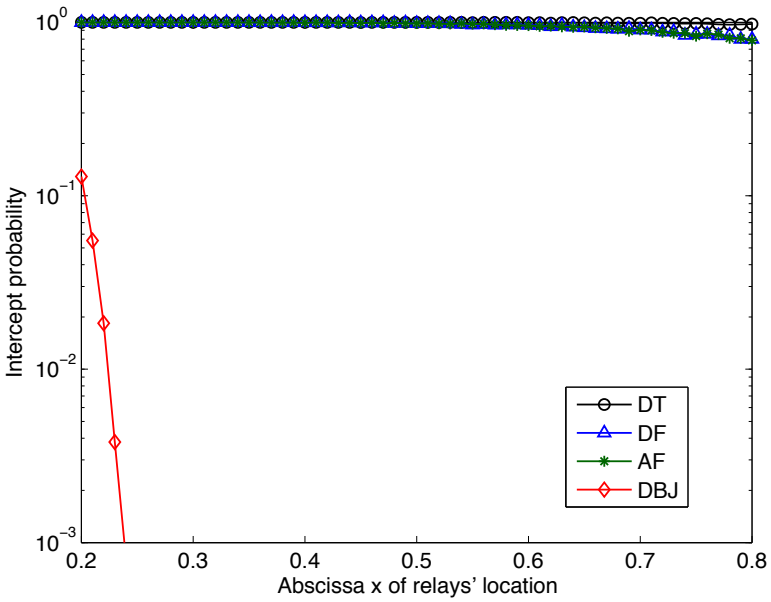

Figure 6.5: Intercept probability vs. locations of relays ($K = 2$ and $N = 1000$)

discussions. First, the simulation results for HARQ at the receivers are given in Fig 6.6. The intercept probability is nearly the same between the Basic ARQ and HARQ receivers. The one reason is that both the relays and the destination can benefit from the HARQ protocol. In addition, the worst case that the information accumulation among the relays is also considered. Although the information accumulation among the relays deteriorates the secrecy performance, the intercept probability is still reduced to zero as N increases.

In Fig 6.7, the effect of the alpha on the intercept probability is shown. It is observed that the intercept probability is decreased by reducing the value of alpha (i.e., increasing the interference caused by the jamming signal at the relays). However, reducing the value of alpha means more power is provided to generate the jamming signal and thus less power is available for the data transmission, such that the data transmission needs more time slots. To satisfy both the transmission efficiency and security requirement, the values of alpha and N should be selected jointly.

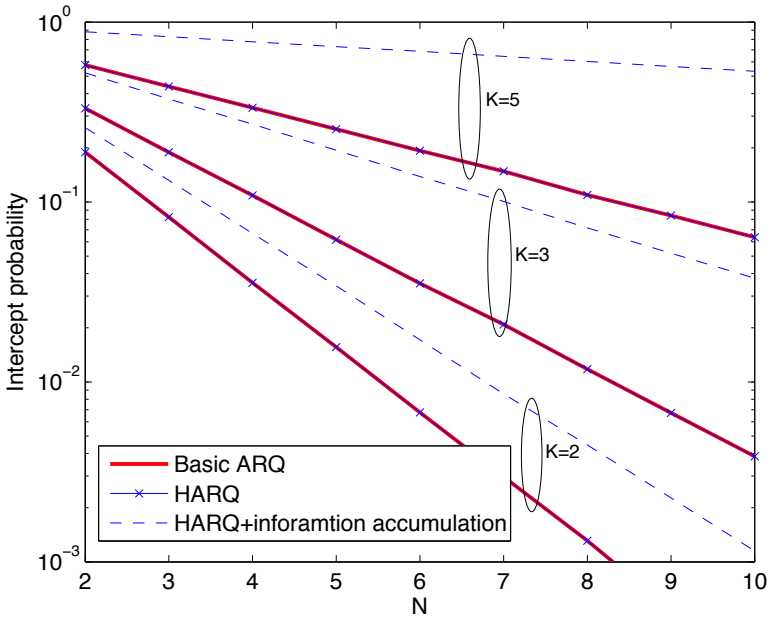

Figure 6.6: Intercept probability vs. N for the receivers with different ARQ protocols

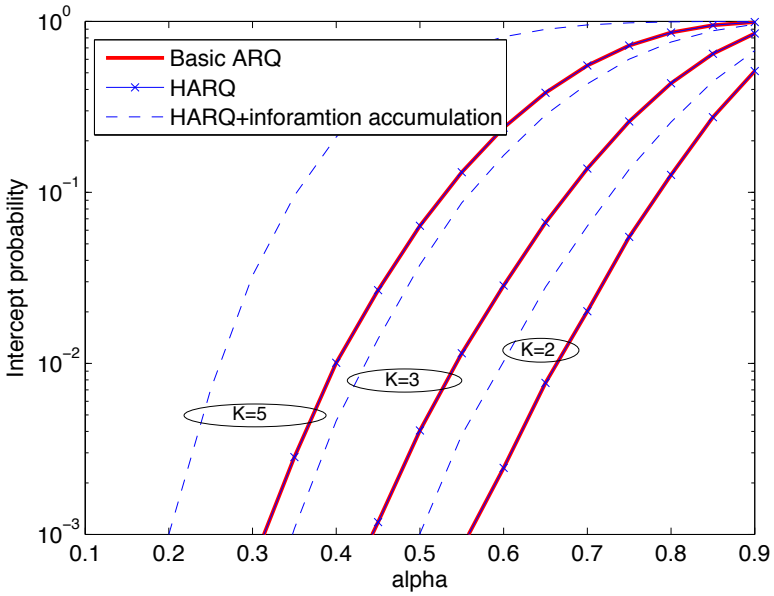

Figure 6.7: Intercept probability vs. alpha values ($N = 10$)

6.6 Comparisons of FLCAS with FCAS and Experiment Evaluations

The design of FLCAS is mainly to overcome the small quantity of data leakage caused by the randomness characteristics of fountain codes in FCAS. There are also some similarities and other differences between them, which are listed as follows.

A. Similarities

1) The data transmissions for both FCAS and FLCAS are according to the ordinary channel capacity instead of the secrecy capacity, which reduces the transmission delay.

2) The intercept probabilities for both FCAS and FLCAS are decreased to zero (near-)exponentially with increased number of source packets. That is to say, an arbitrary small intercept probability can be realized by simply increasing the number of source packets.

3) The least required complexities of both FCAS and FLCAS are linear, which does not cause much resource consumption. More importantly, the basic FCAS and FLCAS only passively employ the wireless channel fading and do not have any complicated requirements at the physical layer (e.g., channel state information at the transmitter and node synchronization). They are thus more practical and easier to be implemented compared to the regular PLS techniques.

B. Differences

1) Since the fountain codes are a kind of forward error correction codes, the data transmission based on FCAS does not require ARQ mechanism. On the other hand, the completion of data transmission based on FLCAS should utilize ARQ and/or other error control methods.

2) As shown in the second similarity, both of FCAS and FLCAS have the characteristic that the intercept probability is decreased to zero (near-)exponentially with increased number of source packets. However, FCAS holds this characteristic only when the destination has a higher packet reception rate than the eavesdroppers (/untrusted relays). If the wireless channel fading cannot ensure this requirement, other physical layer strategies like transmit power control should be combined as shown in Chapter 5. However, FLCAS always works well even when the destination does not have a higher packet reception rate than the eavesdroppers. That is to say, other physical layer strategies are

not necessary for FLCAS, although adopting them may accelerate the rate of decrease as analyzed in this chapter.

The experiments on basic FCAS and FLCAS, which only employ the wireless channel fading passively, are conducted to confirm their security features (mainly the second similarity and the second difference).

Three USRPs are used in the experiments, where one USRP (Tx) transmits the confidential data through packet based transmission and the other two USRPs (Rx1 and Rx2) act as the receivers. As shown in Fig 6.8, Tx and Rx1 are in the same room and Rx2 is outside of the room. Therefore, it is expected that Rx1 has a better channel condition, i.e., a higher packet reception rate, than Rx2.

For FCAS, considering that the required number of coded packets to recover the original data is N=10, 100 and 1000, the numbers of correctly received packets at Rx2 when Rx1 correctly receives N packets for 10 times experiments are illustrated in Fig 6.9. It can be observed that if Rx1 is the destination and Rx2 is the eavesdropper the secure transmission is realized for all the experiments. However, for the reverse case that Rx2 is the destination and Rx1 is the eavesdropper the confidential data is always intercepted. In this case, the secure transmission needs other physical layer strategies like transmit power control as discussed above.

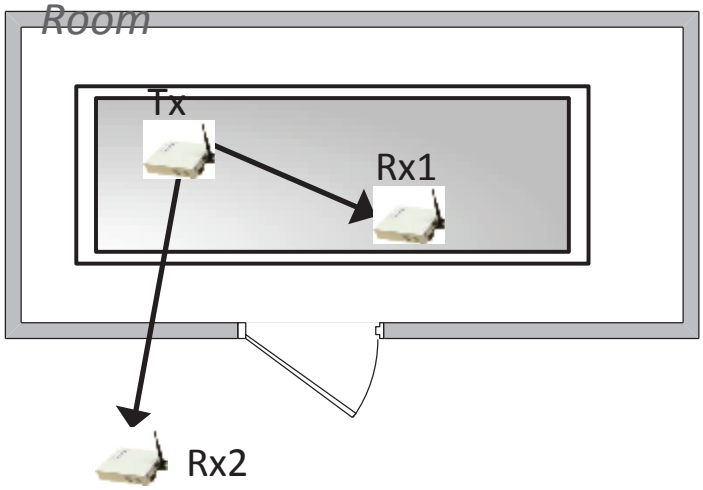

Figure 6.8: Experiment setup for FCAS and FLCAS.

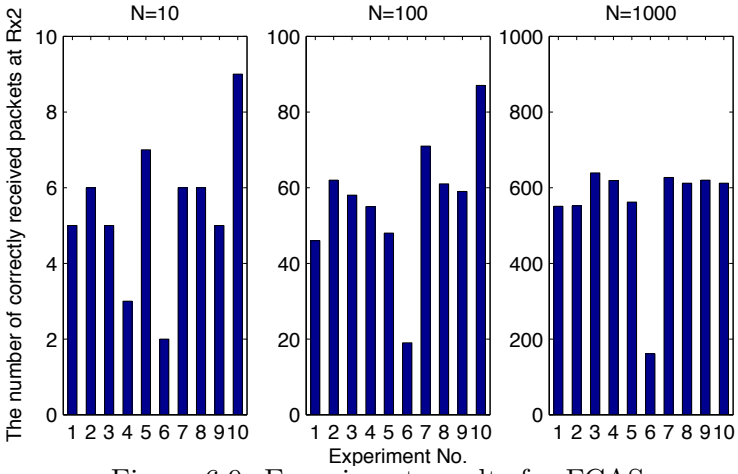

Figure 6.9: Experiment results for FCAS.

For FLCAS, the secure transmission is also realized for all the experiments if Rx1 is the destination and Rx2 is the eavesdropper, since there are always some packets that Rx1 receives correctly but Rx2 does not. If Rx2 is the destination and Rx1 is the eavesdropper, the No. of the packets that Rx2 receives correctly but Rx1 does not are listed in Table 6.1 considering N=10, 100 and 1000 packets[2]. These packets are not retransmitted again according to the ARQ mechanism, and thus Rx1 cannot obtain them forever, which makes that Rx1 is unable to recover the original data if the set of these packets is nonempty. For example, the secure transmission is realized in the 7th experiment for N=10, 1st-8th and 10th experiments for N=100 and all the experiments for N=1000. The results mean that, the secure transmission can be realized by the basic FLCAS even if the eavesdropper has a better channel condition than the destination, while the secure transmission cannot be realized by the basic FCAS in this case. Moreover, the secrecy performance is improved as the number of source packets N increases, which is consistent with the theoretical analysis.

Next, we consider that the Rx2 is the destination and Rx1 is an untrusted relay. For simplicity, the selection combining is adopted that one packet is received correctly at Rx2 if the packet through either of the links TX-Rx2 or Tx-Rx1-Rx2 is decoded correctly. Fig 6.10 shows that the number of correct-

[2]Only a part of the packets are listed for N=1000, but it is already enough to draw the conclusion.

Table 6.1: Experiment results for FLCAS

	N=10	N=100	N=1000
1	[ ]	[13 48 70 90]	[13 48 70 90 109 152 220 221...]
2	[ ]	[26 27 56 59 85]	[26 27 56 59 85 179 224 239 ...]
3	[ ]	[25 64 68 85]	[25 64 68 85 130 156 221 240 ...]
4	[ ]	[59]	[59 105 122 126 167 218 226 234 ...]
5	[ ]	[21 88]	[21 88 278 294 375 392 405 410 ...]
6	[ ]	[19 53]	[19 53 ...]
7	[10]	[10 31 50 52]	[10 31 50 52 104 105 157 176 ...]
8	[ ]	[41 67]	[41 67 152 177 181 185 207 215 ...]
9	[ ]	[ ]	[117 118 125 149 150 151 156 241 ...]
10	[ ]	[26 27 42 47 55...]	[26 27 42 47 55 56 59 64 ...]

ly received packets at Rx2 when the untrusted relay Rx1 receives N packets correctly for 10 times experiments. It is observed that the number of correctly received packets at Rx2 is increased via the cooperation by Rx1. However, the secure transmission is still impossible for the basic FCAS, since Rx1 receives enough packets faster than Rx2. And other physical layer strategies should be combined in this case. On the other hand, the basic FLCAS is constantly workable based on the Table 6.1, because there are always some packets which cannot obtained by the Rx1. Therefore, we can use FLCAS to resist untrusted relays even if no additional physical layer strategies are expected to be embedded.

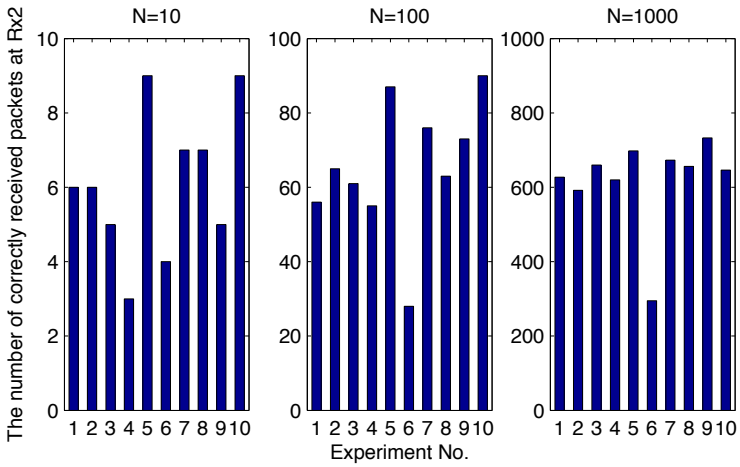

Figure 6.10: Experiment results for FCAS when treating Rx1 as the untrusted relay.

6.7 Summary

A fixed linear code assisted security (FLCAS) scheme is designed in this chapter to resist untrusted relays in the cooperative networks. The FLCAS is based on the idea of utilizing the original packets to encrypt each other as the secret keys, such that the receivers need to receive all of the coded packets to recover the original data. The security is realized if the eavesdroppers (untrusted relays) cannot obtain all of the coded packets due to the physical characteristics of the wireless channels. From the theoretical analysis and numerical results, it is observed that the intercept probability is reduced to zero exponentially with the number of the original packets, and exploiting the cooperation provided by these untrusted relays achieves a better secrecy performance than direct transmission. However, the rate of decrease is slow for a large number of untrusted relays. To solve this problem, the destination based jamming strategy is introduced and a faster rate of decrease is realized. The comparisons of FLCAS with FCAS and the results of experiment evaluations are presented at last.

Chapter 7

Conclusions and Future Work

This thesis focuses on the secrecy-enhanced data transmission for cooperative relay networks. Based on the concept of physical layer security (PLS), both the external eavesdropping attack caused by the pure eavesdropper and the internal eavesdropping attack caused by the untrusted relays are considered.

For the external eavesdropping attack, the opportunistic cooperative relaying is exploited to improve the secrecy performance (which is named cooepratve security). The essence of the cooperative relaying is to provide independent diversity links. Accordingly, the secrecy performance through these links are also independent and time-varying with the channel fading. For every transmission, if the diversity link with the best secrecy performance is utilized, the enhancement of PLS is realized. Based on this idea, I finished the following three works in the first part of this thesis.

In Chapter 2, the two-user cooperation under external eavesdropping is analyzed within the framework of game theory. Since both the destination and the eavesdropper can combine the signals of the direct link and the relaying link, both of them benefit from the conventional cooperation. The secrecy performance is actually deteriorated by the cooperation if the eavesdropper gets more diversity gain, and users are not willing to cooperate with each other in this case. Therefore, we design an opportunistic user cooperation scheme (OUCS) to consistently achieve a higher secrecy performance than the direct transmission. Specifically, if the channel quality of the direct link is better

than the relaying link between the source and the destination, the direct data transmission is performed; otherwise, the source transmits the data to the destination through the relaying link. As a result, only the destination is expected to harvest the diversity gain, which improves the secrecy performance.

In Chapter 3, the OUCS is extended to multi-user cooperation scenarios to achieve the secrecy outage performance with full diversity. The Chapter 2 solves the problem of whether to cooperate under eavesdropping attack, based on which we further consider the problem of with whom to cooperate in Chapter 3. The secrecy-providing capability (SPC) is first defined for both the source and the cooperative relays assuming different channel knowledge of the eavesdropping links. By comparing the values of SPC of these nodes, the transmission link with the best secrecy performance can be selected from the direct link and relaying links. Theoretical analysis and numerical results validate that the OUCS can realize the full secrecy diversity performance, which cannot ensured by the alternatives in the literature. In addition, the application of OUCS for another form of multi-user cooperation where multiple sources share a dedicated relay is also analyzed, from which the superiority of the OUCS is confirmed again.

In Chapter 4, the cooperative security in a kind of specific sensor networks - wireless body area networks (WBANs) is investigated. Due to the severe path loss caused by the human body, we neglect the direct link in OUCS and only consider the relaying links if the cooperative relaying is performed. The secrecy outage probabilities for the direct transmission and the cooperative relaying are derived respectively. It is found that, besides to improve the reliability and efficiency, the cooperative relaying is also an effective strategy to enhance the secrecy performance of the data transmission in WBANs.

For the internal eavesdropping attack, the code assisted security is studied. The theory of code assisted security is to process the original packets to be related packets first by a coding scheme, such that the receivers need a sufficient number of coded packets to recover the original data. The secure transmission is achieved if the destination correctly receives enough coded packets earlier than the eavesdroppers (/untrusted relays), which can be realized through the

physical characteristics of the wireless channels.

In Chapter 5, the fountain code assisted security (FCAS) is proposed and utilized to resist an untrusted relay. The fountain codes have the inherent characteristics that a sufficient number of fountain packets are required at the receivers for the recovery of the original data. We exploit the channel fading and transmit power control to make a higher packet reception rate at the destination, and thus the secure transmission can be achieved. The intercept probability is proved to be decreased to zero (near-)exponentially with the number of the original packets, which is a particular advantage compared to other regular PLS techniques. That is to say, any required security level can be satisfied by simply adjusting the number of the original packets. In addition, the data transmission is according to the original channel capacity instead of the secrecy capacity, which also reduces the data transmission delay.

In Chapter 6, a fixed linear code assisted security (FLCAS) scheme based on FCAS is designed, and the application of it for resisting multiple untrusted relays is analyzed. Due to the randomness characteristics of fountain codes, the FCAS proposed in Chapter 5 still results in a small quantity of data leakage. Therefore, we revise the FCAS and use a fixed linear code to carry out the information self-encryption. It outperforms the fountain codes in terms of secrecy performance but with the same linear complexity. The application of FLCAS for protecting from the internal eavesdropping attack caused by multiple untrusted relays is then studied. The advantages of FCAS are still maintained, especially that the intercept probability is decreased to zero as the number of the original packets increases. In addition, the destination based jamming strategy is introduced to further accelerate the rate of decrease. The comparisons of FLCAS with FCAS and experiment evaluations are also given in this chapter.

In future, we will mainly continue to research on the code assisted security, since its complexity is relatively low and the application of it is more practical. Besides finding new coding schemes, other potential research directions include applying it in different scenarios and combining it with different data transmission techniques. For example, it can be further used to protect from the

external eavesdropping attack for cooperative relay networks. The employment of it in resource-limited sensor networks is feasible due to its low complexity. The combination of it with existing and future data transmission techniques, e.g., OFDM and Massive MIMO, should be also valuable. Moreover, the application of our proposed secrecy-enhanced data transmission schemes from an engineering point of view will be considered, such as the implementations of OUCS in mobile networks and the code assisted security for delay-constrained services.

Appendices

Appendix A

Derivations in Chapter 2

A.1 The utilities of user 1 for strategy profiles with the conventional cooperation

The cumulative distribution function (CDF) and probability density function (PDF) for the sum of two independent exponential random variables are derived first. Given two independent exponential random variables z_1 with parameter λ_1 and z_2 with parameter λ_2, $z = z_1 + z_2$ meets the following distributions:

$$\begin{aligned} F(z) &= \int_0^z \lambda_1 e^{-\lambda_1 x}(1 - e^{-\lambda_2(z-x)})dx \\ &= \begin{cases} 1 + \frac{\lambda_2}{\lambda_1 - \lambda_2} e^{-\lambda_1 z} - \frac{\lambda_1}{\lambda_1 - \lambda_2} e^{-\lambda_2 z}, \lambda_1 \neq \lambda_2 \\ 1 - e^{-\lambda_1 z} - \lambda_1 z e^{-\lambda_1 z}, \lambda_1 = \lambda_2 \end{cases} \end{aligned}$$

$$\begin{aligned} f(z) &= F'(z) \\ &= \begin{cases} \frac{-\lambda_1 \lambda_2}{\lambda_1 - \lambda_2} e^{-\lambda_1 z} + \frac{\lambda_1 \lambda_2}{\lambda_1 - \lambda_2} e^{-\lambda_2 z}, \lambda_1 \neq \lambda_2 \\ \lambda_1^2 z e^{-\lambda_1 z}, \lambda_1 = \lambda_2 \end{cases} \end{aligned}$$

where, $F(\cdot)$ and $f(\cdot)$ denote CDF and PDF respectively. The channel gain $|h_{ij}|^2$ for the Rayleigh fading is exponentially distributed. Therefore,

$$\begin{aligned}
u_1\left(\frac{\rho_1}{2},\frac{\rho_2}{2}\right) &= \Pr\left\{\frac{1}{2}\log_2\left(\frac{\frac{\rho_1}{2}|h_{1D}|^2+\frac{\rho_2}{2}|h_{2D}|^2}{\frac{\rho_1}{2}|h_{1E}|^2+\frac{\rho_2}{2}|h_{2E}|^2}\right)\geq R_s\right\}\\
&= \Pr\left\{\frac{|h_{1D}|^2+|h_{2D}|^2}{|h_{1E}|^2+|h_{2E}|^2}\geq 2^{2R_s}\triangleq\delta^2\right\}\\
&= \int_0^\infty \lambda_{sd}^2 z e^{-\lambda_{sd}z}(1-e^{-\lambda_{se}z/\delta^2}-\lambda_{se}z e^{-\lambda_{se}z/\delta^2})dz\\
&= \frac{3\lambda_{sd}(\lambda_{se}/\delta^2)^2+(\lambda_{se}/\delta^2)^3}{(\lambda_{sd}+\lambda_{se}/\delta^2)^3} = \frac{3\xi+1}{(\xi+1)^3}
\end{aligned}$$

$$\begin{aligned}
u_1\left(\rho_1,\frac{\rho_2}{2}\right) &= \Pr\left\{\frac{1}{2}\log_2\left(\frac{\rho_1|h_{1D}|^2+\frac{\rho_2}{2}|h_{2D}|^2}{\rho_1|h_{1E}|^2+\frac{\rho_2}{2}|h_{2E}|^2}\right)\geq R_s\right\}\\
&= \int_0^\infty\left(\frac{-\lambda_{sd}2\lambda_{sd}}{\lambda_{sd}-2\lambda_{sd}}e^{-\lambda_{sd}z}+\frac{\lambda_{sd}2\lambda_{sd}}{\lambda_{sd}-2\lambda_{sd}}e^{-2\lambda_{sd}z}\right)\\
&\left(1+\frac{2\lambda_{se}}{\lambda_{se}-2\lambda_{se}}e^{-\lambda_{se}z/\delta^2}-\frac{\lambda_{se}}{\lambda_{se}-2\lambda_{se}}e^{-2\lambda_{se}z/\delta^2}\right)dz\\
&= \frac{7\xi+2}{(\xi+1)(\xi+2)(2\xi+1)}
\end{aligned}$$

$$\begin{aligned}
u_1\left(\frac{\rho_1}{2},0\right) &= \Pr\left\{\log_2\left(\frac{\frac{\rho_1}{2}|h_{1D}|^2}{\frac{\rho_1}{2}|h_{1E}|^2}\right)\geq R_s\right\}\\
&= \int_0^\infty \lambda_{sd}e^{-\lambda_{sd}z}(1-e^{-\lambda_{se}z/\delta})dz\\
&= \frac{\lambda_{se}/\delta}{\lambda_{sd}+\lambda_{se}/\delta} = \frac{1}{\xi/\delta+1}
\end{aligned}$$

$$\begin{aligned}
u_1(\rho_1,0) &= \Pr\left\{\log_2\left(\frac{\rho_1|h_{1D}|^2}{\rho_1|h_{1E}|^2}\right)\geq R_s\right\}\\
&= \frac{\lambda_{se}/\delta}{\lambda_{sd}+\lambda_{se}/\delta} = \frac{1}{\xi/\delta+1}
\end{aligned}$$

where, $\lambda_{sd(e)} = \frac{1}{\sigma^2_{sd(e)}}$ and $\xi = \frac{\lambda_{sd}}{\lambda_{se}/\delta^2} = \frac{\sigma^2_{se}\delta^2}{\sigma^2_{sd}}$ with $\delta = 2^{R_s}$.

A.2 The utilities of user 1 for strategy profiles with the OUCS

If user 2 does not provide cooperation, the utilities of user 1 are the same as the results of Appendix A.1, i.e., $u_1\left(\frac{\rho_1}{2}, 0\right) = u_1\left(\rho_1, 0\right) = \frac{1}{\xi/\delta+1}$. If user 2 chooses to cooperate, the utilities of user 1 are derived as follows,

$$
\begin{aligned}
& u_1\left(\frac{\rho_1}{2}, \frac{\rho_2}{2}\right) = u_1\left(\rho_1, \frac{\rho_2}{2}\right) \\
= \;& 1 - \Pr(|h_{1D}|^2 \geq a \min\left\{|h_{in}|^2, |h_{2D}|^2\right\}, \\
& \qquad \log_2\left(\frac{|h_{1D}|^2}{|h_{1E}|^2}\right) < R_s) \\
& - \Pr(|h_{1D}|^2 < a \min\left\{|h_{in}|^2, |h_{2D}|^2\right\}, \\
& \qquad \frac{1}{2}\log_2\left(\min\left\{\frac{|h_{in}|^2}{|h_{1E}|^2}, \frac{|h_{2D}|^2}{|h_{2E}|^2}\right\}\right) < R_s) \\
= \;& 1 - \int_0^\infty \lambda_{sd} e^{-\lambda_{sd} z}\left[1 - e^{-(\lambda_{in}+\lambda_{sd})z/a}\right] e^{-\lambda_{se} z/\delta} dz \\
& - \Bigg[\int_0^\infty \lambda_{sd} e^{-\lambda_{sd} z}\left(\int_{z/a}^\infty \lambda_{in} e^{-\lambda_{in} x} e^{-\lambda_{se} x/\delta^2} dx \right. \\
& \qquad \int_{z/a}^\infty \lambda_{sd} e^{-\lambda_{sd} y} dy \\
& \qquad + \int_{z/a}^\infty \lambda_{in} e^{-\lambda_{in} x} dx \int_{z/a}^\infty \lambda_{sd} e^{-\lambda_{sd} y} e^{-\lambda_{se} y/\delta^2} dy \\
& \qquad - \int_{z/a}^\infty \lambda_{in} e^{-\lambda_{in} x} e^{-\lambda_{se} x/\delta^2} dx \\
& \qquad \left.\int_{z/a}^\infty \lambda_{sd} e^{-\lambda_{sd} y} e^{-\lambda_{se} y/\delta^2} dy\right) dz\Bigg] \\
\overset{a=\frac{1}{\delta}}{=} \;& \frac{1}{\xi/\delta+1} + \Phi
\end{aligned}
$$

where $\Phi = \frac{\xi^2+2\xi\delta+\xi\xi'\delta+\xi^2\delta(1-\xi')}{(\xi+1)(\xi'+1)(\xi+\xi\delta+\xi'\delta+\delta)(\xi+\xi\delta+\xi'\delta+2\delta)}$ and $\xi' = \frac{\lambda_{in}}{\lambda_{se}/\delta^2} = \frac{\sigma^2_{se}\delta^2}{\sigma^2_{in}}$.

Appendix B

Derivations in Chapter 3

B.1 Diversity order analysis of P_{out}^{A-up}

Eq. (3.9) can be divided into different parts based on "+" and "−" operations,

$$\begin{aligned}
P_{out}^{A-up1} &= \int_0^\infty \prod_{n=1}^{N} \left[(\lambda_{Sn}+\lambda_{nD})x\right] \lambda_{SD} e^{-\lambda_{SD}x} e^{-\lambda_{SE}\frac{x}{2^{2R_s}}} dx \\
&= \prod_{n=1}^{N} \left[(\lambda_{Sn}+\lambda_{nD})\right] \lambda_{SD} \frac{\Gamma(N+1)}{\left(\lambda_{SD}+\frac{\lambda_{SE}}{2^{2R_s}}\right)^{N+1}} \\
&= \prod_{n=1}^{N} \left(\frac{1}{c_{Sn}\sigma_{SD}^2}+\frac{1}{c_{nD}\sigma_{SD}^2}\right) \frac{1}{\sigma_{SD}^2} \frac{\Gamma(N+1)}{\left(\frac{1}{\sigma_{SD}^2}+\frac{1}{2^{2R_s}\sigma_{SE}^2}\right)^{N+1}} \\
&= \left(\frac{1}{\delta_{de}}\right)^{N+1} \prod_{n=1}^{N} \left(\frac{1}{c_{Sn}}+\frac{1}{c_{nD}}\right) \frac{\Gamma(N+1)}{\left(\delta_{de}^{-1}+a\right)^{N+1}}
\end{aligned}$$

$$\begin{aligned}
P_{out}^{A-up2} &= \sum_{n=1}^{N} \int_0^\infty \lambda_{SD} x \prod_{\substack{m=1 \\ m\neq n}}^{N} \left[(\lambda_{Sm}+\lambda_{mD})x\right] \\
&\quad \lambda_{Sn} e^{-\lambda_{Sn}x} e^{-\lambda_{SE}\frac{x}{2^{2R_s}}} e^{-\lambda_{nD}x} dx \\
&= \left(\frac{1}{\delta_{de}}\right)^{N+1} \sum_{n=1}^{N} \frac{1}{c_{Sn}} \prod_{\substack{m=1 \\ m\neq n}}^{N} \left(\frac{1}{c_{Sm}}+\frac{1}{c_{mD}}\right)
\end{aligned}$$

$$\frac{\Gamma(N+1)}{\left[\left(\frac{1}{c_{Sn}}+\frac{1}{c_{nD}}\right)\delta_{de}^{-1}+a\right]^{N+1}}$$

$$\begin{aligned}
P_{out}^{A-up3} &= \sum_{n=1}^{N}\int_0^\infty \lambda_{SD}x\prod_{\substack{m=1\\m\neq n}}^{N}[(\lambda_{Sm}+\lambda_{mD})x]\lambda_{Sn}e^{-\lambda_{Sn}x} \\
&\quad \int_x^\infty \lambda_{nD}e^{-\lambda_{nD}y}e^{-\lambda_{nE}\frac{y}{2^{2R_s}}}dydx \\
&= \left(\frac{1}{\delta_{de}}\right)^{N+2}\sum_{n=1}^{N}\frac{1}{c_{Sn}c_{nD}}\prod_{\substack{m=1\\m\neq n}}^{N}\left(\frac{1}{c_{Sm}}+\frac{1}{c_{mD}}\right) \\
&\quad \frac{\Gamma(N+1)}{\left(\frac{1}{c_{nD}}\delta_{de}^{-1}+\frac{a}{c_{nE}}\right)\left[\left(\frac{1}{c_{Sn}}+\frac{1}{c_{nD}}\right)\delta_{de}^{-1}+\frac{a}{c_{nE}}\right]^{N+1}}
\end{aligned}$$

$$\begin{aligned}
P_{out}^{A-up4} &= \sum_{n=1}^{N}\int_0^\infty \lambda_{SD}x\prod_{\substack{m=1\\m\neq n}}^{N}[(\lambda_{Sm}+\lambda_{mD})x]\lambda_{Sn}e^{-\lambda_{Sn}x} \\
&\quad e^{-\lambda_{SE}\frac{x}{2^{2R_s}}}\int_x^\infty \lambda_{nD}e^{-\lambda_{nD}y}e^{-\lambda_{nE}\frac{y}{2^{2R_s}}}dydx \\
&= \left(\frac{1}{\delta_{de}}\right)^{N+2}\sum_{n=1}^{N}\frac{1}{c_{Sn}c_{nD}}\prod_{\substack{m=1\\m\neq n}}^{N}\left(\frac{1}{c_{Sm}}+\frac{1}{c_{mD}}\right) \\
&\quad \frac{\Gamma(N+1)}{\left(\frac{1}{c_{nD}}\delta_{de}^{-1}+\frac{a}{c_{nE}}\right)\left[\left(\frac{1}{c_{Sn}}+\frac{1}{c_{nD}}\right)\delta_{de}^{-1}+\left(1+\frac{1}{c_{nE}}\right)a\right]^{N+1}}
\end{aligned}$$

where, $a=\frac{1}{2^{2R_s}}$. The results of the last three parts of Eqn (3.9) are similar to P_{out}^{A-up2}, P_{out}^{A-up3} and P_{out}^{A-up4} respectively. Therefore,

$$\begin{aligned}
d_{secrery}^{A-up} &= \min\left\{-\lim_{\delta_{de}\to\infty}\frac{\log(P_{out}^{A-up1})}{\log(\delta_{de})}, -\lim_{\delta_{de}\to\infty}\frac{\log(P_{out}^{A-up2})}{\log(\delta_{de})}, ...\right\} \\
&= N+1
\end{aligned}$$

Appendix C

Derivations in Chapter 6

C.1 Derivations of $\varepsilon_{R,D}^{AF+}$

Denoting the relay selected to cooperate is $\dot{k}$, the derivation of $\varepsilon_{R,D}^{AF+}$ can be divided into two parts: 1) $\gamma_{S\dot{k}} \leq \gamma_{\dot{k}D}$; 2) $\gamma_{S\dot{k}} > \gamma_{\dot{k}D}$, and

$$\varepsilon_{R,D}^{AF+} = \varepsilon_{R,D(1)}^{AF+} + \varepsilon_{R,D(2)}^{AF+} \tag{C.1}$$

Correspondingly,

$$\begin{aligned}
\varepsilon_{R,D(1)}^{AF+} &= \sum_{\dot{k}=1}^{K} \Pr\left\{ \max_{k\in \mathrm{R}} \{\gamma_{Sk}\} < \tau', \gamma_{SD} + \frac{1}{2}\gamma_{S\dot{k}} < \tau_1, \gamma_{S\dot{k}} \leq \gamma_{\dot{k}D} \right\} \\
&= \sum_{\dot{k}=1}^{K} \int_0^{\tau'} \lambda_{S\dot{k}} e^{-\lambda_{S\dot{k}} x} e^{-\lambda_{\dot{k}D} x} \left[1 - e^{-\lambda_{SD}(\tau_1 - \frac{1}{2}x)}\right] \\
&\quad \prod_{k'\in\{1,\ldots,K\}-\{\dot{k}\}} \left(\int_0^x \lambda_{Sk'} e^{-\lambda_{Sk'} y} e^{-\lambda_{k'D} y} dy + \right. \\
&\quad \left. \int_0^x \lambda_{k'D} e^{-\lambda_{k'D} y} \int_y^{\tau'} \lambda_{Sk'} e^{-\lambda_{Sk'} z} dz dy \right) dx \\
&= K \int_0^{\tau'} \lambda_{SR} e^{-\lambda_{SR} x} e^{-\lambda_{RD} x} \left[1 - e^{-\lambda_{SD}(\tau_1 - \frac{1}{2}x)}\right] \\
&\quad \left[1 - e^{-\lambda_{SR}\tau'} - e^{-(\lambda_{SR}+\lambda_{RD})x} + e^{-\lambda_{SR}\tau' - \lambda_{RD}x}\right]^{K-1} dx
\end{aligned}$$

$$= G\left(F\left(\lambda_{SR}\tau'\right), \frac{\lambda_{SR}}{I_1}F\left(I_1\tau'\right) - A_1\right) \tag{C.2}$$

where,

$$G\left(\alpha,\beta\right) = K\sum_{k_1=0}^{K-1}\sum_{k_2=0}^{K-1-k_1}\left[\begin{pmatrix} K-1 \\ k_1 \end{pmatrix} \begin{pmatrix} K-1-k_1 \\ k_2 \end{pmatrix}\alpha^{k_1}\left(-1\right)^{k_2}\left(1-\alpha\right)^{K-1-k_1-k_2}\beta\right]$$

$F\left(\chi\right) = 1-\exp\left(-\chi\right)$, $I_1 = \left(\lambda_{SR}+\lambda_{RD}\right)\left(k_2+1\right)+\lambda_{RD}\left(K-1-k_1-k_2\right)$, $I_2 = I_1 - 0.5\lambda_{SD}$, $\tau_1 = 2^{2R}-0.75$ and,

$$A_1 = \begin{cases} \lambda_{SR}\left[1-F(\lambda_{SD}\tau_1)\right]\tau', I_2 = 0 \\ \frac{\lambda_{SR}[1-F(\lambda_{SD}\tau_1)]}{I_2}F\left(I_2\tau'\right), else \end{cases}$$

Similarly, we can derive that

$$\begin{aligned} \varepsilon_{R,D(2)}^{AF+} &= \sum_{k=1}^{K}\Pr\left\{\max_{k\in\mathrm{R}}\left\{\gamma_{Sk}\right\} < \tau', \gamma_{SD}+\frac{1}{2}\gamma_{kD} < \tau_1, \gamma_{Sk} > \gamma_{kD}\right\} \\ &= G\left(F\left(\lambda_{SR}\tau'\right), \frac{\lambda_{RD}}{I_1-\lambda_{SR}}\left[F\left(\lambda_{SR}\tau'\right) - \frac{\lambda_{SR}}{I_1}F\left(I_1\tau'\right)\right] - A_2\right) \end{aligned} \tag{C.3}$$

where,

$$A_2 = \begin{cases} \frac{\lambda_{RD}[1-F(\lambda_{SD}\tau_1)]}{\lambda_{SR}}\left[F(\lambda_{SR}\tau')\right. \\ \quad \left.-\lambda_{SR}\tau'\exp\left(-\lambda_{SR}\tau'\right)\right], I_2-\lambda_{SR}=0 \\ \frac{\lambda_{RD}[1-F(\lambda_{SD}\tau_1)]}{I_2-\lambda_{SR}}\left[F\left(\lambda_{SR}\tau'\right)-\lambda_{SR}\tau'\right], I_2 = 0 \\ \frac{\lambda_{RD}[1-F(\lambda_{SD}\tau_1)]}{I_2-\lambda_{SR}}\left[F\left(\lambda_{SR}\tau'\right)-\frac{\lambda_{SR}}{I_2}F\left(I_2\tau'\right)\right], else \end{cases}$$

Then, the $\varepsilon_{R,D}^{AF}$ is obtained by combining Eqn (C.1), (C.2) and (C.3).

Bibliography

[1] John G Proakis and Masoud Salehi. *Digital communications, 5th edition*. McGraw-Hill, 2007.

[2] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[3] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[4] Andrea Goldsmith. *Wireless communications*. Cambridge university press, 2005.

[5] Da-Shan Shiu, Gerard J Foschini, Michael J Gans, and Joseph M Kahn. Fading correlation and its effect on the capacity of multielement antenna systems. *Communications, IEEE Transactions on*, 48(3):502–513, 2000.

[6] Thomas R Derryberry, Steven D Gray, Mihai D Ionescu, Giridhar Mandyam, and Balaji Raghothaman. Transmit diversity in 3g cdma systems. *Communications Magazine, IEEE*, 40(4):68–75, 2002.

[7] Christopher Cox. *An introduction to LTE: LTE, LTE-advanced, SAE and 4G mobile communications*. John Wiley & Sons, 2012.

[8] Lucent Technologies. Enhancements for hsdpa using multiple antennas. ftp://www.3gpp.org/tsg_ran/WG1_RL1/TSGR1_15/Docs/PDFs/R1-00-1057.pdf. Accessed Novermber 15, 2015.

[9] 3GPP TR 25.996 V12.0.0. Spatial channel model for multiple input multiple output (mimo) simulations. http://www.etsi.org/deliver/etsi_tr/125900_125999/125996/12.00.00_60/. Accessed Novermber 15, 2015.

[10] Cisco Systems. Multipath and diversity. http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/27147-multipath.html. Accessed Novermber 15, 2015.

[11] Tyco Electronics Corporation. White paper: Distributed antenna systems and mimo technology. http://www.te.com/usa-en/industries/das/insights/distributed-antenna-systems-and-mimo-technology.html. Accessed Novermber 15, 2015.

[12] Antenna-theory.com. Diversity cell phone antenna design. http://www.antenna-theory.com/design/diversity.php. Accessed Novermber 15, 2015.

[13] CJ Reddy and G Gampala. Antenna design considerations for lte mobile applications. *Long Island Chapter of the IEEE Antennas & Propagation Society*, 2011, http://www.ieee.li/pdf/viewgraphs/antenna_design_lte.pdf. Accessed Novermber 15, 2015.

[14] TechInsights. Cutting-edge smartphones: A teardown comparison of the apple iphone 5 a1428, nokia lumia 920, and samsung galaxy s4 gt-i9505. https://www.techinsights.com/uploadedFiles/Public_Website/Content_-_Primary/Marketing/2013/Cutting-Edge_Smartphones/Report/Special-Project-Report-Teardown-Comparison-062013.pdf. Accessed Novermber 15, 2015.

[15] Andrew Sendonaris, Elza Erkip, and Behnaam Aazhang. User cooperation diversity. part i. system description. *Communications, IEEE Transactions on*, 51(11):1927–1938, 2003.

[16] J Nicholas Laneman, David NC Tse, and Gregory W Wornell. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *Information Theory, IEEE Transactions on*, 50(12):3062–3080, 2004.

[17] Jonathan Rodriguez. *Fundamentals of 5G Mobile Networks*. John Wiley & Sons, 2015.

[18] Nikolaj Marchenko, Torsten Andre, Guenther Brandner, Wasif Masood, and Christian Bettstetter. An experimental study of selective cooperative relaying in industrial wireless sensor networks. *Industrial Informatics, IEEE Transactions on*, 10(3):1806–1816, 2014.

[19] Dusit Niyato and Ping Wang. Cooperative transmission for meter data collection in smart grid. *Communications Magazine, IEEE*, 50(4):90–97, 2012.

[20] Suhail Al-Dharrab, Mustafa Uysal, and Tolga M Duman. Cooperative underwater acoustic communications. *Communications Magazine, IEEE*, 51(7):146–153, 2013.

[21] Thomas M Cover and Abbas El Gamal. Capacity theorems for the relay channel. *Information Theory, IEEE Transactions on*, 25(5):572–584, 1979.

[22] Anders Høst-Madsen and Junshan Zhang. Capacity bounds and power allocation for wireless relay channels. *Information Theory, IEEE Transactions on*, 51(6):2020–2040, 2005.

[23] Deqiang Chen and J Nicholas Laneman. Modulation and demodulation for cooperative diversity in wireless systems. *Wireless Communications, IEEE Transactions on*, 5(7):1785–1794, 2006.

[24] Tairan Wang, Alfonso Cano, Georgios B Giannakis, and J Nicholas Laneman. High-performance cooperative demodulation with decode-and-forward relays. *Communications, IEEE Transactions on*, 55(7):1427–1438, 2007.

[25] IEEE WG802.16 Braodband Wireless Access Working Group. Ieee standard for air interface for broadband wireless access systems. 2012.

[26] TR 36.819 3GPP. Coordinated multi-point operation for lte physical layer aspects. 2011.

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

[28] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *Information Theory, IEEE Transactions on*, 24(3):339–348, 1978.

[29] Joao Barros and Miguel RD Rodrigues. Secrecy capacity of wireless channels. In *Information Theory, 2006 IEEE International Symposium on*, pages 356–360. IEEE, 2006.

[30] Praveen Kumar Gopala, Lifeng Lai, and Hesham El Gamal. On the secrecy capacity of fading channels. *Information Theory, IEEE Transactions on*, 54(10):4687–4698, 2008.

[31] Yi-Sheng Shiu, Shih Yu Chang, Hsiao-Chun Wu, Scott C-H Huang, and Hsiao-Hwa Chen. Physical layer security in wireless networks: a tutorial. *Wireless Communications, IEEE*, 18(2):66–74, 2011.

[32] Walid Saad, Xiangyun Zhou, Merouane Debbah, and H Vincent Poor. Wireless physical layer security: Part 1 [guest editorial]. *Communications Magazine, IEEE*, 53(6):15–15, 2015.

[33] Ashish Khisti and Gregory W Wornell. Secure transmission with multiple antennas i: The misome wiretap channel. *Information Theory, IEEE Transactions on*, 56(7):3088–3104, 2010.

[34] Satashu Goel and Rohit Negi. Guaranteeing secrecy using artificial noise. *Wireless Communications, IEEE Transactions on*, 7(6):2180–2189, 2008.

[35] Raef Bassily, Ersen Ekrem, Xiang He, Eylem Tekin, Jianwei Xie, Mark Bloch, Sennur Ulukus, and Aylin Yener. Cooperative security at the physical layer: A summary of recent advances. *Signal Processing Magazine, IEEE*, 30(5):16–28, 2013.

[36] Ioannis Krikidis, John S Thompson, and Steve McLaughlin. Relay selection for secure cooperative networks with jamming. *Wireless Communications, IEEE Transactions on*, 8(10):5003–5011, 2009.

[37] Lun Dong, Zhu Han, Athina P Petropulu, and H Vincent Poor. Improving wireless physical layer security via cooperating relays. *Signal Processing, IEEE Transactions on*, 58(3):1875–1888, 2010.

[38] Junsu Kim, Aissa Ikhlef, and Robert Schober. Combined relay selection and cooperative beamforming for physical layer security. *Communications and Networks, Journal of*, 14(4):364–373, 2012.

[39] Raef Bassily and Sennur Ulukus. Deaf cooperation and relay selection strategies for secure communication in multiple relay networks. *Signal Processing, IEEE Transactions on*, 61(6):1544–1554, 2013.

[40] Hui Hui, Guobing Li, Junli Liang, et al. Secure relay and jammer selection for physical layer security. *Signal Processing Letters, IEEE*, 22(8):1147–1151, 2015.

[41] Ahmed S Ibrahim, Ahmed K Sadek, Weifeng Su, and KJ Liu. Cooperative communications with relay-selection: when to cooperate and whom to cooperate with? *Wireless Communications, IEEE Transactions on*, 7(7):2814–2827, 2008.

[42] Qing F Zhou, Francis Lau, and Sau F Hau. Asymptotic analysis of opportunistic relaying protocols. *Wireless Communications, IEEE Transactions on*, 8(8):3915–3920, 2009.

[43] Xiaowen Gong, Thejaswi PS Chandrashekhar, Junshan Zhang, and H Vincent Poor. Opportunistic cooperative networking: To relay or not to relay? *Selected Areas in Communications, IEEE Journal on*, 30(2):307–314, 2012.

[44] Ioannis Krikidis. Opportunistic relay selection for cooperative networks with secrecy constraints. *Communications, IET*, 4(15):1787–1791, 2010.

[45] Yulong Zou, Xianbin Wang, and Weiming Shen. Optimal relay selection for physical-layer security in cooperative wireless networks. *Selected Areas in Communications, IEEE Journal on*, 31(10):2099–2111, 2013.

[46] Lisheng Fan, Xianfu Lei, Trung Q Duong, Maged Elkashlan, and George K Karagiannidis. Secure multiuser communications in multiple amplify-and-forward relay networks. *Communications, IEEE Transactions on*, 62(9):3299–3310, 2014.

[47] Hefdhallah Sakran, Mona Shokair, Omar Nasr, Sayed El-Rabaie, and Atef Abou El-Azm. Proposed relay selection scheme for physical layer security in cognitive radio networks. *Communications, IET*, 6(16):2676–2687, 2012.

[48] Azzam Y Al-nahari, Ioannis Krikidis, Ahmed S Ibrahim, Moawad I Dessouky, and Fathi E Abd El-Samie. Relaying techniques for enhancing the physical layer secrecy in cooperative networks with multiple eavesdroppers. *Transactions on Emerging Telecommunications Technologies*, 25(4):445–460, 2014.

[49] Yulong Zou, Jia Zhu, Xianbin Wang, and Victor Leung. Improving physical-layer security in wireless communications using diversity techniques. *Network, IEEE*, 29(1):42–48, 2015.

[50] Elisabeth Reusens, Wout Joseph, Benoît Latré, Bart Braem, Günter Vermeeren, Emmeric Tanghe, Luc Martens, Ingrid Moerman, and Chris Blondia. Characterization of on-body communication channel and energy efficient topology design for wireless body area networks. *Information Technology in Biomedicine, IEEE Transactions on*, 13(6):933–945, 2009.

[51] Stéphane Van Roy, François Quitin, LingFeng Liu, Claude Oestges, François Horlin, J Dricot, and Philippe De Doncker. Dynamic channel modeling for multi-sensor body area networks. *Antennas and Propagation, IEEE Transactions on*, 61(4):2200–2208, 2013.

[52] Bart Braem, Benoit Latre, Ingrid Moerman, Chris Blondia, Elisabeth Reusens, Wout Joseph, Luc Martens, and Piet Demeester. The need for cooperation and relaying in short-range high path loss sensor networks. In *Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on*, pages 566–571. IEEE, 2007.

[53] Aida Ehyaie, Massoud Hashemi, and Pejman Khadivi. Using relay network to increase life time in wireless body area sensor networks. In *World*

of Wireless, Mobile and Multimedia Networks & Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a, pages 1–6. IEEE, 2009.

[54] Raffaele D'Errico, Ramona Rosini, and Mickael Maman. A performance evaluation of cooperative schemes for on-body area networks based on measured time-variant channels. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–5. IEEE, 2011.

[55] Song Yang, Jia-Liang Lu, Fan Yang, Linghe Kong, Wei Shu, and Min-You Wu. Behavior-aware probabilistic routing for wireless body area sensor networks. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 444–449. IEEE, 2013.

[56] Jocelyne Elias, Abdallah Jarray, Javier Salazar, Ahmed Karmouch, and Ahmed Mehaoua. A reliable design of wireless body area networks. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 2742–2748. IEEE, 2013.

[57] KS Deepak and AV Babu. Improving energy efficiency of incremental relay based cooperative communications in wireless body area networks. *International Journal of Communication Systems*, 28(1):91–111, 2015.

[58] Jun-ichi Naganawa, Karma Wangchuk, Minseok Kim, Takahiro Aoyagi, and Jun-ichi Takada. Simulation-based scenario-specific channel modeling for wban cooperative transmission schemes. *Biomedical and Health Informatics, IEEE Journal of*, 19(2):559–570, 2015.

[59] Xiang He and Aylin Yener. Two-hop secure communication using an untrusted relay: A case for cooperative jamming. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5. IEEE, 2008.

[60] Xiang He and Aylin Yener. Cooperation with an untrusted relay: A secrecy perspective. *Information Theory, IEEE Transactions on*, 56(8):3807–3827, 2010.

[61] Cheol Jeong, Il-Min Kim, and Dong In Kim. Joint secure beamforming design at the source and the relay for an amplify-and-forward mimo untrusted relay system. *Signal Processing, IEEE Transactions on*, 60(1):310–325, 2012.

[62] Jing Huang, Arjun Mukherjee, and A Lee Swindlehurst. Secure communication via an untrusted non-regenerative relay in fading channels. *Signal Processing, IEEE Transactions on*, 61(10):2536–2550, 2013.

[63] Lifeng Wang, Maged Elkashlan, Jing Huang, Nghi H Tran, and Trung Q Duong. Secure transmission with optimal power allocation in untrusted relay networks. *Wireless Communications Letters, IEEE*, 3(3):289–292, 2014.

[64] Li Sun, Taiyi Zhang, Yubo Li, and Hao Niu. Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes. *Vehicular Technology, IEEE Transactions on*, 61(8):3801–3807, 2012.

[65] Li Sun, Pinyi Ren, Qinghe Du, Yichen Wang, and Zhenzhen Gao. Security-aware relaying scheme for cooperative networks with untrusted relay nodes. *Communications Letters, IEEE*, 19(3):463–466, 2015.

[66] Jung-Bin Kim, Jaesung Lim, and John M. Cioffi. Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays. *Wireless Communications, IEEE Transactions on*, 14(7):3866–3876, 2015.

[67] Patrick Murphy, Ashutosh Sabharwal, and Behnaam Aazhang. On building a cooperative communication system: Testbed implementation and first results. *EURASIP Journal on Wireless Communications and Networking*, 2009:7, 2009.

[68] Thanasis Korakis, Michael Knox, Elza Erkip, and Shivendra Panwar. Cooperative network implementation using open-source platforms. *Communications Magazine, IEEE*, 47(2):134–141, 2009.

[69] Patrick Murphy and Ashutosh Sabharwal. Design, implementation, and characterization of a cooperative communications system. *Vehicular Technology, IEEE Transactions on*, 60(6):2534–2544, 2011.

[70] Dejun Yang, Xi Fang, and Guoliang Xue. Game theory in cooperative communications. *Wireless Communications, IEEE*, 19(2):44–49, 2012.

[71] Yingda Chen and Shalinee Kishore. A game-theoretic analysis of decode-and-forward user cooperation. *Wireless Communications, IEEE Transactions on*, 7(5):1941–1951, 2008.

[72] Matthew Nokleby and Behnaam Aazhang. User cooperation for energy-efficient cellular communications. In *Communications (ICC), 2010 IEEE International Conference on*, pages 1–5. IEEE, 2010.

[73] Beibei Wang, Zhu Han, and KJ Liu. Distributed relay selection and power control for multiuser cooperative communication networks using stackelberg game. *Mobile Computing, IEEE Transactions on*, 8(7):975–990, 2009.

[74] Majid Janzamin, MohammadReza Pakravan, and Hanie Sedghi. A game-theoretic approach for power allocation in bidirectional cooperative communication. In *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, pages 1–6. IEEE, 2010.

[75] Jianwei Huang, Zhu Han, Mung Chiang, and H Vincent Poor. Auction-based resource allocation for cooperative communications. *Selected Areas in Communications, IEEE Journal on*, 26(7):1226–1237, 2008.

[76] Andreas F Molisch. *Wireless communications*. John Wiley & Sons, 2012.

[77] William CY Lee and Yu S Yeh. Polarization diversity system for mobile radio. *Communications, IEEE Transactions on*, 20(5):912–923, 1972.

[78] Rodney Vaughan and J Bach Andersen. *Channels, propagation and antennas for mobile communications*. Number 50. Iet, 2003.

[79] Paul Mattheijssen, Matti HAJ Herben, Guido Dolmans, and Lukas Leyten. Antenna-pattern diversity versus space diversity for use at handhelds. *Vehicular Technology, IEEE Transactions on*, 53(4):1035–1042, 2004.

[80] Walid Saad, Zhu Han, Tamer Başar, Mérouane Debbah, and Are Hjørungnes. Physical layer security: Coalitional games for distributed cooperation. In *Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2009. WiOPT 2009. 7th International Symposium on*, pages 1–8. IEEE, 2009.

[81] Zhu Han, Ninoslav Marina, Mérouane Debbah, and Are Hjørungnes. Physical layer security game: interaction between source, eavesdropper, and friendly jammer. *EURASIP Journal on Wireless Communications and Networking*, 2009:11, 2009.

[82] Igor Stanojev and Aylin Yener. Improving secrecy rate via spectrum leasing for friendly jamming. *Wireless Communications, IEEE Transactions on*, 12(1):134–145, 2013.

[83] An Wang, Yueming Cai, Wendong Yang, and Zhao Hou. A stackelberg security game with cooperative jamming over a multiuser ofdma network. In *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, pages 4169–4174. IEEE, 2013.

[84] O Ozan Koyluoglu, Can Emre Koksal, and Hesham El Gamal. On secrecy capacity scaling in wireless networks. *Information Theory, IEEE Transactions on*, 58(5):3000–3015, 2012.

[85] Aggelos Bletsas, Ashish Khisti, David P Reed, and Andrew Lippman. A simple cooperative diversity method based on network path selection. *Selected Areas in Communications, IEEE Journal on*, 24(3):659–672, 2006.

[86] Hyo-Sang Lim, Gabriel Ghinita, Elisa Bertino, and Murat Kantarcioglu. A game-theoretic approach for high-assurance of data trustworthiness in sensor networks. In *Data Engineering (ICDE), 2012 IEEE 28th International Conference on*, pages 1192–1203. IEEE, 2012.

[87] Yindi Jing and Hamid Jafarkhani. Single and multiple relay selection schemes and their achievable diversity orders. *Wireless Communications, IEEE Transactions on*, 8(3):1414–1423, 2009.

[88] Yang Liu, Yi Man, Mei Song, Hongtao Zhang, and Li Wang. A cooperative diversity transmission scheme by superposition coding relaying for a wireless system with multiple relays. *Wireless Networks*, pages 1–17, 2014.

[89] Nikolaos Nomikos, Themistoklis Charalambous, Ioannis Krikidis, Dimitrios Skoutas, Demosthenes Vouyioukas, and Mikael Johansson. A buffer-aided successive opportunistic relay selection scheme with power adaptation and inter-relay interference cancellation for cooperative diversity systems. *Communications, IEEE Transactions on*, 63(5):1623–1634, 2015.

[90] Jianhua Mo, Meixia Tao, and Yuan Liu. Relay placement for physical layer security: A secure connection perspective. *Communications Letters, IEEE*, 16(6):878–881, 2012.

[91] Lifeng Lai and Hesham El Gamal. The relay–eavesdropper channel: Cooperation for secrecy. *Information Theory, IEEE Transactions on*, 54(9):4005–4019, 2008.

[92] Zohaib Hassan Awan, Abdellatif Zaidi, and Luc Vandendorpe. Secure communication over parallel relay channel. *Information Forensics and Security, IEEE Transactions on*, 7(2):359–371, 2012.

[93] Yulong Zou, Xuelong Li, and Ying-Chang Liang. Secrecy outage and diversity analysis of cognitive radio systems. *Selected Areas in Communications, IEEE Journal on*, 32(11):2222–2236, 2014.

[94] Alan Jeffrey and Daniel Zwillinger. *Table of integrals, series, and products*. Academic Press, 2007.

[95] Sam Vakil and Ben Liang. Decentralized multiuser diversity with cooperative relaying in wireless sensor networks. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*, pages 560–569. IEEE, 2007.

[96] Hee-Jin Joung and Cheol Mun. Capacity of multiuser diversity with cooperative relaying in wireless networks. *Communications Letters, IEEE*, 12(10):752–754, 2008.

[97] Xing Zhang, Wenbo Wang, and Xiaodong Ji. Multiuser diversity in multiuser two-hop cooperative relay wireless networks: system model and performance analysis. *Vehicular Technology, IEEE Transactions on*, 58(2):1031–1036, 2009.

[98] Shuping Chen, Wenbo Wang, and Xing Zhang. Performance analysis of multiuser diversity in cooperative multi-relay networks under rayleigh-fading channels. *Wireless Communications, IEEE Transactions on*, 8(7):3415–3419, 2009.

[99] Constantine A Balanis. *Antenna theory: analysis and design*. John Wiley & Sons, 2005.

[100] Jie Dong and David Smith. Cooperative body-area-communications: Enhancing coexistence without coordination between networks. In *Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on*, pages 2269–2274. IEEE, 2012.

[101] David JC MacKay. Fountain codes. *IEE Proceedings-Communications*, 152(6):1062–1068, 2005.

[102] Thomas Courtade, Richard D Wesel, et al. A cross-layer perspective on rateless coding for wireless channels. In *Communications, 2009. ICC'09. IEEE International Conference on*, pages 1–6. IEEE, 2009.

[103] Xijun Wang, Wei Chen, and Zhigang Cao. Sparc: superposition-aided rateless coding in wireless relay systems. *Vehicular Technology, IEEE Transactions on*, 60(9):4427–4438, 2011.

[104] Thomas Stockhammer, Amin Shokrollahi, Mark Watson, Michael Luby, and Tiago Gasiba. Application layer forward error correction for mobile multimedia broadcasting. Technical report, CRC Press, 2008.

[105] 3GPP TS 26.346. 3rd generation partnership project;. technical specification group services and system aspects;. multimedia broadcast/multicast service (mbms);. protocols and codecs (release 10). 2010.

[106] Bappi Barua, Hien Quoc Ngo, and Hyundong Shin. On the sep of cooperative diversity with opportunistic relaying. *Communications Letters, IEEE*, 12(10):727–729, 2008.

[107] Hamid Khodakarami and Farshad Lahouti. Link adaptation with untrusted relay assignment: Design and performance analysis. *Communications, IEEE Transactions on*, 61(12):4874–4883, 2013.

[108] Aydin Behnad, Reza Parseh, and Hamid Khodakarami. Upper bound for the performance metrics of amplify-and-forward cooperative networks based on harmonic mean approximation. In *Telecommunications (ICT), 2011 18th International Conference on*, pages 157–161. IEEE, 2011.

List of Published Papers

Journal Articles

1. Hao Niu, Nanhao Zhu, Li Sun, Athanasios V. Vasilakos, and Kaoru Sezaki, Security-embedded opportunistic user cooperation with full diversity, Wireless Networks (Springer), DOI:10.1007/s11276-015-1044-7, Aug. 2015.

2. Hao Niu, Masayuki Iwai, Kaoru Sezaki, Li Sun, and Qinghe Du, Exploiting fountain codes for secure wireless delivery, IEEE Communications Letters, vol. 18, no. 5, pp. 777-780, May 2014.

3. Hao Niu, Li Sun, Masayuki Iwai, and Kaoru Sezaki, Secrecy-enhanced cooperation scheme with multiuser diversity in wireless relay networks, IEICE Communications Express, vol. 2, no. 10, pp. 409-414, Oct. 2013.

International Conference Papers

1. Hao Niu, Li Sun, Masaki Ito, and Kaoru Sezaki, Secure transmission through multihop relaying in wireless body area networks, IEEE Global Conference on Consumer Electronics (GCCE), Tokyo, Oct.7-10, 2014, pp. 395-396.

2. Hao Niu, Li Sun, Masaki Ito, and Kaoru Sezaki, User cooperation analysis under eavesdropping attack: a game theory perspective, IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Washington D.C., Sept. 2-5, 2014. pp. 139-144.

Domestic Conference Papers

1. Hao Niu, Tiantian Jiang, Masaki Ito, and Kaoru Sezaki, Relay selection scheme with a more precise definition of secrecy capacity for decode-and-forward cooperative data transmission, 2015 IEICE General Conference, vol. BS-3-49, Mar. 2015.

2. Hao Niu, Tiantian Jiang, Masaki Ito, and Kaoru Sezaki, Secure co-

operation scheme using fountain codes to resist untrustworthy relay, IEICE Technical Report, vol. 114, no. 395, pp.147-150, Jan. 2015.

3. Hao Niu, and Kaoru Sezaki, Secure communication through matrix transform in wireless networks, 2014 IEICE General Conference, vol. BS-1-39, Mar. 2014.

4. Hao Niu, Masayuki Iwai, and Kaoru Sezaki, Improving the secrecy performance of cooperative networks via adaptive transmission and multiuser diversity, IEICE Technical Report, vol. 112, no. 239, pp. 201-204, Oct. 2012.

5. Hao Niu, Masayuki Iwai, and Kaoru Sezaki, Outage-optimal relay selection with jamming for secrecy purpose in cooperative networks, 2012 IEICE Society Conference, vol. BS-5-39, Sept. 2012.